ANNALES

DE

L'INSTITUT FOURIER

Everett W. HOWE, Enric NART & Christophe RITZENTHALER

Jacobians in isogeny classes of abelian surfaces over finite fields

Tome 59, nº 1 (2009), p. 239-289.

<http://aif.cedram.org/item?id=AIF_2009__59_1_239_0>

Ann. Inst. Fourier, Grenoble
59, 1 (2009) 239-289

JACOBIANS IN ISOGENY CLASSES OF ABELIAN SURFACES OVER FINITE FIELDS

by Everett W. HOWE,
Enric NART & Christophe RITZENTHALER (*)

ABSTRACT. — We give a complete answer to the question of which polynomials occur as the characteristic polynomials of Frobenius for genus-2 curves over finite fields.

RÉSUMÉ. — Nous donnons une réponse complète à la question de savoir quels sont les polynômes caractéristiques du Frobenius des courbes de genre 2 sur les corps finis.

1. Introduction

The *Weil polynomial* of an abelian variety over a finite field $\mathbb{F}_q$ is the characteristic polynomial of its Frobenius endomorphism; the *Weil polynomial* of a curve over $\mathbb{F}_q$ is the Weil polynomial of its Jacobian. In this paper we determine which polynomials occur as the Weil polynomials of genus-2 curves over a finite field.

Weil's 'Riemann Hypothesis' shows that the Weil polynomial of an abelian surface over $\mathbb{F}_q$ has the form

$$x^4 + ax^3 + bx^2 + aqx + q^2,$$

and the Honda-Tate theorem [36] makes it a straightforward matter to determine which such polynomials come from abelian surfaces (see [31, Thm. 1.1], [25, Thm. 2.9], and the Appendix to this paper). Since two abelian varieties over $\mathbb{F}_q$ are isogenous to one another if and only if they

Keywords: Curve, Jacobian, abelian surface, zeta function, Weil polynomial, Weil number.
Math. classification: 11G20, 14G10, 14G15.
(*) The second author was supported in part by project MTM2006-11391 from the Spanish MEC.

have the same Weil polynomial [35], we may phrase our main question as follows.

Question 1.1. — (cf. [1, Question 11.3]) *Suppose $f = x^4 + ax^3 + bx^2 + aqx + q^2$ is the Weil polynomial for an isogeny class of abelian surfaces over $\mathbb{F}_q$. Is there a projective smooth genus-2 curve over $\mathbb{F}_q$ whose Weil polynomial is equal to f ?*

While this question has been settled in many special cases (as we explain in detail below), until now there have been two kinds of isogeny classes for which the question has remained largely unanswered: the split isogeny classes and the supersingular isogeny classes. We analyze these two remaining cases and provide a complete answer to Question 1.1.

Theorem 1.2. — *Let $f = x^4 + ax^3 + bx^2 + aqx + q^2$ be the Weil polynomial of an isogeny class $\mathcal{A}$ of abelian surfaces over $\mathbb{F}_q$, where q is a power of a prime p.*

(1) *Suppose that $\mathcal{A}$ contains a product of elliptic curves, so that f can be written as a product*

$$f = (x^2 - sx + q)(x^2 - tx + q)$$

where the two factors are the Weil polynomials of isogeny classes of elliptic curves over $\mathbb{F}_q$ and where we may assume that $|s| \geqslant |t|$. Then $\mathcal{A}$ does not contain a Jacobian if and only if the conditions in one of the rows of Table 1.1 are met.

(2) *Suppose that $\mathcal{A}$ is simple. Then $\mathcal{A}$ does not contain a Jacobian if and only if the conditions in one of the rows of Table 1.2 are met.*

The analog of Question 1.1 for elliptic curves was answered by Waterhouse [37, Thm. 4.1]. The generalization from elliptic curves to genus-2 curves is surely quite natural, but to the best of our knowledge Question 1.1 did not occur in print until 1990, when Rück [31] provided some sufficient conditions for a positive answer to the question. In the literature starting with Rück we find a large variety of methods and techniques that provide both positive and negative answers to Question 1.1 for particular classes of Weil polynomials. Almost all of the positive results are based on the following theorem of Weil; the version we give here is due to González, Guàrdia, and Rotger [3, Thm. 3.1].

Theorem 1.3 (Weil). — *Let (A, λ) be a principally polarized abelian surface defined over a field k. Then (A, λ) is either*

(a) *the polarized Jacobian of a genus-2 curve over k,*

(b) *the product of two polarized elliptic curves over k, or*
(c) *the restriction of scalars of a polarized elliptic curve over a quadratic extension of k.*

Furthermore, these three possibilities are mutually exclusive.

Let us say that an isogeny class of abelian varieties is *principally polarizable* if it contains a principally polarized variety. In light of Weil's theorem, if an isogeny class of abelian surfaces over $\mathbb{F}_q$ is simple over $\mathbb{F}_{q^2}$, then it contains a Jacobian if and only if it is principally polarizable. The problem of determining the principally polarizable isogeny classes of abelian varieties was studied by the first author in a series of papers [7], [8], [9], where he expressed the obstruction to the existence of principal polarizations in terms of the vanishing of an element of a group constructed from the Grothendieck group of the category of finite group schemes that can be embedded in varieties in the isogeny class. Recall that an abelian surface over a field of characteristic $p > 0$ is said to be *ordinary* when its p-rank is 2, *almost ordinary* when its p-rank is 1, and *supersingular* when its p-rank is 0; the p-rank of an abelian surface over a finite field can be read from the Newton polygon of the Weil polynomial in a well-known way. The principally polarizable isogeny classes of ordinary abelian surfaces over a finite field were determined in [7, Thm. 1.3]. In [25] it was proved

p-rank of $\mathcal{A}$	**Condition on p and q**	**Conditions on s and t**
—	—	$\lvert s-t\rvert = 1$
2	—	$s = t$ and $t^2 - 4q \in \{-3, -4, -7\}$
	$q = 2$	$\lvert s\rvert = \lvert t\rvert = 1$ and $s \neq t$
1	q square	$s^2 = 4q$ and $s - t$ squarefree
0	$p > 3$	$s^2 \neq t^2$
	$p = 3$ and q nonsquare	$s^2 = t^2 = 3q$
	$p = 3$ and q square	$s - t$ is not divisible by $3\sqrt{q}$
	$p = 2$	$s^2 - t^2$ is not divisible by $2q$
	$q = 2$ or $q = 3$	$s = t$
	$q = 4$ or $q = 9$	$s^2 = t^2 = 4q$

Table 1.1. Conditions that ensure that the split isogeny class with Weil polynomial $(x^2 - sx + q)(x^2 - tx + q)$ does not contain a Jacobian. Here we assume that $\lvert s\rvert \geqslant \lvert t\rvert$.

p-rank of $\mathcal{A}$	**Condition on p and q**	**Conditions on s and t**
—	—	$a^2 - b = q$ and $b < 0$ and all prime divisors of b are 1 mod 3
2	—	$a = 0$ and $b = 1 - 2q$
	$p > 2$	$a = 0$ and $b = 2 - 2q$
0	$p \equiv 11 \bmod 12$ and q square	$a = 0$ and $b = -q$
	$p = 3$ and q square	$a = 0$ and $b = -q$
	$p = 2$ and q nonsquare	$a = 0$ and $b = -q$
	$q = 2$ or $q = 3$	$a = 0$ and $b = -2q$

Table 1.2. Conditions that ensure that the simple isogeny class with Weil polynomial $x^4 + ax^3 + bx^2 + aqx + q^2$ does not contain a Jacobian.

that all almost-ordinary isogeny classes over a finite field are principally polarizable by applying criteria developed in [8]; in particular, since the simple almost-ordinary classes are absolutely simple they always contain Jacobians. Finally, the supersingular case was worked out in [14] using the ideas of [8] and [9]. Gathering all these results one obtains:

Theorem 1.4 ([14]). — *Let $\mathcal{A}$ be an isogeny class of abelian surfaces over $\mathbb{F}_q$ with Weil polynomial $x^4 + ax^3 + bx^2 + aqx + q^2$. Then $\mathcal{A}$ is not principally polarizable if and only if the following three conditions are satisfied*:

(a) $a^2 - b = q$,

(b) $b < 0$, *and*

(c) *all prime divisors of* b *are congruent to* 1 *modulo* 3.

This result, together with Weil's theorem, answers Question 1.1 for every isogeny class that is simple over $\mathbb{F}_{q^2}$.

The answer to Question 1.1 for the simple ordinary isogeny classes that split over $\mathbb{F}_{q^2}$ was determined by the first author and Maisner. The Weil polynomial of such an isogeny class is of the form $x^4 + bx^2 + q^2$. The first author [25, App.] proved that when $b = 1 - 2q$ there is no curve with the given Weil polynomial by showing that such a curve would have an automorphism whose existence is incompatible with the number of rational points on the curve over $\mathbb{F}_{q^2}$. For $p > 2$, the first author [10] used a counting argument to show that when $b = 2 - 2q$ there is again no curve with the given Weil polynomial. He found explicit formulas for the number of principally polarized surfaces (A,λ) with A belonging to the given isogeny class, as well as for the number of these polarized surfaces that are restrictions of scalars of elliptic curves over $\mathbb{F}_{q^2}$. The formulas for these two numbers both involve arithmetic invariants of the biquadratic field generated by the Weil polynomial, and a comparison of the two numbers using the Brauer relations shows that they coincide; thus, all (A,λ) are non-Jacobians. Maisner [23] extended these ideas to show that for all other values of b coming from simple isogeny classes, there is a curve with the given Weil polynomial.

For supersingular surfaces over finite fields of characteristic 2, Question 1.1 was answered by Maisner and the second author [24] by an explicit computation of the zeta functions of all supersingular curves of genus 2, using ideas of van der Geer and van der Vlugt [2]. For supersingular surfaces over finite fields of characteristic 3, the question was answered by the first author [11], again by explicit methods.

McGuire and Voloch [26, §3] determined which isogeny classes of split almost-ordinary abelian surfaces contain Jacobians, and gave the complete details of the argument in the case that one factor of the Weil polynomial of the isogeny class is $x^2 \pm 2\sqrt{q}x + q$.

In this paper we cover the last steps to get a complete answer to Question 1.1. In Part 1 we deal with the split isogeny classes not covered by the work of McGuire and Voloch, and in Part 2 we study the simple supersingular isogeny classes that split over $\mathbb{F}_{q^2}$. These cases are solved with the use of completely different techniques. For the split case we use a result of Kani [19] that characterizes when two elliptic curves can be tied together along finite subgroups to get a common covering by a curve of genus two; Kani's result reduces the question of whether there is a Jacobian isogenous to a product $E \times F$ of two elliptic curves to the question of whether for some $n > 1$ there is an isomorphism from $E[n]$ to $F[n]$ that is an anti-isometry with respect to the Weil pairing (and that is 'non-reducible', see §3). In order to understand the split supersingular case, we determine the Galois twists of the Dieudonné modules of certain supersingular elliptic curves. For the simple supersingular case we use results of Oort [29], Katsura and Oort [20], and Ibukiyama, Katsura, and Oort [16] on supersingular abelian surfaces over the algebraic closures of finite fields and their polarizations. Using these results, together with the theory of twists and work of Hashimoto and Ibukiyama [5] and Ibukiyama [15] on quaternion hermitian forms, we determine which simple supersingular isogeny classes contain geometrically non-split principally polarized surfaces.

In our analyses of the supersingular isogeny classes, both split and simple, it is convenient to assume that the characteristic of the base field is larger than 3. We may make this assumption because the characteristic 2 case is settled in [24] and the characteristic 3 case in [11].

Conventions and notation. When we speak of a *variety* over a finite field k, we mean a variety defined over the algebraic closure $\overline{k}$ of k together with Galois descent data. By a *morphism* of varieties over a finite field k, we mean a morphism of varieties over $\overline{k}$ that is Galois-equivariant. By a *geometric morphism* of varieties over k, we mean a morphism of varieties over $\overline{k}$. Thus, if E_1 and E_2 are elliptic curves over a finite field, we will often speak of geometric isogenies from E_1 to E_2. As a consequence of this convention, operators such as Hom and End applied to varieties over k will always refer to k-rational homomorphisms and endomorphisms.

If q is a power of a prime p, say $q = p^m$, we let $\mathbb{Q}_q$ denote the unramified degree-m extension of the p-adic numbers $\mathbb{Q}_p$, and we let $\mathbb{Z}_q$ denote the ring of integers of $\mathbb{Q}_q$. We will sometimes denote by $\mathcal{A}_{(a,b)}$ the isogeny class of abelian surfaces over $\mathbb{F}_q$ with Weil polynomial $x^4 + ax^3 + bx^2 + aqx + q^2$.

Part 1. Split abelian surfaces as Jacobians

2. Introduction

In this part of the paper we determine the Weil polynomials of the split isogeny classes of abelian surfaces that contain Jacobians.

Our first two theorems concern the case of isogeny classes that contain product surfaces of the form $E_1 \times E_2$, where E_1 and E_2 are elliptic curves over $\mathbb{F}_q$ that are not isogenous to one another and that are not both supersingular. Let s and t be the traces of the Frobenius endomorphisms of E_1 and E_2, respectively, so that $s \neq t$ and so that the Weil polynomial of $E_1 \times E_2$ is

$$(x^2 - sx + q)(x^2 - tx + q).$$

Theorem 2.1. — *Suppose that neither s^2 nor t^2 is equal to $4q$ and that E_1 and E_2 are not both supersingular. Then there is a Jacobian isogenous to $E_1 \times E_2$ if and only if $|s - t| \neq 1$ and $\{q, \{s, t\}\} \neq \{2, \{1, -1\}\}$.*

Theorem 2.2. — *Suppose that E_2 is ordinary and that $s^2 = 4q$, so that E_1 is supersingular. Then there is a Jacobian isogenous to $E_1 \times E_2$ if and only if $s - t$ is divisible by the square of an integer greater than 1.*

Theorem 2.2 was proven by McGuire and Voloch [26], who also mention the special case of Theorem 2.1 in which one of the curves is supersingular. We reprove their results here for completeness.

Next we consider isogeny classes that contain squares of ordinary elliptic curves.

Theorem 2.3. — *Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with trace of Frobenius equal to t. Then there is a Jacobian isogenous to $E \times E$ if and only if $t^2 - 4q$ is neither -3 nor -4 nor -7.*

Finally, we turn to the split supersingular isogeny classes. We restrict our attention to finite fields of characteristic greater than 3, because the characteristic 3 case is considered in [11] and the characteristic 2 case is considered in [24]. Suppose that E_1 and E_2 are supersingular elliptic curves over a finite field $\mathbb{F}_q$ of characteristic greater than 3, and let s and t be the traces of Frobenius of E_1 and E_2, respectively.

Theorem 2.4. — *There is a Jacobian isogenous to $E_1 \times E_2$ if and only if $s^2 = t^2$.*

Our main tool in proving these theorems is a result of Kani [19], which we review in §3. In §4 we state and prove a few elementary lemmas that we will need later in the paper. In §5, §6, and §7 we prove our theorems for split non-supersingular isogeny classes. In §8 we compute certain twists of the Dieudonné modules of supersingular elliptic curves, and in §9 we use these computations to prove Theorem 2.4.

3. Tying elliptic curves together along torsion subgroups

In this section we review a result of Kani that gives necessary and sufficient conditions for certain split abelian surfaces to be Jacobians.

Suppose E_1 and E_2 are elliptic curves over a field k and let n be a positive integer. Suppose $\psi\colon E_1[n] \to E_2[n]$ is an isomorphism of group schemes over k that is an anti-isometry with respect to the Weil pairings on $E_1[n]$ and $E_2[n]$. Let A be the abelian surface $(E_1 \times E_2)/\operatorname{Graph}(\psi)$ and let $\varphi\colon E_1 \times E_2 \to A$ be the natural isogeny. Then A fits in a diagram

$$\begin{tikzcd} E_1 \times E_2 \arrow[r, "n"] \arrow[d, "\varphi"] & E_1 \times E_2 \\ A \arrow[r, "\lambda"] & \widehat{A}. \arrow[u, "\widehat{\varphi}"'] \end{tikzcd}$$

Here the top arrow is the multiplication-by-n map and $\widehat{A}$ is the dual abelian surface of A. The existence of the bottom arrow follows from the fact that the graph of ψ is a maximal isotropic subgroup of the n-torsion of $E_1 \times E_2$ (see [27, Prop. 16.8, p. 135]). In fact, the induced map $\lambda\colon A \to \widehat{A}$ is a polarization, and by looking at the degrees of the maps in the diagram we see that λ is a principal polarization. Conversely, if λ is a principal polarization of a non-simple abelian surface A over k, then λ can be obtained in this way from a pair of elliptic curves (E_1, E_2) and an anti-isometry $E_1[n] \to E_2[n]$, for some n.

Kani [19] gives a criterion that allows one to determine when a principally polarized surface (A, λ) obtained from an anti-isometry $\psi\colon E_1[n] \to E_2[n]$ is isomorphic to the Jacobian of a curve. The criterion is easiest to state when n is a prime.

Theorem 3.1 (Kani [19, Thm. 3, p. 95]). — *Suppose n is a prime, and let E_1, E_2, and ψ be as in the discussion above. The principally polarized surface*

$$(E_1 \times E_2)/\operatorname{Graph}(\psi)$$

is not a Jacobian if and only if there is an integer i (with $0 < i < n$) and a geometric isogeny $\varphi\colon E_1 \to E_2$ of degree $i(n-i)$ such that $i\psi = \varphi|_{E_1[n]}$.

There is a more complicated criterion when n is composite. We will only need to use the case $n = 4$.

Theorem 3.2 (Kani). — *Suppose $n = 4$ and the characteristic of the base field k is not equal to 2. Let E_1, E_2, and ψ be as in the discussion above. The principally polarized surface*

$$(E_1 \times E_2)/\operatorname{Graph}(\psi)$$

is not a Jacobian if and only if one of the following conditions holds:

(a) *There is a geometric isogeny $\varphi\colon E_1 \to E_2$ of degree 3 such that $\psi = \varphi|_{E_1[n]}$.*

(b) *There are two order-2 subgroups G_1 and G_2 of $E_1(\overline{\mathbb{F}}_q)$ and a geometric isomorphism $\varphi\colon E_1 \to E_2$ such that the graph of ψ is equal to the set of points $(x, \varphi(y))$ in $E_1[4](\overline{\mathbb{F}}_q) \times E_2[4](\overline{\mathbb{F}}_q)$ such that $x + y \in G_1$ and $x - y \in G_2$.*

Proof. — This follows from Theorem 2.6 of [19]. We make the assumption about the characteristic of k not being 2 only so that condition (b) can be stated in terms of groups and not group-schemes. □

We say that an anti-isometry $\psi\colon E_1[n] \to E_2[n]$ is *reducible* if (A, λ) is not a Jacobian. If ψ is not reducible, then we refer to the process of constructing a Jacobian from E_1, E_2, and ψ as *tying E_1 and E_2 together along their n-torsion subgroups via ψ.*

4. Useful lemmas

In this section we present some lemmas that will be helpful in later sections.

Suppose that E is an elliptic curve over $\mathbb{F}_q$ with trace of Frobenius t, and suppose that $t^2 \neq 4q$. Let π be the Frobenius endomorphism of E and let R be the subring $\mathbb{Z}[\pi]$ of $\mathrm{End}(E)$. Then R is an imaginary quadratic order of discriminant $t^2 - 4q$. Let $\mathcal{O}$ be the integral closure of R in $R \otimes \mathbb{Q}$. The endomorphism ring of E is an order that is contained in $\mathcal{O}$ and that contains R. Let ℓ be a prime integer. We say that E is *maximal* at ℓ if ℓ does not divide the index of $\mathrm{End}(E)$ in $\mathcal{O}$. We say that E is *minimal* at ℓ if ℓ does not divide the index of R in $\mathrm{End}(E)$.

Given an E as above, let ℓ be a prime that does not divide both t and q. Then it follows from [37, Thm. 4.2] that there is a curve isogenous to E that is minimal at ℓ.

Lemma 4.1. — *Let E be an elliptic curve over $\mathbb{F}_q$ whose Weil polynomial is $x^2 - tx + q$, and suppose that $t^2 \neq 4q$. Let ℓ be a prime that does not divide both t and q, and suppose that E is minimal at ℓ. Then the minimal polynomial of Frobenius acting on $E[\ell]$ is $x^2 - tx + q \in \mathbb{F}_\ell[x]$.*

Proof. — The characteristic polynomial of Frobenius on $E[\ell]$ is $x^2 - tx + q$, and the only way that this might not be the minimal polynomial of Frobenius is if $t^2 - 4q \equiv 0 \bmod \ell$.

Suppose $t^2 - 4q \equiv 0 \bmod \ell$. Let b be an integer such that $t \equiv 2b \bmod \ell$, and let π be the Frobenius endomorphism of E. Then the characteristic polynomial of π on $E[\ell]$ is $(x - b)^2$, and the minimal polynomial will be $x - b$ if and only if $(\pi - b)/\ell$ lies in $\mathrm{End}(E)$. But the index of $\mathbb{Z}[\pi]$ in $\mathrm{End}(E)$ is coprime to ℓ by assumption. $\square$

Lemma 4.2. — *Let ℓ be either 4 or an odd prime and let K be an imaginary quadratic field whose discriminant is not equal to $-\ell$. Then there are infinitely many rational primes m that split in K and that are nonsquares modulo ℓ.*

Proof. — Let Δ be the discriminant of K. The splitting of a rational prime in K depends only on its congruence class modulo Δ. If Δ is coprime to ℓ, then we can choose a congruence class modulo $\ell\Delta$ such that every prime m in this congruence class splits in K and is a nonsquare modulo ℓ. So from this point on we consider the case where ℓ and Δ have a common factor.

We first consider the case where ℓ is prime.

Write $\Delta = -2^e\ell D$ for some odd positive D, and suppose that $D > 1$. If m is a prime that is congruent to 1 modulo 8, that is not a square modulo ℓ, and such that the Jacobi symbol (m/D) is -1, then we have

$$\left(\frac{\Delta}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{2}{m}\right)^e\left(\frac{\ell}{m}\right)\left(\frac{D}{m}\right) = 1 \cdot 1 \cdot \left(\frac{m}{\ell}\right)\left(\frac{m}{D}\right) = 1.$$

So when $D > 1$, there are infinitely many primes that split in K and that are not squares modulo ℓ.

Suppose $D = 1$, so that either $\Delta = -8\ell$ or $\Delta = -4\ell$. Suppose $\Delta = -8\ell$. Then if m is a prime that is congruent to 5 modulo 8 and that is a nonsquare modulo ℓ, then

$$\left(\frac{\Delta}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{2}{m}\right)\left(\frac{\ell}{m}\right) = 1 \cdot (-1) \cdot \left(\frac{m}{\ell}\right) = 1.$$

On the other hand, suppose that $\Delta = -4\ell$. This can only happen if $\ell \equiv 1 \bmod 4$. If m is a prime that is congruent to 3 modulo 4 and that is a nonsquare modulo ℓ, then

$$\left(\frac{\Delta}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{\ell}{m}\right) = (-1) \cdot \left(\frac{m}{\ell}\right) = 1.$$

Thus, in every case there are infinitely many primes that split in K and that are not squares modulo ℓ.

Next we consider the case where $\ell = 4$.

Suppose $\Delta = -4D$ for some odd $D > 1$. This can only be the case if $D \equiv 1 \bmod 4$. If m is a prime that is congruent to 3 modulo 4 and such that the Jacobi symbol (m/D) is -1, then we have

$$\left(\frac{\Delta}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{D}{m}\right) = (-1) \cdot \left(\frac{m}{D}\right) = 1,$$

and we see that there are infinitely many primes that split in K and that are not squares modulo ℓ.

Suppose $\Delta = -8D$ for some odd $D > 0$ (with $D = 1$ being allowed). Suppose $D \equiv 1 \bmod 4$. Then if m is a prime that is 3 modulo 8 and such that the Jacobi symbol (m/D) is 1, we have

$$\left(\frac{\Delta}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{2}{m}\right)\left(\frac{D}{m}\right) = (-1)\cdot(-1)\cdot\left(\frac{m}{D}\right) = 1.$$

On the other hand, if $D \equiv 3 \bmod 4$, we can consider primes m that are 7 modulo 8 and such that the Jacobi symbol (m/D) is -1, so that

$$\left(\frac{\Delta}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{2}{m}\right)\left(\frac{D}{m}\right) = (-1)\cdot 1\cdot\left(\frac{m}{D}\right) = 1.$$

Again we see that in both cases there are infinitely many primes that split in K and that are not squares modulo ℓ. □

Next we present a lemma that provides us with a large supply of anti-isometries. This lemma and the one that follows it will refer to integers ℓ that are assumed to be either prime or equal to 4. It will be convenient to define ℓ^* to be the unique prime divisor of such an integer ℓ.

Lemma 4.3. — *Let E_1 and E_2 be elliptic curves over a finite field $\mathbb{F}_q$ and let s and t be their traces of Frobenius. Suppose that $|s-t|$ is neither 0 nor 1 and that neither s^2 nor t^2 is equal to $4q$. Let ℓ be a divisor of $s-t$ that is either 4 or a prime, and assume that ℓ is coprime to q if either E_1 or E_2 is supersingular. If $\ell = 2$ then let $m = 1$; otherwise, let m be a positive integer coprime to ℓ whose image in $(\mathbb{Z}/\ell\mathbb{Z})$ is a nonsquare. Suppose that E_1 and E_2 are minimal at ℓ^*, and that E_1' is an elliptic curve that is m-isogenous to E_1. Then either there is an $\mathbb{F}_q$-defined anti-isometry from $E_1[\ell]$ to $E_2[\ell]$, or there is one from $E_1'[\ell]$ to $E_2[\ell]$.*

Proof. — By Lemma 4.1 the minimal polynomials of Frobenius on $E_1[\ell^*]$ and $E_2[\ell^*]$ are both equal to $x^2 - tx + q \in \mathbb{F}_\ell[x]$. It follows easily that there are points $P_1 \in E_1[\ell](\overline{\mathbb{F}}_q)$ and $P_2 \in E_2[\ell](\overline{\mathbb{F}}_q)$ that generate the Galois modules $E_1[\ell](\overline{\mathbb{F}}_q)$ and $E_2[\ell](\overline{\mathbb{F}}_q)$, respectively.

We claim that the k-group schemes $E_1[\ell]$ and $E_2[\ell]$ are isomorphic. If $p \neq \ell^*$ then we can see this by defining an isomorphism $E_1[\ell] \to E_2[\ell]$ by sending P_1 to P_2 and extending by Galois equivariance. If $p = \ell^*$, then $E_1[\ell]$ and $E_2[\ell]$ are both products of a reduced group scheme of rank ℓ and a local group scheme of rank ℓ. On each of the reduced group schemes, the Frobenius acts as multiplication-by-t, so the reduced subschemes of $E_1[\ell]$ and $E_2[\ell]$ are isomorphic. But the local subschemes are the duals of the reduced subschemes, so the local subschemes are isomorphic as well. Thus $E_1[\ell]$ and $E_2[\ell]$ are isomorphic.

Let $\psi\colon E_1[\ell] \to E_2[\ell]$ be an isomorphism of group schemes over $\mathbb{F}_q$. For each $i = 1, 2$ let e_i be the Weil pairing $E_i[\ell] \times E_i[\ell] \to \mu_\ell$. Then there is an element r of $\operatorname{Aut}\mu_\ell \cong (\mathbb{Z}/\ell\mathbb{Z})^*$ such that the diagram commutes:

$$\begin{tikzcd} E_1[\ell] \times E_1[\ell] \arrow[r, "(\psi,\psi)"] \arrow[d, "e_1"] & E_2[\ell] \times E_2[\ell] \arrow[d, "e_2"] \\ \mu_\ell \arrow[r, "r"] & \mu_\ell \end{tikzcd}$$

Let F be an elliptic curve isogenous to E_1, and suppose $\varphi\colon F \to E_1$ is an isogeny of degree coprime to ℓ. If we replace E_1 by F and ψ by $\psi \circ \varphi$, then r is replaced with r times the degree of φ. Using multiplication by integers in $\mathrm{End}(E_1)$, we can modify r in this way by arbitrary squares in $(\mathbb{Z}/\ell\mathbb{Z})^*$. Using the isogeny $E_1' \to E_1$, we can modify r by the integer m, which is a nonsquare modulo ℓ when $\ell \neq 2$. Therefore we can modify r so that it is equal to -1; in other words, we can find an anti-isometry that maps either $E_1[\ell]$ or $E_1'[\ell]$ to $E_2[\ell]$. □

The next lemma is a useful special case of Lemma 4.3.

Lemma 4.4. — *Let E_1 and E_2 be elliptic curves over a finite field $\mathbb{F}_q$ and let s and t be their traces of Frobenius. Suppose that $|s-t|$ is neither 0 not 1 and that neither s^2 nor t^2 is equal to $4q$. Write $s^2 - 4q = f_1^2\Delta_1$ and $t^2 - 4q = f_2^2\Delta_2$ for integers f_i and fundamental discriminants Δ_i. Let ℓ be a divisor of $s-t$ that is either 4 or a prime, and assume that ℓ is coprime to q if either E_1 or E_2 is supersingular. Suppose that Δ_1 and Δ_2 are not both equal to $-\ell$. Then there are elliptic curves F_1 and F_2, isogenous to E_1 and E_2, respectively, for which there is an $\mathbb{F}_q$-defined anti-isometry $F_1[\ell] \to F_2[\ell]$.*

Proof. — By symmetry, we may assume that $\Delta_1 \neq -\ell$.

Replace E_1 and E_2 with isogenous curves that are minimal at ℓ^*. If $\ell = 2$ then Lemma 4.3 shows that there is an anti-isometry $E_1[\ell] \to E_2[\ell]$, so we may assume that $\ell > 2$.

Let m be a prime number. If m splits in $\mathrm{End}(E_1) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{\Delta_1})$ then there is a degree-m isogeny from E_1 to some other elliptic curve F. (Indeed, Ito [18] proves that there is a degree-m isogeny from E_1 to some F if and only if either m splits or ramifies in $\mathrm{End}(E_1) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{\Delta_1})$ or m divides f_1.) Lemma 4.2 says that there are infinitely many m that are nonsquares modulo ℓ and that split in $\mathrm{End}(E_1)\otimes\mathbb{Q}$, so we know there is an elliptic curve E_1' that is m-isogenous to E_1 for some m that is not a square modulo ℓ. Using Lemma 4.3, we see that there is either an anti-isometry $E_1[\ell] \to E_2[\ell]$ or an anti-isometry $E_1'[\ell] \to E_2[\ell]$, and we are done. □

We end with a lemma that will help us show that certain anti-isometries are not reducible.

Lemma 4.5. — *Suppose E and F are ordinary elliptic curves over a finite field k, let F'/k be a twist of F, and let $\chi\colon F' \to F$ be a geometric isomorphism. Suppose that E and F' are isogenous over k. Let ℓ be a prime, and suppose $\psi\colon E[\ell] \to F[\ell]$ is a Galois-equivariant anti-isometry. If ψ is reducible, then $\chi|_{F'[\ell]}$ is Galois equivariant.*

Proof. — Suppose ψ is reducible. Then Theorem 3.1 shows that there is an integer i and a geometric isogeny $\varphi\colon E \to F$ of degree $i(n-i)$ such that $i\psi = \varphi|_{E[\ell]}$. The left-hand side of this equality is Galois equivariant, so $\varphi|_{E[\ell]}$ is Galois equivariant.

Every geometric isogeny $E \to F$ can be written as the composition of a geometric isogeny $E \to F'$ with the geometric isomorphism $\chi\colon F' \to F$, so we may write $\varphi = \chi \circ \varphi'$ for a geometric isogeny $\varphi'\colon E \to F'$. Since E and F' are ordinary, all of their endomorphisms are defined over k, and all isogenies from E to F' are defined over k. It follows that φ' is Galois equivariant. Also, φ' gives an isomorphism $E[\ell] \to F'[\ell]$, so χ induces a Galois equivariant isomorphism from $F'[\ell]$ to $F[\ell]$. □

5. Proof of Theorem 2.1

Suppose that $|s-t| = 1$. Then a result of Serre (see [21, Lem. 1] or [12, Thm. 1(a)]) shows that there is no Jacobian isogenous to $E_1 \times E_2$.

Suppose that $|s-t| > 1$. The remainder of the proof of Theorem 2.1 breaks into five cases:

(1) E_1 and E_2 are geometrically non-isogenous.
(2) E_1 and E_2 become isogenous to one another over a degree-2 extension.
(3) E_1 and E_2 become isogenous to one another over a degree-3 extension.
(4) E_1 and E_2 become isogenous to one another over a degree-4 extension, but not over a degree-2 extension.
(5) E_1 and E_2 become isogenous to one another over a degree-6 extension, but not over a degree-2 or degree-3 extension.

To see that these cases include all possibilities, we note that if E_1 and E_2 are geometrically isogenous to one another then they must both be ordinary (because the hypotheses of the theorem preclude them from both being supersingular). Let π_1 and π_2 be the Weil numbers of E_1 and E_2, considered as elements of $\overline{\mathbb{Q}}$. If E_1 and E_2 become isogenous over a degree-n extension (and no smaller extension), then π_1^n and π_2^n are conjugate quadratic integers; replacing π_1 with its conjugate, if necessary, we may assume that $\pi_1^n = \pi_2^n$. Then the two quadratic fields $\mathbb{Q}(\pi_1)$ and $\mathbb{Q}(\pi_2)$ are equal, and they contain the primitive n-th root of unity π_1/π_2. This restricts the possible values for n to be 2, 3, 4, and 6.

We will consider these cases separately. In each case, we will denote the characteristic of $\mathbb{F}_q$ by p.

5.1. Case 1: E_1 and E_2 are geometrically non-isogenous

Pick a prime ℓ dividing $s-t$. Since E_1 and E_2 are not both supersingular, ℓ is not equal to p if either curve is supersingular.

Let π_1 and π_2 be the Weil numbers of E_1 and E_2, respectively, and let K_1 and K_2 be the imaginary quadratic fields generated by π_1 and π_2. If one of these fields has discriminant unequal to $-\ell$, then Lemma 4.4 shows that we can replace E_1 and E_2 with isogenous curves for which there is an $\mathbb{F}_q$-defined anti-isometry $E_1[\ell] \to E_2[\ell]$. Since E_1 and E_2 are geometrically non-isogenous by assumption, Theorem 3.1 shows that we can tie E_1 and E_2 together along their ℓ-torsion to get a genus-2 curve with Jacobian isogenous to $E_1 \times E_2$.

We are left to consider the case where K_1 and K_2 are both isomorphic to the imaginary quadratic field K of discriminant $-\ell$. In this case, we may view π_1 and π_2 as elements of K.

If E_1 and E_2 are both ordinary, then their Weil numbers must differ from one another by a root of unity (and perhaps complex conjugation). But then E_1 and E_2 become isogenous to one another after a base field extension, contradicting our hypotheses.

So suppose one of our elliptic curves, say E_1, is supersingular and the other is ordinary. We have already noted that in this case $\ell \neq p$. Now, we know the possible Weil numbers for supersingular elliptic curves — see [32] or [37, Thm. 4.2] for example — and the only way a supersingular Weil number can generate an imaginary quadratic field of prime discriminant unequal to $-p$ is if that field is $\mathbb{Q}(\sqrt{-3})$ and if $p \not\equiv 1 \bmod 3$. But then p does not split in $\mathbb{Q}(\sqrt{-3})$, so there are no ordinary elliptic curves over $\mathbb{F}_q$ with CM by $\mathbb{Q}(\sqrt{-3})$, contradicting the existence of E_2.

5.2. Case 2: E_1 and E_2 become isogenous to one another over a degree-2 extension

In this case, there is an integer t such that the Weil polynomials of E_1 and E_2 are x^2-tx+q and x^2+tx+q. Also, E_1 and E_2 are both ordinary. Let $\Delta = t^2 - 4q$ and let R be the imaginary quadratic order of discriminant Δ.

We have two arguments that each cover many cases, and that together cover all but one case.

LEMMA 5.1. — *If the class number of R is greater than* 1, *there is a Jacobian isogenous to $E_1 \times E_2$.*

Proof. — If the class number of R is greater than 1, we can choose E_1 and E_2 to have endomorphism ring R, and to be geometrically non-isomorphic. Then E_1 and E_2 are minimal at 2, so Lemma 4.3 shows that there is an anti-isometry $\psi\colon E_1[2] \to E_2[2]$. Theorem 3.1 shows that ψ is not reducible because there are no geometric isomorphisms $E_1 \to E_2$. Thus we can tie E_1 and E_2 together along their 2-torsion to get a Jacobian isogenous to $E_1 \times E_2$. □

LEMMA 5.2. — *If $|t| > 1$ then there is a Jacobian isogenous to $E_1 \times E_2$.*

Proof. — Let ℓ be a prime divisor of t.

First suppose that ℓ is odd. Note that ℓ is not equal to p, because ℓ divides t and E_1 and E_2 are not both supersingular. It follows that ℓ does not divide $\Delta = t^2 - 4q$. Then Lemma 4.4 shows that we can replace E_1 and E_2 with isogenous curves for which there is an $\mathbb{F}_q$-defined anti-isometry $\psi\colon E_1[\ell] \to E_2[\ell]$. Let E_2' be the quadratic twist of E_2 and let $\chi\colon E_2' \to E_2$ be the standard geometric isomorphism. Then Lemma 4.5 shows that if ψ is reducible, then χ induces a Galois-equivariant isomorphism from $E_2'[\ell]$ to $E_2[\ell]$. But from the definition of the quadratic twist, we know that $\chi(P^\sigma) = -(\chi(P))^\sigma$ for all geometric points P, where σ denotes the q-th power Frobenius automorphism of $\overline{\mathbb{F}}_q$. From this it is clear that χ does *not* give a Galois-equivariant isomorphism $E_2'[\ell] \to E_2[\ell]$, because $\ell > 2$. Thus ψ is not reducible, and we can tie E_1 and E_2 together along their ℓ-torsion via ψ to get a Jacobian isogenous to $E_1 \times E_2$.

Next suppose $\ell = 2$. Lemma 4.4 shows that we can replace E_1 and E_2 with isogenous curves for which there is an anti-isometry $\psi\colon E_1[4] \to E_2[4]$. According to Lemma 4.5, there are two ways in which ψ might be reducible. In the first way, there is a geometric isogeny $\varphi\colon E_1 \to E_2$ of degree 3 such that $\varphi|_{E_1[\ell]} = \pm\psi$. But as in the argument for odd ℓ, we obtain a contradiction from the facts that $\pm\psi$ is Galois equivariant while $\varphi|_{E_1[\ell]}$ is not.

The other way that ψ can be reducible is if there is a geometric isomorphism $\varphi\colon E_1 \to E_2$ and two order-2 subgroups G_1 and G_2 of $E_1(\overline{\mathbb{F}}_q)$ such that the graph of ψ is equal to the set of $(x, \varphi(y))$ in $E_1[4](\overline{\mathbb{F}}_q) \times E_2[4](\overline{\mathbb{F}}_q)$ such that $x + y \in G_1$ and $x - y \in G_2$.

In particular, if E_2 is not the quadratic twist of E_1 then ψ is not reducible. Suppose E_2 is the quadratic twist of E_1 and that ψ is reducible.

Identify $E_2[4]$ with $E_1[4]$ provided with the negative Galois action. Pick 4-torsion points X and Y of $E_1(\overline{\mathbb{F}}_q)$ such that $G_1 = \langle 2X \rangle$ and $G_2 = \langle 2Y \rangle$. Then $\psi(aX + bY) = \varphi(aX - bY)$ for some automorphism φ of E_2. Since E_2 is ordinary, all of its automorphisms are defined over $\mathbb{F}_q$, so ψ is Galois equivariant if and only if $\varphi^{-1} \circ \psi$ is Galois equivariant, and one can show that this is the case if and only if $2X^\sigma = 2Y$ and $2Y^\sigma = 2X$; here σ denotes the Frobenius element of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

So assume that $2X^\sigma = 2Y$ and $2Y^\sigma = 2X$. Under this assumption, we can compute the number of reducible Galois equivariant anti-isometries. The only choices for G_1 and G_2 are $G_1 = \langle 2X \rangle$, $G_2 = \langle 2Y \rangle$ and $G_1 = \langle 2Y \rangle$, $G_2 = \langle 2X \rangle$, and swapping G_1 and G_2 is equivalent to replacing φ with $-\varphi$. Thus we see that the automorphism group of E_2 acts transitively on the set of reducible Galois-equivariant anti-isometries.

Let us compute the number of Galois equivariant anti-isometries there are from $E_1[4]$ to $E_2[4]$. To make the computation simpler, we replace Y with X^σ (this does not change the group G_2), and write $Y^\sigma = \varepsilon X + fY$, where $\varepsilon = \pm 1$ and $f \in \{0, 2\}$. Note that it follows that the characteristic polynomial of Frobenius on the 4-torsion of E_1 is $x^2 + fx - \varepsilon$. Since the Weil polynomial of E_1 is $x^2 - tx + q$, we see that $\varepsilon \equiv -q \bmod 4$ and $f \equiv t \bmod 4$.

A Galois-equivariant map $\chi\colon E_1[4] \to E_2[4]$ that sends X to $aX + bY$ must send Y to $bqX - (a + tb)Y$, and χ will be an anti-isometry if and only if $a^2 + tab + qb^2 \equiv 1 \bmod 4$. There are four pairs (a, b) of elements of $(\mathbb{Z}/4\mathbb{Z})$ that satisfy this condition if $q \equiv -1 \bmod 4$ and eight if $q \equiv 1 \bmod 4$, so there are either exactly 4 or exactly 8 Galois-equivariant anti-isometries.

If $\#\,\mathrm{Aut}\, E_2 = 2$ then we have only 2 reducible Galois-equivariant anti-isometries, so there are at least two nonreducible ones. If $\#\,\mathrm{Aut}\, E_2 = 6$ then either there are 8 Galois-equivariant anti-isometries in total and we can choose a nonreducible one, or else there are only 4 Galois-equivariant anti-isometries, in which case $\mathrm{Aut}\, E_2$ cannot act faithfully on the reducible Galois-equivariant anti-isometries; but since the automorphism -1 doesn't act trivially, the kernel of the action must be of order 3, and once again we see that there are only two reducible Galois-equivariant anti-isometries.

If $\#\,\mathrm{Aut}\, E_2 = 4$ then $\Delta = t^2 - 4q = -4$, and the Frobenius can be written $\pi = (t/2) + i$. Note that therefore $q \equiv 1 \bmod 4$. We noted above that in this case there are eight Galois-equivariant anti-isometries, so we have four nonreducible ones to choose from. □

The only situations not covered by Lemmas 5.1 and 5.2 are those in which $t = 1$ and in which Δ lies in the set

$$\{-3, -12, -27, -4, -16, -7, -28, -8, -11, -19, -43, -67, -163\}.$$

That means the only cases left to consider are those in which (q, Δ) is one of

$$\{(2,-7),(3,-11),(5,-19),(7,-27),(11,-43),(17,-67),(41,-163)\}.$$

Suppose q is odd. Then characteristic polynomial of Frobenius is congruent to x^2+x+1 modulo 2. In this case there are three Galois-equivariant anti-isometries from $E_1[2]$ to $E_2[2]$. If they are all reducible then we must have $\#\operatorname{Aut} E_1 = 6$, so that $\Delta = -3$. But this is not one of the Δ's on our list of (q, Δ) pairs.

Finally we are left with $t = 1$ and $q = 2$. We find, by explicitly enumerating the genus-2 curves over $\mathbb{F}_2$, that none of them has Weil polynomial $(x^2+x+2)(x^2-x+2)$.

5.3. Case 3: E_1 and E_2 become isogenous to one another over a degree-3 extension

In this case the Weil numbers of E_1 and E_2 must both live in $\mathbb{Q}(\omega)$, where $\omega^2+\omega+1=0$, and they can be chosen so that they differ multiplicatively by ω. So let us write

$$\begin{aligned}\pi_1 &= a + b\overline{\omega}\\ \pi_2 &= \omega\pi_1 = b + a\omega.\end{aligned}$$

Note that

$$\begin{aligned}q &= \pi_1\overline{\pi_1} = a^2 - ab + b^2\\ s &= 2a - b\\ t &= 2b - a\\ \Delta_1 &= -3b^2\\ \Delta_2 &= -3a^2\\ s - t &= 3(a-b).\end{aligned}$$

We observe several facts. First, we see that Δ_1 and Δ_2 cannot be equal; if they were equal, then we would have $b = -a$, and 3 would divide both s and q, contradicting the ordinariness of E_1. Second, we note that the same reasoning shows that a and b are coprime to each other. Third, we see that q is congruent to 1 modulo 3, and in particular, the characteristic of $\mathbb{F}_q$ is not 3. And fourth, we see that q is odd, so the characteristic of $\mathbb{F}_q$ is not 2.

Suppose a and b are both odd, so that 2 divides $s-t$. Replace E_1 and E_2 with isogenous curves whose endomorphism rings have discriminants

Δ_1 and Δ_2, respectively, so that in particular E_1 and E_2 are geometrically non-isomorphic. Then there is an anti-isometry $\psi\colon E_1[2] \to E_2[2]$, and since E_1 and E_2 are geometrically non-isomorphic, Theorem 3.1 shows that ψ is not reducible. Thus we may tie E_1 and E_2 together along their 2-torsion to get a genus-2 curve.

We are left to consider the case in which one of a and b is even. By symmetry, we may assume that b is even.

Suppose that a is not a multiple of 3. Replace E_2 with an isogenous curve that has complex multiplication by $\mathbb{Z}[\omega]$. Since a is not a multiple of 3, we see that E_2 is minimal at 3. The proof of Lemma 4.4 shows that we can replace E_1 by an isogenous curve so that there is an anti-isometry $\psi\colon E_1[3] \to E_2[3]$.

Let F be the cubic twist of E_2 that is isogenous to E_1, and let $\chi\colon F \to E_2$ be a geometric isomorphism. Lemma 4.5 shows that if ψ is reducible, then χ induces an isomorphism from $F[3]$ to $E_2[3]$ as group schemes over $\mathbb{F}_q$.

We know that E_2 can be written in the form $y^2 = x^3 + e$ for some $e \in \mathbb{F}_q$, and the twist F of E_2 can be written $y^2 = cx^3 + e$ for some $c \in \mathbb{F}_q$ that is not a cube. Then the geometric isomorphism χ can be taken to be $(x, y) \mapsto (dx, y)$, where $d \in \overline{\mathbb{F}}_q$ satisfies $d^3 = c$. But then it is clear that χ will not induce a Galois-equivariant isomorphism $F[3] \to E_2[3]$ if $F[3]$ contains an element with nonzero x-coördinate. Since $F[3]$ clearly contains such an element, ψ must not be reducible, so we can tie E_1 and E_2 together along their 3-torsion.

Finally, suppose that a is divisible by 3. Replace E_2 with an isogenous elliptic curve whose endomorphism ring has discriminant Δ_2, and replace E_1 with an isogenous elliptic curve with complex multiplication by $\mathbb{Z}[\omega]$. Since b is even, there is a 2-isogeny from E_1 to an elliptic curve whose endomorphism ring is $\mathbb{Z}[\sqrt{-3}]$. Lemma 4.3 shows that there is an anti-isometry ψ from either $E_1[3]$ or $E_1'[3]$ to $E_2[3]$. Theorem 3.1 shows that if this isometry is reducible, there must be a geometric 2-isogeny from E_1 or E_1' to E_2. But by looking at the discriminants of the endomorphism rings of these curves, we see that every isogeny from E_1 or E_1' to E_2 must have degree divisible by 3. Thus ψ is not reducible, so we may use it to produce a genus-2 curve whose Jacobian is isogenous to $E_1 \times E_2$.

5.4. Case 4: E_1 and E_2 become isogenous to one another over a degree-4 extension, but not over a degree-2 extension

In this case the Weil numbers of E_1 and E_2 must live in $\mathbb{Q}(i)$, where $i^2 = -1$, and they may be chosen so that they differ multiplicatively by i.

So let us write

$$\pi_1 = a + bi$$
$$\pi_2 = -b + ai$$

so that we have

$$\begin{aligned} q &= a^2 + b^2 \\ s &= 2a \\ t &= -2b \\ \Delta_1 &= -4b^2 \\ \Delta_2 &= -4a^2. \end{aligned}$$

If b were equal to $\pm a$ then q and s would both be even, contradicting our assumption that E_1 is ordinary. Therefore Δ_1 and Δ_2 are not equal to one another, so if we pick E_1 and E_2 with minimal endomorphism rings, they will be geometrically non-isomorphic. Since $s - t$ is even, we can tie E_1 and E_2 together along their 2-torsion.

5.5. Case 5: E_1 and E_2 become isogenous to one another over a degree-6 extension, but not over a degree-2 or degree-3 extension

In this case the two Weil numbers must live in $\mathbb{Q}(\omega)$, where $\omega^2+\omega+1 = 0$, and they can be chosen to differ multiplicatively by a primitive sixth root of unity, such as $-\omega$. So let us write

$$\begin{aligned} \pi_1 &= a + b\overline{\omega} \\ \pi_2 &= -\omega\pi_1 = -b - a\omega \end{aligned}$$

so that we have

$$\begin{aligned} q &= \pi_1\overline{\pi_1} = a^2 - ab + b^2 \\ s &= 2a - b \\ t &= a - 2b \\ \Delta_1 &= -3b^2 \\ \Delta_2 &= -3a^2 \\ s - t &= a + b. \end{aligned}$$

As in Case 3, we see that $\Delta_1 \neq \Delta_2$, that $(a,b) = 1$, and that the characteristic of $\mathbb{F}_q$ is not 2. Since $(a,b) = 1$, at least one of a and b is odd; by symmetry, we may assume that a is odd. Let ℓ be the smallest prime divisor of $s - t = a + b$. Note that neither a nor b can be divisible by ℓ, so both E_1 and E_2 are automatically minimal at ℓ.

Let us replace E_2 with an isogenous curve that has complex multiplication by $\mathbb{Z}[\omega]$. We will show that we can replace E_1 with an isogenous curve for which there is an anti-isometry $E_1[\ell] \to E_2[\ell]$.

First suppose that $\ell \neq 3$. Since E_1 has complex multiplication by an order in $\mathbb{Q}(\omega)$ and since $\ell \neq 3$, we know from Lemma 4.2 that there is a prime $m \equiv 2 \bmod 3$ for which there is an elliptic curve E_1' that is m-isogenous to E_1. Applying Lemma 4.3, we find that there is an anti-isometry from either $E_1[\ell]$ or $E_1'[\ell]$ to $E_2[\ell]$.

On the other hand, suppose that $\ell = 3$. Since ℓ was chosen to be the smallest prime divisor of $s - t = a + b$, we know that $a + b$ is odd; since a is odd, we know that b is even. It follows that E_1 is 2-isogenous to some other curve E_1'; applying Lemma 4.3, we find that there is an anti-isometry from either $E_1[\ell]$ or $E_1'[\ell]$ to $E_2[\ell]$.

Let F be the sextic twist of E_2 that is isogenous to E_1, and let $\chi\colon F \to E_2$ be a geometric isomorphism. Lemma 4.5 shows that if ψ is reducible, then χ induces an isomorphism from $F[\ell]$ to $E_2[\ell]$ as group schemes over $\mathbb{F}_q$.

We know that E_2 can be written in the form $y^2 = x^3 + e$ for some $e \in \mathbb{F}_q$, and the twist F of E_2 can be written $cy^2 = dx^3 + e$ for some $c \in \mathbb{F}_q$ that is not a square and some $d \in \mathbb{F}_q$ that is not a cube. Then the geometric isomorphism χ can be taken to be $(x,y) \mapsto (gx, fy)$, where $f, g \in \overline{\mathbb{F}}_q$ satisfy $g^3 = d$ and $f^2 = c$. But then it is clear that χ will not induce a Galois-equivariant isomorphism $F[\ell] \to E_2[\ell]$. Therefore, we can tie E_1 and E_2 together along their ℓ-torsion.

This completes the proof of Theorem 2.1. □

6. Proof of Theorem 2.2

Let $d = t - s$, and suppose d is squarefree. Then the proof of Corollary 12 of [12, p. 1689] shows that there is no Jacobian isogenous to $E_1 \times E_2$.

On the other hand, suppose there is a prime ℓ whose square divides d. The Frobenius π_1 on E_1 is equal to an integer r with $r^2 = q$. Let π_2 be the Frobenius on E_2, and let z be the element $(\pi_2 - r)/\ell$ of $\mathrm{End}(E_2) \otimes \mathbb{Q}$. Then we have

$$z^2 - (d/\ell)z - rd/\ell^2 = 0,$$

so z is integral. If we replace E_2 with an isogenous curve whose endomorphism ring is maximal, then $z \in \mathrm{End}(E_2)$ so that π_2 acts as r on $E_2[\ell]$. Therefore there are Galois-equivariant anti-isometries from $E_1[\ell]$ to $E_2[\ell]$. All of them give rise to Jacobians isogenous to $E_1 \times E_2$, because E_1 and E_2 are geometrically non-isogenous. □

7. Proof of Theorem 2.3

Let $\Delta = t^2 - 4q$ and let R be the quadratic order of discriminant Δ. Using Serre's appendix to [22] or the main results of [7], we see that if Δ is a fundamental discriminant, then there is a bijection between the set of Jacobians isogenous to $E \times E$ and the set of indecomposable unimodular hermitian lattices of rank 2 over R. Hoffmann [6] shows that if Δ is -3, -4, or -7, then there are no such indecomposable unimodular hermitian lattices, so for these values of Δ there are no Jacobians isogenous to $E \times E$.

Suppose Δ is neither -3 nor -4 nor -7, and suppose q is odd. Then there is an E' isogenous to E whose automorphism group has order 2, and Corollary 6 of [13] explicitly constructs a genus-2 curve whose Jacobian is isogenous to $E' \times E'$.

Suppose Δ is neither -3 nor -4 nor -7, and suppose q is a power of 2. Then $\Delta \equiv 1 \bmod 8$, so Δ is not the discriminant of an imaginary quadratic order of class number one (all such discriminants other than -7 are either even or are 5 modulo 8). Therefore there is an elliptic curve E' that is isogenous to E but that is geometrically non-isomorphic to E. The group schemes $E[2]$ and $E'[2]$ are both isomorphic to the product of μ_2 with its dual, so there is an anti-isometry $E[2] \to E'[2]$. Since E and E' are geometrically non-isogenous, this anti-isometry gives rise via Theorem 3.1 to a Jacobian isogenous to $E \times E'$. □

Remark 7.1. — It is also possible to prove the existence of a Jacobian isogenous to E^2 in the case where $t^2 - 4q \notin \{-3, -4, -7\}$ directly from the results of Hoffmann, Serre, and the first author that we cited above, but some care must be taken in the case where Δ is not a fundamental discriminant.

8. Twists of Dieudonné modules of supersingular elliptic curves

Let q be an even power of a prime p, say $q = p^{2a}$. Our goal in this section is to prove the following result.

Proposition 8.1. — *Suppose $p > 3$. If E and E' are supersingular elliptic curves over $\mathbb{F}_q$ that are not isogenous to one another over $\mathbb{F}_q$, then the group schemes $E[p]$ and $E'[p]$ are not isomorphic to one another over $\mathbb{F}_q$.*

We will prove this proposition by showing that the Dieudonné modules of $E[p]$ and $E'[p]$ are not isomorphic to one another. For concise background information on Dieudonné modules and p-divisible groups, see [37, Ch. 1] or [28, §3]. The first step in our proof of Proposition 8.1 will be to compute the twists of the Dieudonné module of a particular supersingular curve.

Let E be a supersingular elliptic curve over $\mathbb{F}_q$ whose Weil polynomial is $(x - \sqrt{q})^2$. As noted at the end of §1, we use $\mathbb{Q}_q$ to denote the unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$ and $\mathbb{Z}_q$ to denote the ring of integers of $\mathbb{Q}_q$. Let σ be the automorphism of $\mathbb{Z}_q$ over $\mathbb{Z}_p$ that is the lift of the Frobenius automorphism of $\mathbb{F}_q$ over $\mathbb{F}_p$, and let $\mathfrak{A}$ be the (non-commutative) ring $\mathbb{Z}_q[F, V]$, where F and V are indeterminates that satisfy

$$FV = VF = p, \quad F\lambda = \lambda^\sigma F, \quad \text{and} \quad V\lambda^\sigma = \lambda V.$$

Recall that the Dieudonné module M associated to E (or more precisely, to the p-divisible group of E) is a certain left $\mathfrak{A}$-module. Waterhouse [37, p. 539] computes that M is a free rank-2 $\mathbb{Z}_q$-module with a basis $\{x, y\}$ such that

$$Fx = Vx = y \qquad \text{and} \qquad Fy = Vy = px.$$

In particular, we see that all elliptic curves in the isogeny class with Weil polynomial $(x - \sqrt{q})^2$ have isomorphic Dieudonné modules. Waterhouse also notes that the endomorphism ring of M is isomorphic to the ring of integers $\mathcal{O}$ of the unique quaternion algebra $\mathbb{H}_p$ over $\mathbb{Q}_p$, and it follows from Waterhouse's analysis that M gains no further endomorphisms when the base field is extended to $\overline{\mathbb{F}}_q$.

For every (p^2-1)st root of unity ζ in $\mathbb{Q}_{p^2}$ we define a Dieudonné module M_ζ as follows: Let $\xi \in \mathbb{Q}_q$ be a $(p^{2a} - 1)$st root of unity whose norm to $\mathbb{Q}_{p^2}$ is equal to ζ. Let M_ζ be a free rank-2 $\mathbb{Z}_q$-module generated by two elements w and z, and let F and V act on w and z via

$$Fw = z, Fz = \xi^{-1}pw \qquad \text{and} \qquad Vw = \xi^{\sigma^{-1}}z, Vz = pw.$$

One can check that this does give a well-defined $\mathfrak{A}$-module structure to M_ζ, and that the isomorphism class of M_ζ does not depend on the choice of ξ.

Proposition 8.2. — *The Dieudonné modules M_ζ over $\mathbb{F}_q$ are pairwise nonisomorphic over $\mathbb{F}_q$, and they are all twists of M over $\overline{\mathbb{F}}_q$. The module M_ζ is the twist of M by the automorphism ζ of M. If $p > 3$, then every $\overline{\mathbb{F}}_q$-twist of M is isomorphic to one of the M_ζ.*

Proof. — Let t be an arbitrary element of M_ζ such that $Ft \notin pM_\zeta$, and write $t = aw + bz$ for some $a, b \in \mathbb{Z}_q$. We see that a must be a unit of $\mathbb{Z}_q$. We compute that

$$Ft = a^\sigma z + b^\sigma \xi^{-1} pw$$
$$Vt = a^{\sigma^{-1}} \xi^{\sigma^{-1}} z + b^{\sigma^{-1}} pw.$$

It follows that for every $c \in \mathbb{Z}_q$ with $Ft \equiv cVt \bmod pM_\zeta$, we have

$$c \equiv (a^\sigma / a^{\sigma^{-1}}) \xi^{-\sigma^{-1}} \bmod p\mathbb{Z}_q.$$

Taking norms to $\mathbb{Q}_{p^2}$, we find that

$$N_{\mathbb{Q}_q/\mathbb{Q}_{p^2}}(c) \equiv 1 \cdot N_{\mathbb{Q}_q/\mathbb{Q}_{p^2}}(\xi^{-\sigma^{-1}}) \equiv \zeta^{-\sigma} \bmod p.$$

Thus, we can recover ζ from M_ζ, so the M_ζ are pairwise nonisomorphic.

Let B be the ring of integers of the maximal unramified extension of $\mathbb{Q}_q$ and let $\mathfrak{B} = B[F, V]$, where F and V satisfy the same properties as before. The base extensions of the M_ζ to $\overline{\mathbb{F}}_q$ are the $\mathfrak{B}$-modules $\overline{M}_\zeta$ generated as B-modules by w and z and with

$$Fw = z, \quad Fz = \xi^{-1} pw \quad \text{and} \quad Vw = \xi^{\sigma^{-1}} z, \quad Vz = pw.$$

Let $\alpha \in B^*$ satisfy $\alpha^{\sigma^2 - 1} = \xi$. Then one can check that the map of $\mathfrak{B}$-modules that sends x to αw and y to $\alpha^\sigma z$ gives an isomorphism φ from $\overline{M}$ to $\overline{M}_\zeta$.

The Frobenius automorphism of $\overline{\mathbb{F}}_q$ over $\mathbb{F}_q$ acts on $\operatorname{Hom}(\overline{M}, \overline{M}_\zeta)$, and we let $\varphi^{(q)}$ denote the image of φ under this action. We see that the automorphism $\varphi^{-1}\varphi^{(q)}$ of $\overline{M}$ is the map that sends x to $\alpha^{\sigma^{2a}-1} x$. Since $\xi = \alpha^{\sigma^2 - 1}$, we have

$$\alpha^{\sigma^{2a}-1} = \xi^{1 + \sigma^2 + \cdots + \sigma^{2a-2}} = \operatorname{Norm}_{\mathbb{Q}_q/\mathbb{Q}_{p^2}}(\xi) = \zeta.$$

Thus, M_ζ is the twist of M by ζ.

The general theory of twists [33] shows that the $\overline{\mathbb{F}}_q/\mathbb{F}_q$-twists of M correspond to the elements of the pointed cohomology set $H^1(\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), \mathcal{O}^*)$. Since the Galois group acts trivially on $\mathcal{O}^*$, this cohomology set consists of the conjugacy classes of $\mathcal{O}^*$ whose elements have finite order.

Fix an embedding of $\mathbb{Q}_{p^2}$ into $\mathbb{H}_p$. We know (see [30, Thm. 14.5]) that there is an element $s \in \mathbb{H}_p$ with the properties that $s^2 = p$ and $\mathbb{H}_p = \mathbb{Q}_{p^2}(s)$, and such that $s^{-1} x s = x^\sigma$ for all $x \in \mathbb{Q}_{p^2}$. Suppose that $p > 3$, and suppose that η is a root of unity in $\mathcal{O}$. Then $\mathbb{Q}_p(\eta)$ is at most a quadratic extension of $\mathbb{Q}_p$, and since cyclotomic extension of $\mathbb{Q}_p$ have ramification index at least $p - 1$ if they are ramified at all, it follows that $\mathbb{Q}_p(\eta)$ is an unramified extension of $\mathbb{Q}_p$. Thus there is a root of unity ζ in $\mathbb{Q}_{p^2}$ of the same order as η, and the Skolem-Noether theorem tells us that there is an element x

of $\mathbb{H}_p$ that conjugates η to ζ. Let t be the unique power of s such that $tx \in \mathcal{O}^*$, and let $y = tx$. Then y conjugates η to either ζ or ζ^σ. Thus, the elements of $H^1(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), \mathcal{O}^*)$ are represented by the conjugacy classes that contain roots of unity in $\mathbb{Q}_{p^2}$. On the other hand, it is easy to see that no element of $\mathcal{O}^*$ conjugates one root of unity in $\mathbb{Q}_{p^2}^*$ to another. It follows that when $p > 3$ there is a bijection between $H^1(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), \mathcal{O}^*)$ and the roots of unity in $\mathbb{Q}_{p^2}$. Since the M_ζ are the twists of M associated to these roots of unity, we find that every twist of M is isomorphic to some M_ζ. □

Remark 8.3. — It is not hard to show that when $p = 2$ there are seven conjugacy classes of roots of unity in $\mathcal{O}^*$: in addition to the six conjugacy classes obtained from the roots of unity in $\mathbb{Q}_4$, there is also a single conjugacy class containing a primitive fourth root of unity. Likewise, when $p = 3$ there are ten conjugacy classes of roots of unity in $\mathcal{O}^*$: eight classes obtained from the roots of unity in $\mathbb{Q}_9$, one class containing a primitive cube root of unity, and one class containing a primitive sixth root of unity.

Proof of Proposition 8.1. — Let $s = p^a$ be the positive square root of q. There are at most 5 isogeny classes of supersingular elliptic curves over $\mathbb{F}_q$. There are always isogeny classes with Weil polynomials $(x - s)^2$ and $(x+s)^2$. If $p \equiv 2 \bmod 3$, then there are isogeny classes with Weil polynomial $x^2 + sx + q$ and $x^2 - sx + q$; each of these isogeny classes contains two elliptic curves, and they are both twists of the elliptic curve $y^2 = x^3 - 1$ (by automorphisms of order 3 for the former isogeny class, and of order 6 for the latter). If $p \equiv 3 \bmod 4$ then there is an isogeny class with Weil polynomial $x^2 + q$; there are two curves in this isogeny classes, each a twist of $y^2 = x^3 - x$ by an automorphism of order 4. (These statements follow from [32, Thm. 4.6] and its proof.)

We already noted that the Dieudonné module of every elliptic curve with Weil polynomial $(x - s)^2$ is isomorphic to the module M defined earlier. It is also clear that every elliptic curve with Weil polynomial $(x + s)^2$ has Dieudonné module M_{-1}. When $p \equiv 2 \bmod 3$, the two curves with Weil polynomial $x^2 + sx + q$ have Dieudonné modules M_ζ for two different cube roots of unity ζ in the endomorphism ring of M, and the curves with Weil polynomial $x^2 - sx + q$ have Dieudonné modules M_ζ for two different sixth roots of unity. When $p \equiv 3 \bmod 4$, the two curves with Weil polynomial $x^2 + q$ have Dieudonné modules isomorphic to M_i and M_{-i}, for a square root i of -1 in the endomorphism ring of M.

Since our elliptic curves E and E' lie in different isogeny classes, their Dieudonné modules are isomorphic to M_ζ and M_η for two distinct roots of unity ζ and η in $\mathbb{Z}_{p^2}$. It follows that the Dieudonné module for $E[p]$ is generated as a $\mathbb{Z}_q$-module by two elements w and z that satisfy

$$Fw = z, \quad Fz = 0 \quad \text{and} \quad Vw = \xi^{1/p} z, \quad Vz = 0$$

for an element ξ of $\mathbb{F}_q$ whose norm to $\mathbb{F}_{p^2}$ is the reduction of ζ modulo p. The same holds for the Dieudonné module for $E'[p]$, with ξ replaced by an element ξ' whose norm to $\mathbb{F}_{p^2}$ is equal to the reduction of η modulo p.

We showed above that ζ could be recovered from the module M_ζ. The same proof shows that ζ modulo p can be recovered from the Dieudonné module of $E[p]$, and that η modulo p can be recovered from the Dieudonné module of $E'[p]$. Thus the two Dieudonné modules are not isomorphic to one another, because the reduction map from roots of unity in $\mathbb{Z}_{p^2}$ to elements of $\mathbb{F}_{p^2}$ is injective. □

Remark 8.4. — Consider one of the isogeny classes mentioned above whose Weil polynomial is neither $(x-s)^2$ nor $(x+s)^2$. It is interesting to note that the two elliptic curves in this isogeny class have non-isomorphic Dieudonné modules. It follows that any isogeny between these two curves must have degree divisible by p. These isogeny classes provide the simplest example of the phenomenon discussed in [37, Thm. 5.3]

9. Proof of Theorem 2.4

First suppose that q is not a square. Because we are assuming that the characteristic of $\mathbb{F}_q$ is at least 5, there is only one isogeny class of supersingular elliptic curves over $\mathbb{F}_q$, and its Weil polynomial is x^2+q. From [32, Thm 4.5] we know that there are $H(-4p)$ curves in the isogeny class (up to isomorphism over $\mathbb{F}_q$), where $H(\Delta)$ is the Kronecker class number of the discriminant Δ. Furthermore, two curves in the isogeny class are geometrically isomorphic to one another if and only if they are twists of one another by -1, so the number of distinct j-invariants in the isogeny class is $H(-4p)/2$. In terms of class number of quadratic orders, we have

$$\frac{H(-4p)}{2} = \begin{cases} h(-4p)/2 & \text{if } p \equiv 1 \bmod 4; \\ h(-p) & \text{if } p \equiv 7 \bmod 8; \\ 2h(-p) & \text{if } p \equiv 3 \bmod 8. \end{cases}$$

From this it follows that when $p \notin \{5, 7, 13, 37\}$ there are two curves E_1, E_2 in the isogeny class with distinct j-invariants. Since $E_1[2]$ and $E_2[2]$ are isomorphic Galois modules and E_1 and E_2 are geometrically non-isomorphic, we can use Theorem 3.1 to tie E_1 and E_2 together along their 2-torsion.

For the remaining cases, we note that if q is an odd power of a prime p for which $(-2/p) = -1$, the curve $y^2 = x^6 - 5x^4 - 5x^2 + 1$ over $\mathbb{F}_q$ has Weil polynomial $(x^2 + q)^2$; this is because over $\mathbb{Q}$ its Jacobian is isogenous to the square of the elliptic curve with $j = 8000$, which has complex multiplication by $\mathbb{Z}[\sqrt{-2}]$. Since the primes 5, 7, 13, and 37 all satisfy $(-2/p) = -1$, we are done.

Now suppose that q is a square, and let p be the unique prime divisor of q. Recall that there are at most five isogeny classes of supersingular curves over $\mathbb{F}_q$; the possible traces of Frobenius are

$$\begin{array}{rl} 0 & \text{if } p \equiv 3 \bmod 4; \\ \pm\sqrt{q} & \text{if } p \equiv 2 \bmod 3; \\ \pm 2\sqrt{q} & \text{for all } q. \end{array}$$

Suppose the traces s and t of our two elliptic curves do *not* satisfy $s^2 = t^2$. Then we are to show that there is no Jacobian isogenous to $E_1 \times E_2$.

We begin with a general observation related to Kani's construction (Theorem 3.1). If E_1 and E_2 are elliptic curves over $\mathbb{F}_q$ with traces s and t, respectively, and if $E_1[n] \cong E_2[n]$ as group schemes over $\mathbb{F}_q$, then we must have $s \equiv t \bmod n$. We know that every Jacobian isogenous to $E_1 \times E_2$ is obtained via Kani's construction for some value of n, and the observation we just made shows that this value of n must divide $s - t$.

Suppose that $|s-t| = \sqrt{q}$. If there were a Jacobian isogenous to $E_1 \times E_2$, it would be attainable through Kani's construction for some value of n that divides $\sqrt{q}$, so that this n must be a power of p. But we know from §8 that $E_1[p] \not\cong E_2[p]$, so there are no Jacobians isogenous to $E_1 \times E_2$ in this case.

Suppose that $|s - t| = 2\sqrt{q}$ and that $s \neq -t$, so that one of s and t is 0 and the other is $\pm 2\sqrt{q}$. Say that $s = 0$ and $t = \pm 2\sqrt{q}$. Note that the endomorphism ring of E_1 is isomorphic to $\mathbb{Z}[i]$, and the Frobenius on E_1 is $i\sqrt{q}$; the Frobenius on E_2 is the integer $\pm\sqrt{q}$. The argument we just gave shows that we cannot obtain a Jacobian by gluing together E_1 and E_2 along their n-torsion when n is a multiple of p, so if there is a Jacobian isogenous to $E_1 \times E_2$ it must be obtained from an anti-isometry $E_1[2] \to E_2[2]$. But the Frobenius of E_2 acts as a constant on $E_2[2]$, while the Frobenius of E_1 does not, so in particular there are no anti-isometries from $E_1[2]$ to $E_2[2]$. Thus there are no Jacobians isogenous to $E_1 \times E_2$.

Suppose that $|s - t| = 3\sqrt{q}$, so that one of s and t is $\pm\sqrt{q}$ and the other is $\mp 2\sqrt{q}$. Say that $s = \pm\sqrt{q}$ and $t = \mp 2\sqrt{q}$. Note that the endomorphism ring of E_1 is isomorphic to $\mathbb{Z}[\omega]$ for some cube root of unity ω, and the Frobenius on E_1 is $\mp\omega\sqrt{q}$; the Frobenius on E_2 is the integer $\mp\sqrt{q}$. Again we see that we cannot obtain a Jacobian by gluing together E_1 and E_2 along their n-torsion when n is a multiple of p, so if there is a Jacobian isogenous to $E_1 \times E_2$ it must be obtained from an anti-isometry $E_1[3] \to E_2[3]$. But the Frobenius of E_2 acts as a constant on $E_2[3]$, while the Frobenius of E_1 does not, so again we see there are no Jacobians isogenous to $E_1 \times E_2$.

Now suppose we have $s^2 = t^2$. We must show that there is a Jacobian isogenous to $E_1 \times E_2$. There are three cases to consider.

The case $s^2 = t^2 = q$.

This case arises only when $p \equiv 2 \bmod 3$. Let a be a generator of $\mathbb{F}_q^*$, and consider the curve C defined by $y^2 = x^6 + a$. Arguing as in [13, §3], we see that the Jacobian of C is isogenous to $F_1 \times F_2$, where F_1 is the elliptic curve $y^2 = x^3 + a$ and F_2 is the elliptic curve $y^2 = x^3 + a^2$. Let F_0 be the elliptic curve $y^2 = x^3 + 1$, let b be a sixth root of a in $\overline{\mathbb{F}}_q$, let ζ be the primitive sixth root of unity b^{q-1}, and let ω be the order-6 automorphism $(x, y) \mapsto (\zeta^2 x, \zeta^3 y)$ of E_0. Since F_0 is defined over $\mathbb{F}_p$, its Frobenius endomorphism over $\mathbb{F}_q$ is either $\sqrt{q}$ or $-\sqrt{q}$. It is easy to see that F_1 is the twist of F_0 by ω and that F_2 is the twist of F_0 by ω^2, and it follows that F_1 and F_2 have traces of opposite sign, and they both are square roots of q.

Similar reasoning shows that the Jacobian of the curve $y^2 = x^6 + a^2$ is isogenous to either $F_1 \times F_1$ or $F_2 \times F_2$; furthermore, whichever product of elliptic curves we get from $y^2 = x^6 + a^2$, we get the other product from the quadratic twist $ay^2 = x^6 + a^2$.

Thus, whenever $s^2 = t^2 = q$ there is a Jacobian isogenous to $E_1 \times E_2$.

The case $s^2 = t^2 = 0$.

This case occurs only when $p \equiv 3 \bmod 4$. Let F_0 be the elliptic curve over $\mathbb{F}_q$ defined by $y^2 = x^3 - x$, so that $j(F_0) = 1728$ and F_0 has an automorphism i of order 4. The two elliptic curves F_1 and F_2 over $\mathbb{F}_q$ with trace 0 are the twists of F_0 by i and by $-i$. Let us fix, once and for all, two $\overline{\mathbb{F}}_q$-isomorphisms $\varphi_1 \colon F_0 \to F_1$ and $\varphi_2 \colon F_0 \to F_2$. Using these isomorphisms, we will identify geometric points of F_1 and F_2 with geometric points of F_0, and we will identify the geometric automorphism groups of F_1 and F_2 with $\operatorname{Aut} F_0$. Let s be the positive square root of q, and reindex the curves if necessary so that the q-power Frobenius on F_1 is equal to si. Then the Frobenius on F_2 is equal to $-si$.

We will show that there is a Jacobian isogenous to $F_1 \times F_2$ by gluing the two curves together along their 4-torsion subgroups, as in Theorem 3.2.

Let P be a geometric point of F_0 such that P and iP generate $F_0[4]$. Let $Q = iP$. Let ψ be the isomorphism $F_1[4] \to F_2[4]$ that sends $\varphi_1(P)$ to $\varphi_2(P + 2Q)$ and $\varphi_1(Q)$ to $\varphi_2(2P - Q)$. It is easy to check that ψ is a Galois-equivariant anti-isometry with respect to the Weil pairing. We will be finished if we can show that neither condition (a) nor condition (b) of Theorem 3.2 holds.

We know that F_1 and F_2 are both elliptic curves with j-invariant 1728. Let $\Phi_3(j, j') \in \mathbb{Z}[j, j']$ be the classical modular polynomial for 3-isogenies. We compute that

$$\Phi_3(1728, 1728) = 2^{36} \cdot 3^6 \cdot 7^8 \cdot 11^4,$$

so when $p > 11$ there are no geometric 3-isogenies from F_1 to F_2, and condition (a) of Theorem 3.2 does not hold. For $p = 7$ and $p = 11$, we can explicitly write down all 3-isogenies from F_0 to F_0 and note that none of them induce the given anti-isometry ψ from $F_1[4]$ to $F_2[4]$.

If condition (b) of Theorem 3.2 were to hold, there would be two order-2 subgroups G_1 and G_2 of $F_0[4]$ and an automorphism α of F_0 such that

$$\begin{aligned} P + \alpha(P + 2Q) &\in G_1 \qquad & P - \alpha(P + 2Q) &\in G_2 \\ Q + \alpha(2P - Q) &\in G_1 \qquad & Q - \alpha(2P - Q) &\in G_2 \end{aligned}$$

Note that the only automorphisms of F_0 are ± 1 and $\pm i$. We check that $P + \alpha(P)$ is a 2-torsion element only when $\alpha = \pm 1$. But if $\alpha = 1$ then we find that G_1 contains both $2P + 2Q$ and $2P$, a contradiction, while if $\alpha = -1$ then G_1 contains both $2Q$ and $2P + 2Q$, another contradiction. Thus, condition (b) of Theorem 3.2 does not hold. It follows that there is a Jacobian with Weil polynomial $(x^2 + q)^2$.

The case $s^2 = t^2 = 2q$.

Note that the Galois group of $\overline{\mathbb{F}}_q/\mathbb{F}_q$ acts trivially on both $E_1[2]$ and $E_2[2]$, because for each curve the Frobenius endomorphism is either $\sqrt{q}$ or $-\sqrt{q}$. There are therefore six Galois-equivariant anti-isometries $E_1[2] \to E_2[2]$. Since we are not in characteristic 2 or 3, the number of isomorphisms $E_1 \to E_2$ is at most 6, and in the case that there are 6 isomorphisms, there are only 3 induced isomorphisms $E_1[2] \to E_2[2]$. Thus, at least one of the six anti-isometries $E_1[2] \to E_2[2]$ is not reducible, so there is a Jacobian isogenous to $E_1 \times E_2$. ∎

(a,b)	Conditions on p	Conditions on q
$(0,0)$	$p \not\equiv 1 \bmod 4$	—
$(0,q)$	$p \not\equiv 1 \bmod 3$	q nonsquare
$(0,-q)$	$p \not\equiv 1 \bmod 3$	—
$(0,-2q)$	—	q nonsquare
$(0,2q)$	$p \equiv 1 \bmod 4$	q square

Table 10.1. Simple supersingular isogeny classes over $\mathbb{F}_q$ that split over $\mathbb{F}_{q^2}$. The characteristic p of $\mathbb{F}_q$ is assumed to be at least 5.

Part 2. Simple supersingular abelian surfaces as Jacobians

10. Introduction

Let $k = \mathbb{F}_q$ be a finite field of characteristic $p > 3$, and let $\mathcal{A}$ be an isogeny class of simple supersingular abelian surfaces over k that split over the quadratic extension of k. In this part of the paper we determine whether or not there is a Jacobian in $\mathcal{A}$.

In [25, Table 1] we find a list of all simple supersingular isogeny classes of abelian surfaces defined over a finite field, with an indication of the smallest field extension over which each class splits. We present in Table 10.1 the isogeny classes over finite fields $\mathbb{F}_q$ of characteristic $p > 3$ that split over $\mathbb{F}_{q^2}$. Theorem 1.4 shows that these classes are all principally polarizable. We will show that all of these isogeny classes contain Jacobians, except for one special case.

Theorem 10.1. — *Let $\mathcal{A}_{(a,b)}$ be an isogeny class of simple supersingular abelian surfaces over a finite field $\mathbb{F}_q$ of characteristic $p > 3$. Then $\mathcal{A}_{(a,b)}$ does not contain a Jacobian if and only if q is a square, $p \equiv 11 \bmod 12$, and $(a,b) = (0,-q)$.*

This part of the paper is organized as follows. In §11 we review results of Oort [29], Katsura and Oort [20], and Ibukiyama, Katsura, and Oort [16] on supersingular abelian surfaces over the algebraic closure of a finite field, paying special attention to the principal polarizations of these surfaces. In §12 we look at supersingular surfaces over finite fields and determine which of their geometric principal polarizations can be defined over the base field. Finally, in §13 we use the results of §11 and §12, together with some explicit constructions, to prove Theorem 10.1.

11. Supersingular surfaces, quaternion lattices, and polarizations

In this section we review some results of Oort [29], Katsura and Oort [20], and Ibukiyama, Katsura, and Oort [16] on supersingular abelian surfaces, quaternion hermitian forms, and polarizations. The results on abelian surfaces assume that the base field is algebraically closed; we will consider the case of finite base fields in §12.

11.1. Supersingular abelian surfaces

Let E be an elliptic curve over $\mathbb{F}_p$ with trace 0, so that E is supersingular and all of the geometric endomorphisms of E are defined over $\mathbb{F}_{p^2}$. Let K be the algebraic closure of $\mathbb{F}_p$ and let $\mathcal{O}$ be the K-endomorphism ring of E; the algebra $B = \mathcal{O} \otimes \mathbb{Q}$ is a definite quaternion algebra over $\mathbb{Q}$ with discriminant p, and $\mathcal{O}$ is a maximal order in B. We will denote the canonical anti-involutions of $\mathcal{O}$ and B by $x \mapsto \overline{x}$.

Let π denote the p-power Frobenius endomorphism on E, and fix a K-isomorphism between $E[\pi]$ and α_p, where α_p is the unique local-local group scheme over $\mathbb{F}_p$; then we can identify $\operatorname{Hom}_K(\alpha_p, E)$ with $\operatorname{End}_K(\alpha_p) = K$. The kernel of the restriction map

$$\begin{aligned} \tilde{}: \operatorname{End}_K(E) &\to \operatorname{End}_K(\alpha_p) \\ u &\mapsto \tilde{u} = u|_{\alpha_p} \end{aligned}$$

is a two-sided prime ideal $\mathfrak{P}$ of $\mathcal{O}$ above p, with residual degree 2. The restriction map thus gives a natural embedding $\mathcal{O}/\mathfrak{P} \hookrightarrow \operatorname{End}_K(\alpha_p) = K$ with image $\mathbb{F}_{p^2}$. Since $\pi^2 = -p$, the prime ideal $\mathfrak{P}$ is principal and generated by π.

For every $(i,j) \in K^2$, we denote by A_{ij} the abelian surface over K given by the following diagram:

$$0 \to \alpha_p \xrightarrow{(i,j)} E \times E \to A_{ij} \to 0.$$

It is easy to check that

$$\begin{aligned} A_{ij} = A_{i'j'} &\iff (i,j)(\alpha_p) = (i',j')(\alpha_p) \\ &\iff \exists a \in K^* \text{ such that } (i',j') = a(i,j). \end{aligned}$$

Thus, the set of all A_{ij} (apart from $A_{00} = E \times E$) is parametrized by $\mathbb{P}^1(K)$.

For every $i \in K$ the composition $\alpha_p \xrightarrow{i} E \xrightarrow{u} E$ corresponds to the element $i\,\tilde{u}$ of K. For every endomorphism $\alpha \in \mathrm{End}_K(E \times E) \cong M_2(\mathcal{O})$ and every $[i:j] \in \mathbb{P}^1(K)$, the composition

$$\alpha_p \xrightarrow{(i,j)} E \times E \xrightarrow{\alpha} E \times E$$

has the same image as the element $\widetilde{\alpha}[i:j] \in \mathbb{P}^1(K)$, where $\widetilde{\alpha} \in M_2(\mathbb{F}_{p^2})$ is obtained by reduction modulo $\mathfrak{P}$ of the entries of α, and the action of $M_2(\mathbb{F}_{p^2})$ on $\mathbb{P}^1(K)$ is the usual projective action.

If A is an abelian surface over K we denote by $a(A)$ the quantity

$$a(A) = \dim \mathrm{Hom}_K(\alpha_p, A),$$

sometimes called the *a-number* of A. When A is a supersingular abelian surface we have $a(A) \in \{1, 2\}$. The value of $a(A)$ gives us information about the global structure of A, as the following result shows.

Proposition 11.1. — *We have $a(A) = 2$ if and only if $A \cong E \times E$. We have $a(A) = 1$ if and only if $A \cong A_{ij}$ for some $[i:j] \in \mathbb{P}^1(K) \setminus \mathbb{P}^1(\mathbb{F}_{p^2})$. Furthermore, if $a(A) = 1$ then $a(A/\alpha_p) = 2$.*

Proof. — This follows from [Oort 75, Introduction], [Oort 75, Thm. 2], and [Oort 75, Cor. 7]. □

11.2. Quaternion hermitian forms and lattices

Most of the material that we present without reference in this section can be found in [34].

Let B be a definite quaternion algebra over $\mathbb{Q}$ with discriminant p. There is a positive definite hermitian form on the right B-module B^2, which is unique up to base change over B; it is given explicitly by $\sum \overline{x_i} y_i$, where $x \mapsto \overline{x}$ is the standard involution on B. For every prime ℓ (possibly equal to p) we set $B_\ell = B \otimes \mathbb{Q}_\ell$. Then the hermitian form on B^2 extends to give a hermitian form on B_ℓ^2. Let $\dagger$ denote the conjugate-transpose involution on $M_2(B)$ and on $M_2(B_\ell)$, where 'conjugation' means the standard involution. Then the groups of similitudes of the hermitian forms on B^2 and on B_ℓ^2 are given by

$$G = \{g \in M_2(B) \mid g^\dagger g = n(g) I \text{ for some } n(g) \in \mathbb{Q}^*\}$$

and

$$G_\ell = \{g \in M_2(B_\ell) \mid g^\dagger g = n(g) I \text{ for some } n(g) \in \mathbb{Q}_\ell^*\}.$$

Let $\mathcal{O}$ be a maximal order of B. A $\mathbb{Z}$-lattice L in B^2 is called a (*right*) *$\mathcal{O}$-lattice* if L is a right $\mathcal{O}$-module. Two $\mathcal{O}$-lattices L_1 and L_2 are *globally equivalent* if $L_1 = gL_2$ for some $g \in G$, and are *locally equivalent at ℓ* if $L_1 \otimes \mathbb{Z}_\ell = g(L_2 \otimes \mathbb{Z}_\ell)$ for some $g \in G_\ell$. One denotes by $\mathrm{Aut}(L) = \{g \in G \mid gL = L\}$ the *automorphism group* of L and by $\mathrm{Aut}'(L) = \mathrm{Aut}(L)/\pm 1$ the *reduced automorphism group* of L. These groups are finite because the hermitian form on B^2 is positive definite.

A *genus* of $\mathcal{O}$-lattices is a set of $\mathcal{O}$-lattices in B^2 that are equivalent to one another locally at every prime ℓ. There are only two genera: the *principal genus* $\mathcal{L}_2(p,1)$ that contains the right $\mathcal{O}$-lattices in B^2 that are equivalent to $\mathcal{O}_\ell^2$ for all ℓ, and the *non-principal genus* $\mathcal{L}_2(1,p)$ that contains the right $\mathcal{O}$-lattices in B^2 that are equivalent to $\mathcal{O}_\ell^2$ for all $\ell \neq p$ and equivalent at p to

(11.1)
$$\xi \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix} \mathcal{O}_p^2, \qquad \text{where } \xi \in \mathrm{GL}_2(\mathcal{O}_p) \text{ satisfies } \xi^\dagger \xi = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

with π a prime element of $\mathcal{O}_p$. One denotes by $H_2(p,1)$ the (finite) number of global equivalence classes in $\mathcal{L}_2(p,1)$, and by $H_2(1,p)$ the number of global equivalence classes in $\mathcal{L}_2(1,p)$.

On the other hand one can define two special sets of positive definite hermitian matrices. Let $\mathfrak{P}$ be the two sided prime ideal of $\mathcal{O}$ above p.

Definition 11.2. — *We define Λ^{princ} to be the set of matrices H in $\mathrm{GL}_2(\mathcal{O})$ such that*

$$H = \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix} \text{ with } st - r\bar{r} = 1,$$

where s and t are positive integers. We define $\Lambda^{\mathrm{nprinc}}$ to be the set of matrices H in $M_2(\mathcal{O})$ such that

$$H = \begin{pmatrix} ps & r \\ \bar{r} & pt \end{pmatrix} \text{ with } p^2 st - r\bar{r} = p,$$

where s and t are positive integers and where $r \in \mathfrak{P}$.

Two matrices H_1, H_2 that both lie in Λ^{princ} or in $\Lambda^{\mathrm{nprinc}}$ are said to be *equivalent* if there exists an $\alpha \in \mathrm{GL}_2(\mathcal{O})$ such that $\alpha^\dagger H_1 \alpha = H_2$. For H in Λ^{princ} or $\Lambda^{\mathrm{nprinc}}$, we let

$$\mathrm{Aut}(H) = \{\alpha \in \mathrm{GL}_2(\mathcal{O}) \mid \alpha^\dagger H \alpha = H\}$$

be the *automorphism group* of H and $\mathrm{Aut}'(H) = \mathrm{Aut}(H)/\pm 1$ the *reduced automorphism group* of H. These groups are again finite.

One can relate lattices and hermitian forms in the following way.

Proposition 11.3. — *There are bijective correspondences*

$$\left\{\begin{array}{l}\textit{global equivalence classes}\\ \textit{of lattices in } \mathcal{L}_2(p,1)\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{equivalence classes}\\ \textit{of matrices in } \Lambda^{\mathrm{princ}}\end{array}\right\}$$

and

$$\left\{\begin{array}{l}\textit{global equivalence classes}\\ \textit{of lattices in } \mathcal{L}_2(1,p)\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{equivalence classes}\\ \textit{of matrices in } \Lambda^{\mathrm{nprinc}}\end{array}\right\}$$

that preserve automorphism groups and reduced automorphism groups, as abstract groups.

Proof. — The bijective correspondences are provided by Lemmas 2.3 and 2.5 of [16] in the principal case, and by Lemmas 2.6 and 2.7 of [16] in the non-principal case. The fact that the bijections provided by these lemmas preserve automorphism groups is easily seen from the proofs of the lemmas. □

The automorphisms α of the hermitian forms in $\Lambda^{\mathrm{nprinc}}$ are determined (up to ±1) by the projective action of $\widetilde{\alpha}$. This fact is probably well-known, but for lack of a suitable reference we include a short proof.

Lemma 11.4. — *Let $\Gamma \subseteq \mathrm{GL}_2(\mathcal{O})$ be a finite subgroup of order prime to p. Then reduction modulo $\mathfrak{P}$ determines an embedding*

$$\widetilde{\ }: \Gamma \hookrightarrow \mathrm{GL}_2(\mathbb{F}_{p^2}).$$

Proof. — If $\alpha \in \Gamma$ is the identity modulo $\mathfrak{P}$, then α is an element of the multiplicative group $1 + \pi M_2(\mathcal{O})$. This group has no torsion element of order prime to p, so we must have $\alpha = 1$.

More explicitly, every element of the group $1+\pi M_2(\mathcal{O})$ can be written in the form $1 + \pi^N M$, with $N > 0$ and $M \notin M_2(\mathfrak{P})$. Thus, for every positive integer n we have

$$(1 + \pi^N M)^n \equiv 1 + n\pi^N M \bmod \mathfrak{P}^{2N},$$

and if n is prime to p we cannot have $(1 + \pi^N M)^n = 1$, since $n\pi^N M \not\equiv 0 \bmod \mathfrak{P}^{2N}$. □

Proposition 11.5. — *Let H be an element of $\Lambda^{\mathrm{nprinc}}$ and let $\Gamma \subseteq \mathrm{Aut}(H)$ be a subgroup of order prime to p. Then reduction modulo $\mathfrak{P}$ gives embeddings*

$$\Gamma \hookrightarrow \mathrm{SL}_2(\mathbb{F}_{p^2}) \quad \textit{and} \quad \Gamma/\{\pm1\} \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_{p^2}).$$

Proof. — By the above lemma, we need only check that $\det(\widetilde{\alpha}) = 1$ for all $\alpha \in \mathrm{Aut}(H)$. Put $H = x^\dagger x$ for some $x \in \mathrm{GL}_2(B)$ and let $L = x\mathcal{O}^2$ be the lattice in the non-principal genus attached to H as in Proposition 11.3. Since the lattice $L \otimes \mathbb{Z}_p$ is equivalent to the lattice given in (11.1), there exist $g \in G_p$ and $\beta \in \mathrm{GL}_2(\mathcal{O}_p)$ such that $x = g\xi \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix} \beta$. We compute that

$$H = x^\dagger x = \beta^\dagger \begin{pmatrix} 1 & 0 \\ 0 & -\pi \end{pmatrix} \xi^\dagger g^\dagger g \xi \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix} \beta = n(g) \beta^\dagger \begin{pmatrix} 0 & \pi \\ -\pi & 0 \end{pmatrix} \beta.$$

Let $\gamma = \beta\alpha\beta^{-1}$. Then from $H = \alpha^\dagger H \alpha$ we find that

$$\gamma^\dagger \begin{pmatrix} 0 & \pi \\ -\pi & 0 \end{pmatrix} \gamma = \begin{pmatrix} 0 & \pi \\ -\pi & 0 \end{pmatrix}. \tag{11.2}$$

Since γ and β lie in $\mathrm{GL}_2(\mathcal{O}_p)$, we can reduce them modulo $\mathfrak{P}$ as well; thus, it is sufficient to check that $\det(\widetilde{\gamma}) = 1$. Now, $\overline{\gamma}\pi = \pi\gamma'$ with $\widetilde{\gamma'} = \widetilde{\gamma}$. Hence, we can cancel π in both sides of (11.2) to get

$$(\gamma')^t \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \gamma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

and this implies that $\widetilde{\gamma}$ belongs to the symplectic group and has determinant equal to 1. □

Katsura and Oort determined the groups that can occur as the reduced automorphism group of a hermitian form in $\Lambda^{\mathrm{nprinc}}$ (see [20] and [15, Lem. 2.1]). This result will play a crucial role in our strategy.

THEOREM 11.6. — *If $p \geqslant 7$, then the reduced automorphism group of a hermitian matrix in $\Lambda^{\mathrm{nprinc}}$ is isomorphic as an abstract group to one of the following groups*:

$$\mathbb{Z}/n\mathbb{Z} \text{ for some } n \in \{1,2,3\}; \quad D_{2n} \text{ for some } n \in \{2,3,6\};\ A_4;\ S_4;\ A_5.$$

If $p = 3$ or $p = 5$, then $H(1,p) = 1$ and the reduced automorphism group of the single class is isomorphic to A_6 when $p = 3$ and to $\mathrm{PGL}_2(\mathbb{F}_5)$ when $p = 5$.

Given a monic polynomial $f \in \mathbb{Z}[x]$ and a subgroup Γ of $\mathrm{GL}_2(B)$, let Γ_f denote the set of elements of Γ whose reduced characteristic polynomials (as elements of $M_2(B)$) are equal to f. For each possible reduced automorphism group Γ' of a hermitian matrix in $\Lambda^{\mathrm{nprinc}}$, Ibukiyama [15, Thm. 7.1] determined the cardinality of the set of equivalence classes of hermitian matrices $H \in \Lambda^{\mathrm{nprinc}}$ with $\mathrm{Aut}'(H) \cong \Gamma'$. An important ingredient in this computation is the determination of mass formulas for the number of elements in Γ_f for all Γ and f. Given a monic degree-4 polynomial $f \in \mathbb{Z}[x]$, we define $m(f)$ to be the quantity

$$m(f) := \sum_{i=1}^{h} \frac{|\Gamma_{i,f}|}{|\Gamma_i|},$$

where $h = H(1,p)$ is the number of classes in Λ^{nprinc} and where the Γ_i are the automorphism groups of a set of representatives for the equivalence classes of Λ^{nprinc}. Ibukiyama computed the masses $m(f)$ explicitly ([15, Thm. 2.2]).

Theorem 11.7. — *Assume that $p \geqslant 7$. Then $m(f) = 0$ for all polynomials $f \in \mathbb{Z}[x]$ except for those with $f(x)$ or $f(-x)$ belonging to the following list*:

$$f_1 = (x-1)^4, \quad f_2 = (x^2+1)^2, \quad f_3 = (x^2+x+1)^2,$$
$$f_4 = x^4+1, \quad f_5 = x^4+x^3+x^2+x+1, \quad f_6 = x^4-x^2+1.$$

Moreover, $m(f_2) > 0$ for all $p \geqslant 7$, and

$$m(f_4) > 0 \text{ if and only if } p \equiv 3,\ 5 \bmod 8,$$
$$m(f_6) > 0 \text{ if and only if } p \equiv 5 \bmod 12.$$

Remark 11.8. — There is a similar result in the principal genus case; see [5, Part I].

11.3. Polarizations

Later in the paper we will need to understand the principal polarizations on the supersingular abelian surfaces over the algebraic closure K of a finite field $\mathbb{F}_q$. In this section we present the relevant results.

Recall that in §11.1 we chose a trace-0 elliptic curve E over $\mathbb{F}_p$. The K-endomorphism ring $\mathcal{O}$ of E is a maximal order in the quaternion algebra B over $\mathbb{Q}$ with discriminant p.

Let λ_0 be the product principal polarization on $E \times E$ and let $\dagger$ be the Rosati involution on $\operatorname{End}_K(E \times E)$ associated to this polarization. It is well-known that under the natural isomorphism $\operatorname{End}_K(E \times E) \cong M_2(\mathcal{O})$, the Rosati involution becomes the conjugate-transpose involution.

The polarization λ_0 induces an injection from the Néron-Severi group $\operatorname{NS}(E \times E)$ to $\operatorname{End}_K(E \times E)$ by $\lambda \mapsto \lambda_0^{-1}\lambda$. The image of this map is also well-known (see for instance [16, Prop. 2.8]).

Proposition 11.9. — *The map given above induces a bijection between* $\mathrm{NS}(E \times E)$ *and the set of hermitian matrices in* $M_2(\mathcal{O})$. *Moreover, this map restricts to a bijection between the set of principal polarizations on* $E \times E$ *and* Λ^{princ}.

We can understand in a similar way the principal polarizations of the supersingular surfaces that are not geometrically isomorphic to $E \times E$. Let A be a supersingular abelian surface with $a(A) = 1$, and let ψ be the natural degree-p isogeny from $E \times E$ to A (see §11.1). Then we can define a map $\mathrm{NS}(A) \to M_2(\mathcal{O})$ by

$$\lambda \mapsto \lambda_0^{-1}\widehat{\psi}\lambda\psi.$$

Proposition 2.14 of [16] tells us the following.

Proposition 11.10. — *The map given above induces a bijection between the set of principal polarizations on* A *and the set* $\Lambda^{\mathrm{nprinc}}$.

12. Supersingular surfaces over finite fields.

Let $k = \mathbb{F}_q$ be a finite field of characteristic p that has even degree over $\mathbb{F}_p$, and let $K = \overline{\mathbb{F}}_q$. In this section we answer some basic questions concerning supersingular abelian surfaces over k, their isogeny classes, and their principal polarizations.

Suppose A is a supersingular abelian surface over k. If $a(A) = 2$ then A is a K/k-twist of the abelian surface $E \times E$, where, as before, E is a trace-0 elliptic curve over $\mathbb{F}_p$. On the other hand, if $a(A) = 1$ then there is a unique copy of α_p in A, which must necessarily be defined over k, and by Proposition 11.1 the quotient A/α_p has a-number 2. Therefore, every A is either a K/k twist of $E \times E$ or a quotient of such a twist by a rank-p subgroup. In particular, every isogeny class of supersingular surfaces over k contains a K/k-twist of $E \times E$.

Thus, to understand the supersingular abelian surfaces over k and their principal polarizations, we need only answer the following questions:

- What are the K/k-twists of $E \times E$, and what are the Weil polynomials of these twists?
- Which rank-p geometric subgroups of these twists can be defined over k?
- Which geometric polarizations of these twists can be defined over k?

In this section we will answer these questions.

Remark 12.1. — We could ask the same questions for arbitrary finite fields instead of limiting ourselves to those that contain $\mathbb{F}_{p^2}$, but we will only need the answers for even-degree extensions of $\mathbb{F}_p$, and the answers for odd-degree extensions of $\mathbb{F}_p$ are slightly more awkward to state. The answers are simpler for the fields that contain $\mathbb{F}_{p^2}$ because for these fields the Galois group of K/k acts trivially on $\mathrm{End}_K(E \times E)$.

The first of our three questions is easy to answer. We know that the twists of $E \times E$ correspond to elements of the cohomology set $H^1(\mathrm{Gal}(K/k), \mathrm{Aut}_K(E \times E))$, and since all of the geometric endomorphisms of E are defined over k, this cohomology set consists of the conjugacy classes of the elements of finite order in $\mathrm{Aut}(E \times E)$. If A is a twist of $E \times E$, and if $f\colon E \times E \to A$ is a geometric isomorphism, then $\alpha := f^{-1} f^{\sigma}$ is the automorphism of $E \times E$ that corresponds to the twist A; here σ is the Frobenius automorphism of K/k.

Let π be the q-power Frobenius on $E \times E$ and let π_A be the q-power Frobenius of a twist A of $E \times E$. The pullback of π_A via the geometric isomorphism f is equal to $\alpha\pi$, so that π_A and $\alpha\pi$ have the same characteristic polynomial. Since $\pi = \pm\sqrt{q}$ is an integer in $\mathrm{End}_K(E \times E)$, the characteristic polynomial of π_A is $\pi^4 h(x/\pi)$, where $h \in \mathbb{Z}[x]$ is the characteristic polynomial of α. The same argument is valid in a more general situation:

Proposition 12.2. — *Let A and B be abelian surfaces over k with q-power Frobenius endomorphisms π_A and π_B, respectively. Let $f\colon B \longrightarrow A$ be a K-isomorphism and let $h \in \mathbb{Z}[x]$ be the characteristic polynomial of $\alpha = f^{-1} f^{\sigma} \in \mathrm{Aut}_K(B)$. If π_B acts as an integer on B then the characteristic polynomial of π_A is $\pi_B^4 h(x/\pi_B)$.*

We turn to the second question. Given $(i,j) \in K^2$ with $(i,j) \neq (0,0)$, we would like to know whether the subgroup $f((i,j)(\alpha_p))$ of A is definable over k.

Proposition 12.3. — *The subgroup $f((i,j)(\alpha_p))$ of A is definable over k if and only if $[i:j]$ and $\widetilde{\alpha}[i^{\sigma}:j^{\sigma}]$ are equal in $\mathbb{P}^1(K)$.*

Proof. — The morphism $f \circ (i,j)\colon \alpha_p \longrightarrow A$ is defined over k if and only if it is invariant under the action of the Galois group of K/k, so we have

$$f \circ (i,j) = f^{\sigma} \circ (i^{\sigma}, j^{\sigma}) \iff (i,j) = \alpha \circ (i^{\sigma}, j^{\sigma}) \iff [i:j] = \widetilde{\alpha}\,[i^{\sigma}:j^{\sigma}].$$

□

It will also be useful to know when we can be assured of the existence of a rational local-local subgroup of A that gives rise to a quotient with

a-number 1. By Proposition 11.1 we need $[i : j] \in \mathbb{P}^1(K) \setminus \mathbb{P}^1(\mathbb{F}_{p^2})$ such that the morphism $f \circ (i, j)$ is defined over k.

Proposition 12.4. — *Let $H \in \Lambda^{\mathrm{nprinc}}$ and let $\alpha \in \mathrm{Aut}(H)$ be an automorphism of order not divisible by p. Then there exists an element $[i : j] \in \mathbb{P}^1(K) \setminus \mathbb{P}^1(\mathbb{F}_{p^2})$ such that $[i : j] = \widetilde{\alpha}[i^\sigma : j^\sigma]$, unless $q = p^2$ and $\alpha = \pm 1$.*

Proof. — The equation $[i : j] = \widetilde{\alpha}[i^q : j^q]$ can be rewritten as a homogeneous equation in i and j of degree $q + 1$, and it is easy to verify that the subscheme of $\mathbb{P}^1$ defined by this equation is nonsingular, so there are $q+1$ points $[i : j]$ that satisfy the equation. If $q > p^2$, we are guaranteed a solution that does not lie in $\mathbb{P}^1(\mathbb{F}_{p^2})$. If $q = p^2$ and every element of $\mathbb{P}^1(\mathbb{F}_{p^2})$ is a root of the equation, then we see that $\widetilde{\alpha}$ fixes every element of $\mathbb{P}^1(\mathbb{F}_{p^2})$, and Proposition 11.5 shows that $\alpha = \pm 1$. □

The third of our three questions asks when a geometric polarization of $E \times E$ gives rise to a polarization of A defined over k.

Proposition 12.5. — *Let λ be a polarization of $E \times E$ and let $H = \lambda_0^{-1}\lambda \in \mathrm{End}_K(E \times E)$. Then the polarization $\widehat{f^{-1}}\lambda f^{-1}$ of A is defined over k if and only if $H = \alpha^\dagger H \alpha$.*

Proof. — The polarization will descend to A if and only if it is fixed by the action of σ, that is, if and only if

$$\left(\widehat{f^{-1}}\lambda f^{-1}\right)^\sigma = \widehat{f^{-1}}\lambda f^{-1}.$$

Multiplying by f^σ on the right and by $\widehat{f^\sigma}$ on the left, we find that this condition is equivalent to

$$\lambda = \widehat{f^{-1} f^\sigma}\lambda f^{-1} f^\sigma.$$

This translates into the statement that $H = \alpha^\dagger H \alpha$. □

13. Jacobians in isogeny classes of simple supersingular surfaces

In this section we will prove Theorem 10.1. The techniques we use depend on whether or not the base field $k = \mathbb{F}_q$ has even degree over its prime field, so we consider these cases in two separate subsections. Throughout this section we will let K denote an algebraic closure of k, and we will always assume that the characteristic of k is greater than 3.

13.1. The case q a square

We first show how certain Weil polynomials can be produced by Proposition 12.2. We begin with a simple observation: Suppose u is an automorphism of a hyperelliptic curve C, and let ι be the hyperelliptic involution of C. Then u induces an automorphism u' of the genus-0 curve $C/\langle\iota\rangle$, and the order of u' is equal to the order of u unless $\iota \in \langle u\rangle$, in which case the order of u' is half that of u.

PROPOSITION 13.1. — *Let $k = \mathbb{F}_q$ be a finite field (of characteristic at least 5) that has even degree over its prime field. Let C be a supersingular genus-2 curve over k such that the Frobenius endomorphism π of the Jacobian J of C is equal to the integer $\varepsilon\sqrt{q}$, where $\varepsilon = \pm 1$. Let u be a geometric automorphism of C and let u' be the induced automorphism of $\mathbb{P}^1$. Let n and n' be the orders of u and u', respectively, and let C' be the twist of C determined by u. Then the pair (n, n') appears in the left column of Table 13.1, and the Weil polynomial of C' is $q^2 f_{n,n'}(\varepsilon x/\sqrt{q})$, where $f_{n,n'}$ is the polynomial appearing in the right column.*

(n, n')	$f_{n,n'}$
$(1, 1)$	$(x-1)^4$
$(2, 1)$	$(x+1)^4$
$(2, 2)$	$(x-1)^2(x+1)^2$
$(3, 3)$	$(x^2+x+1)^2$
$(4, 2)$	$(x^2+1)^2$
$(5, 5)$	$x^4+x^3+x^2+x+1$
$(6, 3)$	$(x^2-x+1)^2$
$(6, 6)$	$(x^2-x+1)(x^2+x+1)$
$(8, 4)$	x^4+1
$(10, 5)$	$x^4-x^3+x^2-x+1$

Table 13.1. Characteristic polynomials of certain automorphisms of supersingular Jacobians.

Proof. — Igusa [17, §8] computed the groups that can occur as the reduced automorphism groups of hyperelliptic curves. Looking at Igusa's list, we see that n' must be an element of $\{1, 2, 3, 4, 5, 6\}$. Since n is equal to either n' or $2n'$, we see that the left column includes all possibilities except for $n = 4$, $n' = 4$ and $n = 12$, $n' = 6$. These cases can be excluded by computing the automorphism groups of Igusa's curves with many automorphisms.

Now Proposition 13.1 will follow from Proposition 12.2, provided that we can show that the characteristic polynomial g of the automorphism u^* of J is equal to the polynomial f associated to the pair (n, n'). Four facts will be very helpful in our proof that $g = f$:

(1) The gcd of g and $x^n - 1$ does not divide $x^m - 1$ for any $m < n$.
(2) If $n = 2n'$, the gcd of g and $x^{n'} + 1$ does not divide $x^m + 1$ for any $m < n'$.
(3) If $n = n'$, the gcd of g and $x^n - 1$ divides no polynomial of the form $x^m + 1$.
(4) The constant term of g is 1.

The first three facts follow from the definitions of n and n' and from the fact that u^* satisfies the relevant gcd in each case. The fourth fact holds because u^* is an automorphism of the polarized Jacobian, and so its product with its Rosati involute is equal to 1.

These four facts allow us to determine g in all cases, except when $n = 3$ or $n = 6$. Consider the case when $n = 3$. Then g must be either

$$(x-1)^4, \quad (x-1)^2(x^2+x+1), \quad \text{or} \quad (x^2+x+1)^2.$$

The first possibility is eliminated by fact (1) above. If g were equal to the second polynomial, then Proposition 12.2 would show that the Weil polynomial of C' would be

$$(x^2 - 2sx + q)(x^2 + sx + q)$$

for some s with $s^2 = q$. But Theorem 2.4 shows that there are no curves with such a Weil polynomial. It follows that $g = (x^2 + x + 1)^2$, as claimed in the table. The cases with $n = 6$ follow in a similar way. □

Remark 13.2. — Suppose u is an order-n automorphism of a genus-g hyperelliptic curve over an arbitrary algebraically-closed field, and let n' be the order of the automorphism of $\mathbb{P}^1$ induced by u. Theorem 1 of [4] shows that the values of g, n, and n' completely determine the characteristic polynomial f of u^*, unless n and $(2g+2)/n$ are even and $n = n'$, in which case there are two possibilities for f; the theorem gives explicit formulas for the possible values of f in all cases. When $g = 2$, it is not possible for n and $(2g+2)/n$ to both be even, and Table 13.1 can be derived from the results of [4].

We continue to let E denote an elliptic curve over $\mathbb{F}_p$ with trace 0. The following propositions will help us detect the existence of Jacobians among the supersingular surfaces A that have respectively $a(A) = 2$ or $a(A) = 1$.

Proposition 13.3. — *Let C be a supersingular genus-2 curve over k whose Jacobian has a-number 2. If C' is a twist of C, then the Weil polynomial of C' is $q^2 f(x/\sqrt{q})$ for some $f = f_{n,n'}$ from Table 13.1. Furthermore, C has a twist with Weil polynomial $q^2 f_{n,n'}(x/\sqrt{q})$ if and only if there is a geometric automorphism u of C of order n that induces an automorphism of order n' on the projective line.*

Proof. — Since the principally polarized surface $\operatorname{Jac} C$ has a-number 2, it is geometrically isomorphic to $(E \times E, \lambda)$ for some principal polarization λ. Now, $(E \times E, \lambda)$ is defined over $\mathbb{F}_{p^2}$, hence over $\mathbb{F}_q$, and it is k-isomorphic to the canonically polarized Jacobian of a curve C_0 defined over k. By Torelli's theorem, C_0 is a twist of C. Replacing C_0 with its quadratic twist, if necessary, we may assume that the Frobenius on $\operatorname{Jac} C_0$ acts as $\sqrt{q}$.

The proposition is now a direct consequence of Proposition 13.1 because C and C_0 have the same set of twists, the q-power Frobenius endomorphism π_0 of the Jacobian of C_0 satisfies $\pi_0 = \sqrt{q}$, and any isomorphism between the curves C and C_0 induces an isomorphism between their geometric automorphism groups that identifies the hyperelliptic involutions. □

Proposition 13.4. — *Let $\mathcal{A}$ be the isogeny class $\mathcal{A}_{(0,2q)}$ (respectively $\mathcal{A}_{(0,0)}$, respectively $\mathcal{A}_{(0,-q)}$), and let $P \in \mathbb{Z}[x]$ be the polynomial $(x^2+1)^2$ (respectively x^4+1, respectively $x^4 - x^2 + 1$). Then there exists an $H \in \Lambda^{\mathrm{nprinc}}$ with an automorphism $\alpha \in \operatorname{Aut}(H)$ such that $P(\alpha) = 0$ if and only if there exists a curve C over k whose Jacobian lies in the isogeny class $\mathcal{A}$ and has a-number 1.*

Proof. — Suppose H is an element of $\Lambda^{\mathrm{nprinc}}$ and α is an element of $\operatorname{Aut}(H)$ with $P(\alpha) = 0$. Let A be the K/k-twist of $E \times E$ determined by α. Then by Proposition 12.2 we see that A lies in $\mathcal{A}$. By Propositions 11.1, 12.3, and 12.4 there is a k-rational α_p-subgroup G of A such that $a(A/G) = 1$. Now we apply Proposition 11.10 to the degree-p map

$$\varphi\colon E \times E \xrightarrow{\sim} A \longrightarrow A/G.$$

There is a principal polarization λ of A/G whose pullback by φ is the degree-p^2 polarization $\lambda_0 H$ of $E \times E$, where λ_0 is the product principal polarization on $E \times E$. Proposition 12.5 shows that the pullback of λ to A is defined over k; hence, λ is defined over k. The principally polarized variety $(A/G, \lambda)$ is not geometrically a product of elliptic curves (because $a(A/G) = 1$), so it is the Jacobian of a curve.

Conversely, suppose that C is a curve over k whose Jacobian J has a-number 1 and belongs to $\mathcal{A}$. Consider the quotient J/α_p of J by its unique α_p-subgroup, and let f be a geometric isomorphism $E \times E \longrightarrow J/\alpha_p$ (which exists by Proposition 11.1). Apply Proposition 11.10 to the degree-p map

$$\varphi\colon E \times E \xrightarrow{f} J/\alpha_p \longrightarrow J,$$

where the rightmost map is the dual isogeny of the canonical projection. There is some $H \in \Lambda^{\mathrm{nprinc}}$ uniquely associated to the canonical polarization ϑ of J. Since ϑ is defined over k, Proposition 12.5 shows that the automorphism $\alpha = f^{-1}f^{\sigma}$ lies in $\mathrm{Aut}(H)$. Finally, by Proposition 12.2 the characteristic polynomial of α is determined by the class $\mathcal{A}$ as indicated in the statement of the proposition. □

Now we proceed to the proof of Theorem 10.1 in the case that q is a square. Consulting Table 10.1, we see that we must show that there are Jacobians in $\mathcal{A}_{(0,0)}$ when $p \not\equiv 1 \bmod 4$, that there are Jacobians in $\mathcal{A}_{(0,2q)}$ when $p \equiv 1 \bmod 4$, and that when $p \not\equiv 1 \bmod 3$ there are Jacobians in $\mathcal{A}_{(0,-q)}$ if and only if $p \equiv 1 \bmod 4$.

The isogeny class $\mathcal{A}_{(0,2q)}$ when $p \equiv 1 \bmod 4$.

For $p > 5$ we deduce from Theorem 11.7 the existence of a hermitian form $H \in \Lambda^{\mathrm{nprinc}}$ that admits an automorphism α satisfying $(\alpha^2+1)^2 = 0$. By Proposition 13.4 there is a Jacobian in the class $\mathcal{A}_{(0,2q)}$.

For $p = 5$ (or more generally for $p \equiv 5 \bmod 8$), we can use the curve C given by the equation $y^2 = x^5 - x$. By [16, Prop. 1.12], this curve is supersingular and its Jacobian has a-number 2. Moreover, the automorphism u given by $(x, y) \mapsto (-x, \sqrt{-1}\,y)$ satisfies $u^2 = \iota$. By Proposition 13.3, the Jacobian of some twist of C lies in $\mathcal{A}_{(0,2q)}$. □

The isogeny class $\mathcal{A}_{(0,0)}$ when $p \not\equiv 1 \bmod 4$.

First we consider the case $p \equiv 7 \bmod 8$. Let C be the curve $y^2 = x^5 - x$. By [16, Prop. 1.12] we know this curve is supersingular and its Jacobian has a-number 2. Moreover, C has a geometric automorphism u satisfying $u^4 = \iota$; for instance, $(x, y) \mapsto (\zeta^2 x, \zeta y)$, where ζ is a primitive eighth root of unity. By Proposition 13.3, the Jacobian of some twist of C lies in $\mathcal{A}_{(0,0)}$.

Next we consider the case $p \equiv 3 \bmod 8$. In this case Theorem 11.7 shows that there is a hermitian form H in Λ^{nprinc} that has an automorphism α whose characteristic polynomial is $x^4 + 1$. By Proposition 13.4 there is a Jacobian in the class $\mathcal{A}_{(0,0)}$. □

The isogeny class $\mathcal{A}_{(0,-q)}$ when $p \not\equiv 1 \bmod 3$.

We must show that there is a Jacobian in this isogeny class if and only if $p \equiv 5 \bmod 12$.

To begin with, we note that Proposition 13.3 shows that there is no curve whose Jacobian lies in $\mathcal{A}_{(0,-q)}$ and has a-number 2. On the other hand, we see from Proposition 13.4 that there will be a curve C over k whose Jacobian lies in $\mathcal{A}_{(0,-q)}$ and has a-number 1 if and only if there exists an $H \in \Lambda^{\text{nprinc}}$ for which there is an $\alpha \in \operatorname{Aut}(H)$ satisfying $\alpha^4 - \alpha^2 + 1 = 0$. By Theorem 11.7, for $p > 5$ this happens if and only if $p \equiv 5 \bmod 12$.

For $p = 5$ we note that the matrices H in the unique equivalence class in Λ^{nprinc} have reduced automorphism group $\mathrm{PGL}_2(\mathbb{F}_5)$ (see Theorem 11.6). This group contains an element of exact order 6 that lifts to an $\alpha \in \operatorname{Aut}(H)$ that must satisfy $\alpha^6 = -1$. In fact, the reduced characteristic polynomial of α is a power of the minimal polynomial; hence $\alpha^6 = 1$ would imply that α has order 1, 2 or 3 in the reduced group. □

Remark 13.5. — The proof that there is no Jacobian with a-number 1 in $\mathcal{A}_{(0,-q)}$ is also valid for $p = 3$. There is no element of order 6 in the reduced automorphism group of the unique equivalence class in Λ^{nprinc}; in fact, by Theorem 11.6 this reduced group is isomorphic to A_6.

13.2. The case q not a square

We see from Table 10.1 that to prove Theorem 10.1 in the case where q is not a square, we must show that there are Jacobians in $\mathcal{A}_{(0,0)}$ when $p \not\equiv 1 \bmod 4$, in $\mathcal{A}_{(0,q)}$ when $p \not\equiv 1 \bmod 3$, in $\mathcal{A}_{(0,-q)}$ when $p \not\equiv 1 \bmod 3$, and in $\mathcal{A}_{(0,-2q)}$ for all p.

We begin with a remark about twists. Suppose that V is a variety over $k = \mathbb{F}_q$ all of whose automorphisms are defined over $\mathbb{F}_{q^2}$, and let σ denote the Frobenius automorphism of K over k. Let α be an automorphism of V. Then there is a 1-cocycle from $\operatorname{Gal}(K/k)$ to $\operatorname{Aut}_K(V)$ that sends σ to α if and only if $\alpha\alpha^\sigma$ has finite order in $\operatorname{Aut}_K(V)$. (Note that the latter condition is equivalent to $\alpha^\sigma\alpha$ having finite order, and that the orders of $\alpha^\sigma\alpha$ and

$\alpha\alpha^\sigma$ are equal to one another.) As always, the K/k-twists of V correspond to elements of the pointed cohomology set $H^1(\mathrm{Gal}(K/k), \mathrm{Aut}_K(V))$. If V' is a twist of V and $f : V \to V'$ is a K-isomorphism, then V' corresponds to the class of the cocycle that sends σ to $f^{-1}f^\sigma$.

The following proposition, similar to Proposition 13.3, allows us to construct twists in certain isogeny classes.

Proposition 13.6. — *Let C be a supersingular genus-2 curve over k such that the Frobenius endomorphism π of the Jacobian satisfies $\pi^2 = \varepsilon q$, where $\varepsilon = \pm 1$. Let u be a geometric automorphism of C such that uu^σ has order $n \in \{1, 2, 3, 4, 6\}$ and let C' be the twist of C determined by u. Then the Weil polynomial $x^4 + ax^3 + bx^2 + aqx + q^2$ of C' is determined by n as follows:*

n	1	2	3	4	6
(a, b)	$(0, -2\varepsilon q)$	$(0, 2\varepsilon q)$	$(0, \varepsilon q)$	$(0, 0)$	$(0, -\varepsilon q)$

Proof. — Let J be the Jacobian of C. Then the Jacobian J' of C' is the twist of J associated to the automorphism $\alpha = u_*$. Note that $\alpha\alpha^\sigma$ has order n.

Let $\pi \in \mathrm{End}_K(J)$ and $\pi' \in \mathrm{End}_K(J')$ be the q-power Frobenius endomorphisms of J and J', respectively and let $f\colon J \to J'$ be a geometric isomorphism such that $\alpha = f^{-1}f^\sigma$. The condition on π implies that J splits over the quadratic extension of k, and the condition $(\alpha\alpha^\sigma)^n = 1$ implies that f is defined over the extension of k of degree 24; in particular, the isogeny class of J' splits over this extension. Checking the list of supersingular isogeny classes over odd-degree extensions of prime finite fields of odd characteristic that split over the extension of degree 24 (see [25, Thm. 2.9] and [25, Table 1]), we see that the characteristic polynomial of π' is $x^4 + bqx^2 + q^2$ for some integer $b \in \{0, \pm 1, \pm 2\}$.

The pullback of π' by f is $\alpha\pi$. Since $\pi^2 = \varepsilon q$ and $\alpha^\sigma\pi = \pi\alpha$, this implies that

$$(\alpha\alpha^\sigma)^2 + \varepsilon b\, \alpha\alpha^\sigma + 1 = 0$$

in $\mathrm{End}_K(J)$. Comparing this identity with $(\alpha\alpha^\sigma)^n = 1$, we see that $b = -2\varepsilon, 2\varepsilon, \varepsilon, 0$ or $-\varepsilon$, according to $n = 1, 2, 3, 4$ or 6. □

The isogeny classes $\mathcal{A}_{(0,\pm q)}$ when $p \not\equiv 1 \bmod 3$.

Let C be the curve $y^2 = x^6 + 1$ over k, and let E be the supersingular elliptic curve $y^2 = x^3 + 1$. The two obvious maps from C to E show that the Jacobian J of C is $(2, 2)$-isogenous to $E \times E$ over k, so the Frobenius π of J satisfies $\pi^2 = -q$.

Let $\zeta \in K$ be a primitive sixth root of unity, and let u be the K-automorphism

$$(x, y) \mapsto (\zeta/x, y/x^3)$$

of C. One checks easily that $(u^\sigma u)(x, y) = (\zeta^4 x, \zeta^3 y)$; hence, $(u^\sigma u)^3 = \iota$, so $u^\sigma u$ has order 6 and the Jacobian of some twist of C lies in $\mathcal{A}_{(0,q)}$ by Proposition 13.6.

If ζ is a primitive cube root of unity, the same computation shows that the automorphism $u^\sigma u$ has order 3, so the Jacobian of some twist of C lies in $\mathcal{A}_{(0,-q)}$. □

The isogeny class $\mathcal{A}_{(0,-2q)}$.

For this case, we found it simplest to use a direct construction involving Kani's result (Theorem 3.1) combined with Galois descent.

Let F be an elliptic curve over $\mathbb{F}_{q^2}$ whose q^2-Frobenius is equal to q, and let $F^{(q)}$ be its Galois conjugate over $\mathbb{F}_q$. The q^2-Frobenius acts as the identity on the 2-torsion points of E, so all of the 2-torsion points of F are rational over $\mathbb{F}_{q^2}$. Label the nonzero 2-torsion points P, Q, and R, and let $P^{(q)}$, $Q^{(q)}$, and $R^{(q)}$ be the corresponding points on $F^{(q)}$.

We can easily produce four maximal isotropic subgroups of $(F \times F^{(q)})[2]$ that are stable under the action of the Galois group of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$:

$$\begin{aligned}
&\{(0,0), (P, P^{(q)}), (Q, Q^{(q)}), (R, R^{(q)})\},\\
&\{(0,0), (P, P^{(q)}), (Q, R^{(q)}), (R, Q^{(q)})\},\\
&\{(0,0), (P, R^{(q)}), (Q, Q^{(q)}), (R, P^{(q)})\},\\
&\{(0,0), (P, Q^{(q)}), (Q, P^{(q)}), (R, R^{(q)})\}.
\end{aligned}$$

These are the graphs of certain anti-isometries $F[2] \to F^{(q)}[2]$. But the number of reducible geometric anti-isometries from F to $F^{(q)}$ is equal to half of the number of geometric isomorphisms from F to $F^{(q)}$, and since we are in characteristic greater than 3, there are at most 6 such isomorphisms. Therefore, at least one of the subgroups G listed above comes from an irreducible anti-isometry, and so there is a curve C over $\mathbb{F}_{q^2}$ whose Jacobian is isomorphic to $(F \times F^{(q)})/G$. Clearly the polarized Jacobian of C is isomorphic to its Galois conjugate, so C can be defined over $\mathbb{F}_q$. Furthermore, the isogeny $\operatorname{Jac} C_{\mathbb{F}_{q^2}} \to F \times F^{(q)}$ descends to give an isogeny from $\operatorname{Jac} C$ to the restriction of scalars of E. It follows that $\operatorname{Jac} C$ lies in the isogeny class $\mathcal{A}_{(0,-2q)}$. □

The isogeny classes $\mathcal{A}_{(0,0)}$ when $p \not\equiv 1 \bmod 4$.

We require two separate arguments for this case, one when $p \equiv 7 \bmod 8$ and one when $p \equiv 3 \bmod 8$.

First suppose that $p \equiv 7 \bmod 8$. Let C be the curve $y^2 = x^5 - x$. By [16, Prop. 1.12] and [16, Rem. 1.4] we see that the Jacobian J of C is k-isogenous to the product of two supersingular curves. Let $\zeta \in K$ be a primitive eighth root of unity, and let u be the K-automorphism

$$(x, y) \mapsto (\zeta^2/x, \zeta y/x^3)$$

of C. One checks easily that $(u^\sigma u)(x, y) = (-x, \zeta^2 y)$, so that $u^\sigma u$ has order 4 in $\mathrm{Aut}_K(C)$. Proposition 13.6 then shows that the Jacobian of some twist of C lies in $\mathcal{A}_{(0,0)}$.

Now we turn to the case $p \equiv 3 \bmod 8$. Let E be the supersingular elliptic curve $y^2 = x^3 + x$, let i be the geometric automorphism $(x, y) \mapsto (-x, \sqrt{-1}\, y)$ of E, and let α be the automorphism

$$\begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix}$$

of $E \times E$. Note that $\alpha^\sigma \alpha$ has order 4 in $\mathrm{Aut}_K(E \times E)$, so there is a cocycle from $\mathrm{Gal}(K/k)$ to $\mathrm{Aut}_K(E \times E)$ that sends σ to α. Let A be the twist of $E \times E$ corresponding to the cohomology class in

$$H^1(\mathrm{Gal}(K/k), \mathrm{Aut}_K(E \times E))$$

that contains this cocycle .

Let π and π_A be the q-power Frobenius endomorphisms of $E \times E$ and A, respectively. Checking the list of supersingular isogeny classes over odd-degree extensions of finite prime fields of characteristic at least 7 (see [25, Thm. 2.9] or the Appendix), we see that the characteristic polynomial of π_A is $x^4 + bx^2 + q^2$, for some integer b. Let $f \colon E \times E \longrightarrow A$ be a geometric isomorphism such that $\alpha = f^{-1} f^\sigma$. The pullback of π_A by f is $\alpha\pi$, so $\alpha\pi$ also has characteristic polynomial $x^4 + bx^2 + q^2$. From the equalities

$$\pi^2 = -q, \quad \alpha^\sigma \pi = \pi\alpha, \quad \text{and} \quad (\alpha\alpha^\sigma)^2 = -1,$$

we see that we must have $b = 0$, so A lies in the isogeny class $\mathcal{A}_{(0,0)}$.

Lemma 13.7 below shows that there are positive integers r and s such that $pr^2 - 2s^2 = 1$. Let H be the K-endomorphism of $E \times E$ given by

$$H := \begin{bmatrix} pr & s(1+i)\pi \\ -s\pi(1-i) & pr \end{bmatrix} \in \Lambda^{\mathrm{nprinc}},$$

and let $\lambda = \lambda_0 H$ be the corresponding degree-p^2 polarization on $E \times E$, where λ_0 is the product principal polarization on $E \times E$. One checks easily that

$$H = \alpha^\dagger H^\sigma \alpha,$$

where $x \mapsto x^\dagger$ is the Rosati involution on $\mathrm{End}_K(E \times E)$ corresponding to the polarization λ_0, that is, the conjugate-transpose involution. Arguing as in the proof of Proposition 12.5, we see that λ descends to a polarization on A defined over k.

To complete the proof, we need only find a k-rational α_p-subgroup G of A such that $a(A/G) = 1$, for then λ will descend to A/G by Proposition 11.10, and the geometrically non-split principally polarized surface $(A/G, \lambda)$ will be a Jacobian.

By Propositions 11.1 and 12.3 (which is equally valid for q nonsquare) we need only find $[i : j] \in \mathbb{P}^1(K) \backslash \mathbb{P}^1(\mathbb{F}_{p^2})$ such that $[i : j] = \widetilde{\alpha}[i^\sigma : j^\sigma]$. Arguing as in the proof of Proposition 12.4, we see that this is always possible if $q > p^2$. Finally, if $q = p$ not all of the $q + 1$ solutions to $[i : j] = \widetilde{\alpha}[i^\sigma : j^\sigma]$ can be defined over $\mathbb{F}_{p^2}$; in fact, these solutions are fixed points of $\widetilde{\alpha^\sigma\alpha}$, and this transformation would be the identity on $\mathbb{P}^1(\mathbb{F}_{p^2})$. Since $\alpha^\sigma\alpha \in \mathrm{Aut}(H)$, this would imply $\alpha^\sigma\alpha = \pm 1$ by Proposition 11.5, in contradiction with the condition $(\alpha^\sigma\alpha)^2 = -1$. □

Lemma 13.7. — *Let p be a prime that is congruent to* 3 *modulo* 8*. Then there are positive integers r and s such that $pr^2 - 2s^2 = 1$.*

Proof. — Let $F = \mathbb{Q}(\sqrt{2p})$, and let $\mathfrak{p}$ be the prime ideal of F lying over p. Genus theory shows that the class number of F is odd, and since $\mathfrak{p}^2 = (p)$ is principal, we find that $\mathfrak{p}$ is principal as well, say $\mathfrak{p} = (t + s\sqrt{2p})$ for integers t and s that we may take to be positive. Then we have $t^2 - 2ps^2 = \pm p$, so t must be a multiple of p, say $t = pr$. We see that then $pr^2 - 2s^2 = \pm 1$. Considering this equation modulo 8, we find that in fact we must have $pr^2 - 2s^2 = 1$. □

14. Appendix

For the sake of completeness we outline a step-by-step procedure that can be used to check whether a given monic quartic polynomial $f \in \mathbb{Z}[x]$ is the Weil polynomial of a smooth projective genus-2 curve over a finite field $\mathbb{F}_q$. Our main theorem tells when the Weil polynomial for an abelian surface is the Weil polynomial for a Jacobian, so mostly what we must do is identify the Weil polynomials of abelian surfaces. This has been done in other papers ([31] and [25] for example); we are simply restating these results in a convenient form.

Write $q = p^m$ for a prime p.

- *Step 1*: *Check whether f has the right shape for a Weil polynomial.* The complex roots of the Weil polynomial of an abelian variety over $\mathbb{F}_q$ have magnitude $\sqrt{q}$ and come in complex conjugate pairs. A monic quartic polynomial in $\mathbb{Z}[x]$ has this property if and only if it has the shape

$$f = x^4 + ax^3 + bx^2 + qax + q^2,$$

with

$$|a| \leqslant 4\sqrt{q} \quad \text{and} \quad 2|a|\sqrt{q} - 2q \leqslant b \leqslant \frac{a^2}{4} + 2q.$$

- *Step 2*: *Check whether f is the Weil polynomial of an abelian surface.* Suppose f meets the condition of Step 1, and let

$$\Delta = a^2 - 4(b - 2q) \quad \text{and} \quad \delta = (b + 2q)^2 - 4qa^2.$$

  - *Ordinary case*: $v_p(b) = 0$.
    In this case the polynomial f is the Weil polynomial of an ordinary abelian surface over $\mathbb{F}_q$. The surface is split or simple according to Δ being a square in $\mathbb{Z}$ or not.
  - *Almost-ordinary case*: $v_p(a) = 0$ and $v_p(b) > 0$.
    The polynomial f is the Weil polynomial of an almost-ordinary abelian surface if and only if

$$v_p(b) \geqslant m/2 \quad \text{and } \delta \text{ is either 0 or a non-square in } \mathbb{Z}_p.$$

    The surface is split or simple according to Δ being a square in $\mathbb{Z}$ or not.
  - *Supersingular case*: $v_p(a) > 0$ and $v_p(b) > 0$.
    The polynomial f is the Weil polynomial of a supersingular split abelian surface if and only if

$$v_p(a) \geqslant m/2, \quad v_p(b) \geqslant m, \quad \text{and} \quad \Delta \text{ is a square in } \mathbb{Z},$$

    and moreover, if q is a square and we write $a = \sqrt{q}a'$ and $b = qb'$, the following two conditions hold:

$$p \not\equiv 1 \bmod 4, \quad \text{if } b' = 2,$$
$$p \not\equiv 1 \bmod 3, \quad \text{if } a' \not\equiv b' \bmod 2.$$

The polynomial f is the Weil polynomial of a simple supersingular abelian surface if and only if (a,b) belongs to the following list :

(a,b)	**Conditions on p and q**
$(0,0)$	q is a square and $p \not\equiv 1 \bmod 8$, or q is not a square and $p \neq 2$
$(0,-q)$	q is a square and $p \not\equiv 1 \bmod 12$, or q is not a square and $p \neq 3$
$(0,q)$	q is not a square
$(0,-2q)$	q is not a square
$(0,2q)$	q is a square and $p \equiv 1 \bmod 4$
$(\pm\sqrt{q},q)$	q is a square and $p \not\equiv 1 \bmod 5$
$(\pm\sqrt{2q},q)$	q is not a square and $p = 2$
$(\pm 2\sqrt{q},3q)$	q is a square and $p \equiv 1 \bmod 3$
$(\pm\sqrt{5q},3q)$	q is not a square and $p = 5$

- *Step 3*: *Apply Theorem 1.2.* If f is the Weil polynomial of an abelian surface over $\mathbb{F}_q$, one applies Theorem 1.2 to determine if it is the Weil polynomial of a genus-2 curve. Note that in the split case, Δ is a square in $\mathbb{Z}$ and the polynomial $x^2+ax+(b-2q)$ has two roots $s,t \in \mathbb{Z}$, which are the traces of Frobenius of the corresponding elliptic curves.

BIBLIOGRAPHY

[1] G. van der Geer, "Curves over finite fields and codes", in *European Congress of Mathematics, Vol. II* (C. Casacuberta et al., ed.), vol. 202, Progr. Math., Birkhäuser, Basel, 2001, p. 225-238.

[2] G. van der Geer & M. van der Vlugt, "Reed-Muller codes and supersingular curves. I", *Compositio Math.* **84** (1992), p. 333-367.

[3] J. González, J. Guàrdia & V. Rotger, "Abelian surfaces of GL_2-type as Jacobians of curves", *Acta Arith.* **116** (2005), p. 263-287.

[4] R. M. Guralnick & E. W. Howe, "Characteristic polynomials of automorphisms of hyperelliptic curves", arXiv:0804.0578v1 [math.AG]. To appear in the Proceedings of Arithmetic, Geometry, Cryptography, and Coding Theory (AGCT-11), Luminy, 2007.

[5] K. Hashimoto & T. Ibukiyama, "On class numbers of positive definite binary quaternion Hermitian forms. I, II, III", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **27** (1980), p. 549-601, **28** (1981) p. 695–699, **30** (1983) p. 393–401.

[6] D. W. Hoffmann, "On positive definite Hermitian forms", *Manuscripta Math.* **71** (1991), p. 399-429.

[7] E. W. Howe, "Principally polarized ordinary abelian varieties over finite fields", *Trans. Amer. Math. Soc.* **347** (1995), p. 2361-2401.

[8] ———, "Kernels of polarizations of abelian varieties over finite fields", *J. Algebraic Geom.* **5** (1996), p. 583-608.

[9] ———, "Isogeny classes of abelian varieties with no principal polarizations", in *Moduli of abelian varieties* (G. Faber, C. and van der Geer & F. Oort, eds.), vol. 195, Progr. Math., Birkhäuser, Basel, 2001, p. 203-216.

[10] ———, "On the non-existence of certain curves of genus two", *Compos. Math.* **140** (2004), p. 581-592.

[11] ———, "Supersingular genus-2 curves over fields of characteristic 3", *Computational Algebraic Geometry (K. E. Lauter and K. A. Ribet, eds.), Contemp. Math.* **463** (2008), p. 49-69, American Mathematical Society, Providence, RI.

[12] E. W. Howe & K. E. Lauter, "Improved upper bounds for the number of points on curves over finite fields", *Ann. Inst. Fourier (Grenoble)* **53** (2003), p. 1677-1737.

[13] E. W. Howe, F. Leprévost & B. Poonen, "Large torsion subgroups of split Jacobians of curves of genus two or three", *Forum Math.* **12** (2000), p. 315-364.

[14] E. W. Howe, D. Maisner, E. Nart & C. Ritzenthaler, "Principally polarizable isogeny classes of abelian surfaces over finite fields", *Math. Res. Lett.* **15** (2008), p. 121-127.

[15] T. Ibukiyama, "On automorphism groups of positive definite binary quaternion Hermitian lattices and new mass formula", in *Automorphic forms and geometry of arithmetic varieties* (K. Hashimoto and Y. Namikawa, ed.), vol. 15, Adv. Stud. Pure Math., Academic Press, Boston, MA, 1989, p. 301-349.

[16] T. Ibukiyama, T. Katsura & F. Oort, "Supersingular curves of genus two and class numbers", *Compositio Math.* **57** (1986), p. 127-152.

[17] J.-i. Igusa, "Arithmetic variety of moduli for genus two", *Ann. of Math. (2)* **72** (1960), p. 612-649.

[18] H. Ito, "On the number of rational cyclic subgroups of elliptic curves over finite fields", *Mem. College Ed. Akita Univ. Natur. Sci.* (1990), no. 41, p. 33-42.

[19] E. Kani, "The number of curves of genus two with elliptic differentials", *J. Reine Angew. Math.* **485** (1997), p. 93-121.

[20] T. Katsura & F. Oort, "Families of supersingular abelian surfaces", *Compositio Math.* **62** (1987), p. 107-167.

[21] K. Lauter, "Non-existence of a curve over $\mathbb{F}_3$ of genus 5 with 14 rational points", *Proc. Amer. Math. Soc.* **128** (2000), p. 369-374.

[22] K. Lauter with an appendix by J.-P. Serre, "The maximum or minimum number of rational points on genus three curves over finite fields", *Compositio Math.* **134** (2002), p. 87-111.

[23] D. Maisner, *Superficies abelianas como jacobianas de curvas en cuerpos finitos*, Memoir, Universitat Autònoma de Barcelona, 2004.

[24] D. Maisner & E. Nart, "Zeta functions of supersingular curves of genus 2", *Canad. J. Math.* **59** (2007), p. 372-392.

[25] D. Maisner & W. Nart with an appendix by E. W. Howe, "Abelian surfaces over finite fields as Jacobians", *Experiment. Math.* **11** (2002), p. 321-337.

[26] G. McGuire & J. F. Voloch, "Weights in codes and genus 2 curves", *Proc. Amer. Math. Soc.* **133** (2005), p. 2429-2437.

[27] J. S. Milne, "Abelian varieties", Arithmetic geometry, p. 103-150, Arithmetic geometry, Springer-Verlag, New York, G. Cornell and J. H. Silverman ed., 1986.

[28] T. Oda, "The first de Rham cohomology group and Dieudonné modules", *Ann. Sci. École Norm. Sup.* **2** (1969), no. 4, p. 63-135.

[29] F. Oort, “Which abelian surfaces are products of elliptic curves?”, *Math. Ann.* **214** (1975), p. 35-47.

[30] I. Reiner, *Maximal orders*, (corrected reprint of the 1975 original), London Math. Soc. Monogr. (N.S.), vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003.

[31] H.-G. Rück, “Abelian surfaces and Jacobian varieties over finite fields”, *Compositio Math.* **76** (1990), p. 351-366.

[32] R. Schoof, “Nonsingular plane cubic curves over finite fields”, *J. Combin. Theory Ser. A* **46** (1987), p. 183-211.

[33] J.-P. Serre, *Cohomologie Galoisienne*, (fifth edition), Lecture Notes in Math., vol. 5, Springer-Verlag, Berlin, 1994.

[34] G. Shimura, “Arithmetic of alternating forms and quaternion hermitian forms”, *J. Math. Soc. Japan* **15** (1963), p. 33-65.

[35] J. Tate, “Endomorphisms of abelian varieties over finite fields”, *Invent. Math.* **2** (1966), p. 134-144.

[36] ———, “Classes d’isogénie des variétés abéliennes sur un corps fini (d’après T. Honda), Exp. 352”, in *Séminaire Bourbaki vol. 1968/69 Exposés 347–363* (Berlin-New York), Lecture Notes in Math., vol. 179, Springer-Verlag, 1971, p. 95-110.

[37] W. C. Waterhouse, “Abelian varieties over finite fields”, *Ann. Sci. École Norm. Sup.* **2** (1969), no. 4, p. 521-560.

Manuscrit reçu le 9 août 2007,
accepté le 16 mai 2008.

Everett W. HOWE
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1967 (USA)
however@alumni.caltech.edu

Enric NART
Universitat Autònoma de Barcelona
Departament de Matemàtiques
Edifici C
08193 Bellaterra, Barcelona (Spain)
nart@mat.uab.cat

Christophe RITZENTHALER
Institut de Mathématiques de Luminy
UMR 6206 du CNRS
Luminy, Case 907
13288 Marseille (France)
ritzenth@iml.univ-mrs.fr