Journal of Pure and Applied Algebra 223 (2019) 3031–3056

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

Fully maximal and fully minimal abelian varieties ☆

Valentijn Karemaker [a,*], Rachel Pries [b]

[a] Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104, USA
[b] Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA

ARTICLE INFO

Article history:
Received 2 November 2017
Received in revised form 13 August 2018
Available online 4 October 2018
Communicated by I.M. Duursma

MSC:
Primary: 11G10; 11G20; 11M38; 14H37; 14H45; secondary: 11G25; 14G15; 14H40; 14K10; 14K15

Keywords:
Abelian variety
Curve
Supersingular
Maximal
Zeta function
Weil number

ABSTRACT

We introduce and study a new way to categorize supersingular abelian varieties defined over a finite field by classifying them as *fully maximal*, *mixed* or *fully minimal*. The type of A depends on the normalized Weil numbers of A and its twists. We analyze these types for supersingular abelian varieties and curves under conditions on the automorphism group. In particular, we present a complete analysis of these properties for supersingular elliptic curves and supersingular abelian surfaces in arbitrary characteristic, and for a one-dimensional family of supersingular curves of genus 3 in characteristic 2.

1. Introduction

Suppose that X is a smooth projective connected curve of genus $g \geq 1$ defined over a finite field $\mathbb{F}_q$ of characteristic p; write $q = p^r$. The curve X is *supersingular* if the only slope of the Newton polygon of its L-polynomial is $\frac{1}{2}$ or, equivalently, if its normalized Weil numbers are all roots of unity. If $p = 2$, there exists a supersingular curve over $\mathbb{F}_2$ of every genus [42]. If p is odd, it is not known whether there exists a supersingular curve over $\overline{\mathbb{F}}_p$ of every genus. One says that X is *minimal* (resp. *maximal*) over $\mathbb{F}_{q^m}$ if the number of $\mathbb{F}_{q^m}$-points of X realizes the lower (resp. upper) bound in the Hasse–Weil theorem.

☆ Karemaker was partially supported by The Netherlands Organisation for Scientific Research (NWO) through the "Geometry and Quantum Theory" research cluster. Pries was partially supported by NSF grant DMS-15-02227. The authors thank Jeff Achter, Gunther Cornelissen, Frans Oort, Christophe Ritzenthaler, Jeroen Sijsling, Andrew Sutherland, and some referees for helpful comments.

* Corresponding author.
E-mail addresses: vkarem@math.upenn.edu (V. Karemaker), pries@math.colostate.edu (R. Pries).

https://doi.org/10.1016/j.jpaa.2018.10.007
0022-4049/

More generally, suppose that A is a principally polarized abelian variety of dimension $g \geq 1$ defined over $\mathbb{F}_q$. Then A is *supersingular* if the only slope of its p-divisible group $A[p^\infty]$ is $\frac{1}{2}$ or, equivalently, if its normalized Weil numbers are all roots of unity. One says that A is *minimal* (resp. *maximal*) over $\mathbb{F}_{q^m}$ if Frobenius acts on its ℓ-adic Tate module by multiplication by $\sqrt{q^m}$ (resp.-$\sqrt{q^m}$). In fact, A (resp. X) is supersingular if and only if it is minimal over some finite extension of $\mathbb{F}_q$.

Because of applications to cryptosystems and error-correcting codes, there are many papers in the literature about maximal curves but relatively few papers about minimal curves. This led to the motivating question: is a supersingular curve $X/\mathbb{F}_q$ more likely to be maximal or minimal? However, this question is not well-posed, since X may be neither until after a finite field extension. To resolve this, one says that $X/\mathbb{F}_q$ has parity 1 if it is maximal after a finite extension of $\mathbb{F}_q$, and parity -1 otherwise, cf. Definition 4.1. The proportion of supersingular elliptic curves with parity 1 can be determined using [32] (Remark 6.2), but the analogous question for curves of higher genus and abelian varieties of higher dimension is more difficult to answer, since the sizes of the isogeny classes are not known.

In this paper, we address a related question about supersingular curves and abelian varieties, based on the fact that most of the supersingular curves found in the literature have non-trivial automorphism groups and twists. The twists of $X/\mathbb{F}_q$ may have different arithmetic properties. Specifically, it is possible that $X/\mathbb{F}_q$ is not maximal over any extension of $\mathbb{F}_q$ but that it has a twist which is maximal over some extension of $\mathbb{F}_q$. From a geometric perspective, there is no reason to prefer one twist over another.

The following definition addresses this subtlety. Suppose that $X/\mathbb{F}_q$ is a supersingular curve or abelian variety. We define X to be (i) *fully maximal*, (ii) *fully minimal*, (iii) *mixed* over $\mathbb{F}_q$ if (i) all, (ii) none, or (iii) some (but not all) of its $\mathbb{F}_q$-twists have the property that they are maximal over some finite extension of $\mathbb{F}_q$ (Definitions 4.2, 5.2). The type of X depends on its geometric automorphism group, its field of definition, and the normalized Weil numbers of its twists, leading to a fascinating interaction between algebra, geometry, and arithmetic.

It is a natural question to ask: under what conditions is a supersingular curve or abelian variety fully maximal, fully minimal, or mixed over $\mathbb{F}_q$? We answer this question for dimension $g = 1$ in Section 6, proving that a supersingular elliptic curve is fully maximal over $\mathbb{F}_p$ if its j-invariant is in $\mathbb{F}_p$ and is mixed over $\mathbb{F}_{p^2}$ otherwise (Theorem 6.3). When $g = 2$ and p is odd, in Section 7, we give a complete analysis of the three types for simple supersingular abelian surfaces A; in particular, for $A/\mathbb{F}_{p^r}$ with $\mathrm{Aut}_{\bar{\mathbb{F}}_p}(A) \simeq \mathbb{Z}/2\mathbb{Z}$, then A is not mixed over $\mathbb{F}_{p^r}$ if r is odd and A is not fully minimal over $\mathbb{F}_{p^r}$ if r is even (Proposition 7.2).

The results in Sections 6–7 depend on theoretical results in earlier sections which hold for all g and p. Section 2 introduces supersingular abelian varieties and curves. Section 3 contains information about twists, including the bijection between twists of $A/\mathbb{F}_q$ and $\mathbb{F}_q$-Frobenius conjugacy classes of $\mathrm{Aut}_{\bar{\mathbb{F}}_p}(A)$ (Proposition 3.5) and the effect of twists on the relative Frobenius endomorphism (Proposition 3.9).

In Section 4, we study supersingular abelian varieties of arbitrary dimension g. We characterize the fully maximal, fully minimal, and mixed types in terms of arithmetic properties of the normalized Weil numbers of $A/\mathbb{F}_q$. These are roots of unity; the key ingredient for the analysis is the 2-divisibility of their orders, encoded in a multiset $\underline{e}(A/\mathbb{F}_q)$ (Definition 4.4). As an application, we show that A is not fully minimal over $\mathbb{F}_{p^r}$ if A is simple and r is even (Proposition 4.7). We give a complete characterization of the three types under the hypothesis that $|\mathrm{Aut}_{\bar{\mathbb{F}}_p}(A)| = 2$ (Corollary 4.8), and a criterion for the mixed case in terms of the orders of the twists and $\underline{e}(A/\mathbb{F}_q)$ (Corollary 4.13).

In Section 5, we define the three types for a supersingular curve X. If $s \equiv 0 \bmod 4$ and $p \equiv -1 \bmod s$, we prove that the smooth plane curve $X/\mathbb{F}_p$ with equation $x^s + y^s + z^s = 0$ is supersingular and of mixed type over $\mathbb{F}_p$ (Proposition 5.6). In Section 5.3, we study which automorphisms yield parity-changing twists.

Most of the supersingular curves found in the literature are constructed using Artin–Schreier theory. In many cases, the automorphism groups and normalized Weil numbers of these Artin–Schreier curves are known, e.g., in [41] and [2]. An open problem is to determine when these curves are fully maximal, fully minimal, or mixed. As a result in this direction, we end the paper in Section 8 by studying a one-dimensional

family of supersingular curves X of genus 3 in characteristic 2, which are $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$-Galois covers of the projective line. For $X/\mathbb{F}_{2^r}$, we prove that X is fully minimal if $r \equiv 0 \bmod 4$, X is fully minimal or mixed (with about equal probability) if $r \equiv 2 \bmod 4$, and X is fully maximal or mixed (with about equal probability) if r is odd (Theorem 8.1).

2. Background: supersingular abelian varieties and Weil numbers

Let $k = \overline{\mathbb{F}}_p$. Let A be an abelian variety of dimension $g \geq 1$, a priori defined over k. Throughout the paper, we assume A is defined over a finite field $K = \mathbb{F}_q$ of cardinality $q = p^r$. We write K instead of $\mathrm{Spec}(K)$ when this causes no ambiguity.

2.1. Frobenius and its characteristic polynomial

Definition 2.1. [30, 21.2] Consider the generator $Fr_K : \alpha \to \alpha^q$ of the absolute Galois group $G_K = \mathrm{Gal}(k/K)$ of K. If R is a K-algebra and $U = \mathrm{Spec}(R)$, then the map which sends $x \mapsto x^q$ for $x \in R$ induces a Frobenius map f_U on U. The *absolute Frobenius endomorphism* $f_A \colon A \to A$ of A/K is the gluing of f_U over all open affine subschemes U of A.

For a morphism of K-schemes $A \to S$, let $A^{(p)}$ be the fiber product of $A \to S \xleftarrow{f_S} S$. The morphism f_A factors through $A^{(p)}$; this defines a morphism $\pi = \pi_A \colon A \to A^{(p)}$ called the *relative Frobenius endomorphism.* Then

$$\pi_A = f_A \otimes Fr_K^{-1}. \tag{1}$$

By [39, pages 135–138], for any $\ell \neq p$, there is a bijection

$$\mathrm{End}_K(A) \otimes \mathbb{Q}_\ell \to \mathrm{End}_{G_K}(T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell), \tag{2}$$

where $T_\ell(A)$ denotes the ℓ-adic Tate module of A. Via this bijection, π_A can be viewed as a linear operator on $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Since π_A is semisimple (cf. [39, page 138]), this linear operator is diagonalizable over $\overline{\mathbb{Q}}_\ell$. Moreover, the characteristic polynomial $P(A/K, T)$ of π_A (in the sense of [21, page 110]) coincides with that of its corresponding linear operator, by e.g., [21, Chapter VII, Theorem 3].

2.2. Weil numbers and zeta functions

The characteristic polynomial $P(A/\mathbb{F}_q, T)$ of π_A is a monic polynomial in $\mathbb{Z}[T]$ of degree $2g$. Writing $P(A/\mathbb{F}_q, T) = \prod_{i=1}^{2g}(T - \alpha_i)$, the roots $\alpha_i \in \overline{\mathbb{Q}}$ all satisfy $|\alpha_i| = \sqrt{q}$.

Definition 2.2. The roots $\{\alpha_1, \ldots, \alpha_{2g}\} = \{\alpha_1, \bar{\alpha}_1, \ldots, \alpha_g, \bar{\alpha}_g\}$ of $P(A/\mathbb{F}_q, T)$ are the *Weil numbers* of A. The *normalized Weil numbers* of $A/\mathbb{F}_q$ are $\mathrm{NWN}(A/\mathbb{F}_q) = \{z_1, \bar{z}_1, \ldots, z_g, \bar{z}_g\}$, where $z_i = \frac{\alpha_i}{\sqrt{q}}$.

In writing the normalized Weil numbers, we use the convention that $\zeta_n = e^{2\pi i/n}$.

Theorem 2.3. *[27, Chapter II, Section 1], [6, Theorem 1.6], [46, §IX, 71] The zeta function of A over $\mathbb{F}_q$ satisfies*

$$Z(A/\mathbb{F}_q, T) := \exp\left(\sum_{m \geq 1} |A(\mathbb{F}_{q^m})| \frac{T^m}{m}\right) = \frac{P_1(T) \cdot \ldots \cdot P_{2g-1}(T)}{P_0(T) P_2(T) \cdot \ldots \cdot P_{2g-2}(T) P_{2g}(T)},$$

where $P_s(T) \in \mathbb{Z}[T]$ *and* $P_s(T) = \prod_{\sigma \in S_s}(1 - \alpha_\sigma T)$ *where* S_s *is the set of subsets* $\sigma = \{i_1, \ldots, i_s\}$ *of* $\{1, \ldots, 2g\}$ *of cardinality* s *and* $\alpha_\sigma = \alpha_{i_1}\alpha_{i_2} \cdot \ldots \cdot \alpha_{i_s}$.

Note that $P(A/\mathbb{F}_q, T) = T^{2g}P_1(T^{-1})$. The polynomials $P_i(T)$ describe the action of Frobenius on the i-th étale cohomology of $A/\mathbb{F}_q$. By [39, Theorem 1], two abelian varieties A_1 and A_2 over $\mathbb{F}_q$ have the same zeta function if and only if $P(A_1/\mathbb{F}_q, T) = P(A_2/\mathbb{F}_q, T)$, which holds if and only if A_1 and A_2 are isogenous over $\mathbb{F}_q$.

Corollary 2.4. *[27, Chapter II, Theorem 1.1] The number of* $\mathbb{F}_q$*-points of* A *satisfies*

$$|A(\mathbb{F}_q)| = \deg(\pi_{A/\mathbb{F}_q} - \mathrm{id}) = P(A/\mathbb{F}_q, 1) = \prod_{i=1}^{2g}(1 - \alpha_i); \text{ and thus}$$
$$||A(\mathbb{F}_q)| - q^g| \leq 2gq^{(g-\frac{1}{2})} + (2^{2g} - 2g - 1)q^{(g-1)}.$$

2.3. Zeta functions of curves

Let X be a smooth projective connected curve of genus g defined over $\mathbb{F}_q$.

Theorem 2.5. *[45, §IV, 22], [46, §IX, 69] The zeta function of* $X/\mathbb{F}_q$ *can be written as*

$$Z(X/\mathbb{F}_q, T) = \frac{L(X/\mathbb{F}_q, T)}{(1 - T)(1 - qT)}$$

where the L-polynomial $L(X/\mathbb{F}_q, T) \in \mathbb{Z}[T]$ *of* $X/\mathbb{F}_q$ *has degree* $2g$ *and factors as*

$$L(X/\mathbb{F}_q, T) = \prod_{i=1}^{2g}(1 - \alpha_i T).$$

Then $P(\mathrm{Jac}(X)/\mathbb{F}_q, T) = T^{2g}L(X/\mathbb{F}_q, T^{-1})$ is the characteristic polynomial of $\pi_{\mathrm{Jac(X)}}$. The (normalized) *Weil numbers* of X are the (normalized) roots of $P(\mathrm{Jac}(X)/\mathbb{F}_q, T)$.

Corollary 2.6. *Let* $\{\alpha_1, \bar{\alpha}_1, \ldots, \alpha_g, \bar{\alpha}_g\}$ *be the Weil numbers of* X*. The number of* $\mathbb{F}_q$*-points of* X *satisfies* $|X(\mathbb{F}_q)| = q + 1 - \sum_{i=1}^{g}(\alpha_i + \bar{\alpha}_i)$*, which implies the Hasse–Weil bound:*

$$||X(\mathbb{F}_q)| - (q + 1)| \leq 2g\sqrt{q}.$$

2.4. Supersingular abelian varieties and curves

Definition 2.7. An abelian variety A is *supersingular* if the only slope of the p-divisible group $A[p^\infty]$ is $\frac{1}{2}$. A curve X is *supersingular* if its Jacobian $\mathrm{Jac}(X)$ is supersingular.

Theorem 2.8. *Suppose that* $A/\mathbb{F}_q$ *is an abelian variety of dimension* g*. The following properties are each equivalent to* A *being supersingular:*

(1) *the (q-normalized) Newton polygon of* $P(A/\mathbb{F}_q, T)$ *is a line segment of slope* $\frac{1}{2}$*;*
(2) A *is geometrically isogenous to a product of supersingular elliptic curves, i.e.,* $A \times_{\mathbb{F}_q} k \sim E^g \times_{\mathbb{F}_q} k$ *for an elliptic curve* E *such that* $E[p](k) = \{0\}$*, [29, Theorem 4.2];*
(3) *the formal group of* A *is geometrically isogenous to* $(G_{1,1})^g$*, [23, Section 1.4];*
(4) *the normalized Weil numbers of* $A/\mathbb{F}_q$ *are roots of unity, [25, Theorem 4.1].*

2.5. Maximal and minimal

Definition 2.9. An abelian variety $A/\mathbb{F}_q$ or a curve $X/\mathbb{F}_q$ is *maximal* (resp. *minimal*) if its normalized Weil numbers all equal -1 (resp. 1).

By Corollaries 2.4 or 2.6, $|A(\mathbb{F}_q)|$ or $|X(\mathbb{F}_q)|$ realizes its upper (resp. lower) bound exactly when A or X is maximal (resp. minimal). A necessary condition for maximality or minimality is that q is a square (i.e., r is even), by Theorem 2.3 or 2.5. Also $X/\mathbb{F}_q$ is maximal (resp. minimal) if and only if $L(X/\mathbb{F}_q, T) = (1+\sqrt{q}T)^{2g}$ (resp. $(1-\sqrt{q}T)^{2g}$).

The following facts are well-known and hold for curves as well as for abelian varieties, cf. [43, Theorem 1.9] and [37, Theorem V.1.15(f)].

Lemma 2.10.

(1) *If* $P(A/\mathbb{F}_q, T) = \prod_{i=1}^{2g}(T-\alpha_i)$, *then* $P(A/\mathbb{F}_{q^m}, T) = \prod_{i=1}^{2g}(T-\alpha_i^m)$.
(2) *If* $A/\mathbb{F}_q$ *is minimal or maximal, then it is supersingular. Conversely, if* $A/\mathbb{F}_q$ *is supersingular, then it is minimal over some finite extension of* $\mathbb{F}_q$.
(3) (a) *If* $A/\mathbb{F}_q$ *is maximal, then* $A/\mathbb{F}_{q^m}$ *is maximal for odd* m *and minimal for even* m.
    (b) *If* $A/\mathbb{F}_q$ *is minimal, then* $A/\mathbb{F}_{q^m}$ *is minimal for all* $m \in \mathbb{N}$.

3. Twists

Let $K = \mathbb{F}_q$ with $q = p^r$ and let $k = \overline{\mathbb{F}}_p$. For $m \in \mathbb{N}$, let K_m be the unique extension of K of degree m. Let Fr_K be the generator of $G_K = \mathrm{Gal}(k/K)$ as in Definition 2.1.

In this section, we review the theory of twists of abelian varieties following [34] and [5].

3.1. Twists, cocycles, and Frobenius conjugacy classes

Let A/K be a principally polarized abelian variety of dimension $g \geq 1$. We restrict to automorphisms of A that are compatible with the principal polarization λ. For ease of notation, we write A instead of (A, λ) and $\mathrm{Aut}_k(A)$ instead of $\mathrm{Aut}_k(A, \lambda)$.

Definition 3.1. A (K-)*twist* of A/K is an abelian variety A'/K for which there exists a geometric isomorphism

$$\phi : \bar{A} \xrightarrow{\simeq} \bar{A}', \tag{3}$$

where $\bar{A} = A \times_K k$ and $\bar{A}' = A' \times_K k$. A twist A'/K is *trivial* if $A \simeq_K A'$. Let $\Theta(A/K)$ denote the set of K-isomorphism classes of twists A'/K of A/K.

Definition 3.2. Given $\sigma \in G_K$ and $\phi : \bar{A} \xrightarrow{\simeq} \bar{A}'$, let ${}^{\sigma}\phi \colon \bar{A} \xrightarrow{\simeq} \bar{A}'$ denote the (twisted) isomorphism which acts on $x \in \bar{A}(k)$ via ${}^{\sigma}\phi(x) = \sigma(\phi(\sigma^{-1}(x)))$ or, more precisely, via

$${}^{\sigma}\phi = (\mathrm{id}_{A'} \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\sigma)) \circ \phi \circ (\mathrm{id}_A \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\sigma))^{-1}.$$

Similarly, if $A' = A$ and $\tau \in \mathrm{Aut}_k(A)$, let ${}^{Fr_K}\tau$ denote the (twisted) automorphism, which acts on $x \in \bar{A}(k)$ by

$${}^{Fr_K}\tau(x) = Fr_K(\tau(Fr_K^{-1}(x))).$$

Definition 3.3. Two automorphisms $g, h \in \mathrm{Aut}_k(A)$ are *K-Frobenius conjugate* if there exists $\tau \in \mathrm{Aut}_k(A)$ such that

$$g = \tau^{-1} h ({}^{Fr_K}\tau).$$

In particular, g is K-Frobenius conjugate to id if $g = \tau^{-1}({}^{Fr_K}\tau)$ for some $\tau \in \mathrm{Aut}_k(A)$.

Remark 3.4. If all automorphisms of A are defined over K, then G_K acts trivially on $\mathrm{Aut}_k(A)$. (By [39, Theorem 2(d)], this is true if A is maximal or minimal over K.) In this case, the K-Frobenius conjugacy classes are the same as standard conjugacy classes.

Proposition 3.5. *[34, Proposition III.5], [33, Proposition 1], (see also [26, Propositions 5,9] for curves) Given $\phi : \bar{A} \xrightarrow{\simeq} \bar{A}'$ as in (3), consider the cocycle $\xi_\phi \colon G_K \to \mathrm{Aut}_k(A)$ defined by*

$$\xi_\phi(\sigma) = \phi^{-1} \circ {}^{\sigma}\phi. \tag{4}$$

Next, for any $\xi \in C^1(G_K, \mathrm{Aut}_k(A))$, let

$$g_\xi = \xi(Fr_K) \in \mathrm{Aut}_k(A). \tag{5}$$

The maps taking $\phi \mapsto \xi_\phi \mapsto g_\phi := g_{\xi_\phi}$ yield bijections:

$$\Theta(A/K) \to H^1(G_K, \mathrm{Aut}_k(A)) \to \{K\text{-Frobenius conjugacy classes of } \mathrm{Aut}_k(A)\}. \tag{6}$$

Given $g \in \mathrm{Aut}_k(A)$, let $\xi_g \in C^1(G_K, \mathrm{Aut}_k(A))$ be the cocycle such that $\xi_g(Fr_K) = g$ and let $\phi_g : \bar{A} \xrightarrow{\simeq} \bar{A}'$ be such that $\xi_{\phi_g} = \xi_g$. Note that ϕ_g is not uniquely determined: if $\tau \in \mathrm{Aut}_k(A)$ is such that $\tau^{-1} g \, {}^{Fr_K}\tau = g$, then $\phi' = \phi_g \circ \tau : \bar{A} \xrightarrow{\simeq} \bar{A}'$ also has the property that $\xi_{\phi'} = \xi_g$. In this case, τ is defined over K, so $\phi \circ \tau$ and ϕ have the same field of definition.

Definition 3.6. The *order* of a twist A'/K is the smallest $m \in \mathbb{N}$ such that over the degree m extension K_m of K there exists an isomorphism $\phi : A \times_K K_m \xrightarrow{\simeq} A' \times_K K_m$.

If A'/K is a twist of order m and $\phi : \bar{A} \xrightarrow{\simeq} \bar{A}'$ is an isomorphism, then Definition 3.6 implies that $\phi \circ \tau$ is defined over the degree m extension K_m of K for some $\tau \in \mathrm{Aut}_k(A)$.

Remark 3.7. If $T \in \mathbb{N}$, then

$$\xi_g(Fr_K^T) = g({}^{Fr_K}g)({}^{Fr_K^2}g) \cdots ({}^{Fr_K^{T-1}}g). \tag{7}$$

Given $\phi : \bar{A} \xrightarrow{\simeq} \bar{A}'$, write $g := g_\phi$ and let T_g be the smallest $T \in \mathbb{N}$ such that $\xi_g(Fr_K^T) = \mathrm{id}$. Then T_g is the degree of the field of definition of ϕ over K.

Lemma 3.8. *Let c_g be the smallest $c \in \mathbb{N}$ such that $\xi_g(Fr_K^c)$ is defined over K_c. Then c_g divides T_g and T_g/c_g equals the order of $G := g({}^{Fr_K}g)({}^{Fr_K^2}g) \cdots ({}^{Fr_K^{c_g-1}}g)$.*

Proof. When $c_g = 1$, the result is immediate, since g is defined over K and $G = g$.

Now suppose that $c_g > 1$. By Remark 3.7, the twist is an element A' of the set $\Theta(A, K_{T_g}/K)$ of twists A'/K of A/K such that $A \times_K K_{T_g} \simeq_{K_{T_g}} A' \times_K K_{T_g}$. The bijection $\theta \colon \Theta(A, K_{T_g}/K) \to H^1(\mathrm{Gal}(K_{T_g}/K), \mathrm{Aut}_{K_{T_g}}(A))$ from [34, Proposition III.5] shows that A' corresponds to the automorphism $\xi_g(Fr_K) = g$ in $\mathrm{Aut}_{K_{T_g}}(A)$. It follows that g (and thus G) is defined over K_{T_g}. Hence, $K_{c_g} \subset K_{T_g}$ and $c_g | T_g$.

The base changes $A_{c_g} = A \times_K K_{c_g}$ and $A'_{c_g} = A' \times_K K_{c_g}$ first become isomorphic over $K_{T_g} K_{c_g} = K_{T_g}$. So ϕ is defined over an extension of K_{c_g} of degree $T' = [K_{T_g} : K_{c_g}] = T_g/c_g$. The automorphism corresponding to the twist over K_{c_g} is G. Hence, replacing g by G, the conclusion follows from the case when $c_g = 1$. □

3.2. Effect of a twist on the Frobenius endomorphism

In this section, let K_c be a finite field and suppose A is defined over K_c and $G \in \mathrm{Aut}_{K_c}(A)$. The notation is chosen to be compatible with Lemma 3.8: one can consider $c = c_g$ and K_c the unique extension of K of degree c, and G as in Lemma 3.8. We study how twisting A/K_c by G affects the relative Frobenius endomorphism $\pi = \pi_A \in \mathrm{End}_{K_c}(A)$ of A and the normalized Weil numbers of A over K_c.

Proposition 3.9. *Suppose that A is defined over K_c and that $\phi : A \times_{K_c} k \xrightarrow{\simeq} A' \times_{K_c} k$ is a geometric isomorphism. Suppose that $G_\phi = \xi_\phi(Fr_{K_c})$ is in $\mathrm{Aut}_{K_c}(A)$. Then the relative Frobenius endomorphism π' of A' satisfies*

$$\phi^{-1} \circ \pi' \circ \phi = \pi_A \circ G_\phi^{-1}. \tag{8}$$

Remark 3.10. The right hand side of (8) is defined over K_c, so the left hand side is as well. In particular, π' and $\pi_A \circ G_\phi^{-1}$ have the same characteristic polynomial.

Proof. Let $f' = f_{A'}$ be the absolute Frobenius endomorphism of A'. By (1), $\pi_A = f_A \otimes Fr_{K_c}^{-1}$ and $\pi' = f_{A'} \otimes Fr_{K_c}^{-1}$. Also, $f = \phi^{-1} \circ f' \circ \phi$. Furthermore, by (4),

$$G_\phi^{-1} = (\mathrm{id}_A \otimes Fr_{K_c}) \circ \phi^{-1} \circ (\mathrm{id}_A \otimes Fr_{K_c}^{-1}) \circ \phi.$$

Hence, as in [26, Proposition 11],

$$\begin{aligned}
\phi^{-1} \circ \pi' \circ \phi &= \phi^{-1} \circ \left(f' \otimes Fr_{K_c}^{-1}\right) \circ \phi \\
&= \phi^{-1} \circ \left(\left(\phi \circ f \circ \phi^{-1}\right) \otimes Fr_{K_c}^{-1}\right) \circ \phi \\
&= \left(f \otimes Fr_{K_c}^{-1}\right) \circ (\mathrm{id}_A \otimes Fr_{K_c}) \circ \phi^{-1} \circ \left(\mathrm{id}_A \otimes Fr_{K_c}^{-1}\right) \circ \phi \\
&= \pi_A \circ G_\phi^{-1}. \quad \square
\end{aligned}$$

3.3. Twists by automorphisms of order 2

Lemma 3.11. *Given $\phi : \bar{A} \xrightarrow{\simeq} \bar{A}'$, if $g_\phi \in \mathrm{Aut}_K(A)$ has order 2, then the twist A'/K is either quadratic or trivial. It is trivial if and only if g_ϕ is K-Frobenius conjugate to* id.

Proof. Write $g = g_\phi$. By hypothesis, $c_g = 1$, so by Lemma 3.8, $T_g = |g| = 2$. By Definition 3.6, the order of the twist is at most 2. The last statement follows from Proposition 3.5. □

The conclusion of Lemma 3.11 can be false if g_ϕ is not defined over K.

Definition 3.12. Let $\iota \in \mathrm{End}_K(A) \otimes \mathbb{Q}_\ell$ correspond to $[-1] \in \mathrm{End}_{G_K}(T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$ under the bijection in (2). Let A_ι denote the K-twist of A for ι.

Note that ι is defined over K and central in $\mathrm{Aut}_k(A)$. By Lemma 3.11, A_ι/K is either a trivial or a quadratic twist.

By Proposition 3.9, if A/K is maximal, then A_ι/K is minimal, and vice versa. Conversely, the next result shows that ι is the only automorphism whose twist can switch between the maximal and minimal conditions. We generalize this result in Corollary 4.13.

Proposition 3.13. *Suppose that $\phi : A \times_K k \xrightarrow{\simeq} A' \times_K k$ where A/K is maximal and A'/K is minimal (or vice versa). Then $g_\phi = \iota$ and $A'/K \simeq A_\iota/K$ is a quadratic twist of A/K.*

Proof. By Definition 2.9, $P(A/K, T)$ and $P(A'/K, T)$ split completely into linear factors over $\mathbb{Q}$. Thus the linear operators corresponding to π_A and $\pi_{A'}$ under (2) are diagonalizable over $\mathbb{Q}_\ell$. So $\pi_A = \sqrt{q} \cdot \iota$ and $\pi_{A'} = \sqrt{q} \cdot \mathrm{id}$ in $\mathrm{End}_K(A) \otimes \mathbb{Q}_\ell$. By Proposition 3.9, this implies that $g_\phi = \xi_\phi(Fr_K)$ is K-Frobenius conjugate to ι. So $g_\phi = \tau^{-1} \iota \, {}^{Fr_K}\tau$ for some $\tau \in \mathrm{Aut}_k(A)$.

Since A/K is maximal, $\mathrm{Aut}_k(A) = \mathrm{Aut}_K(A)$ [39, Theorem 2d]. In particular, ${}^{Fr_K}\tau = \tau$. Because ι is central in $\mathrm{Aut}_k(A)$, the K-Frobenius conjugacy class of ι consists of one element. Thus $g_\phi = \iota$ and $A'/K \simeq A_\iota/K$. Moreover, ι satisfies the conditions of Lemma 3.11. Since $A \not\simeq_K A'$, the twist A'/K is nontrivial and thus quadratic. □

4. Fully maximal, fully minimal, and mixed abelian varieties

Let $K = \mathbb{F}_q$ with $q = p^r$ and let $k = \overline{\mathbb{F}}_p$. Let A be a principally polarized supersingular abelian variety of dimension $g \geq 1$ defined over K. Let $\mathrm{NWN}(A/K) = \{z_1, \bar{z}_1, \ldots, z_g, \bar{z}_g\}$ be the normalized Weil numbers of A/K, as in Definition 2.2.

4.1. Period, parity, and types

Definition 4.1.

(1) The $\mathbb{F}_q$-*period* $\mu(A)$ of A is the smallest $m \in \mathbb{N}$ such that q^m is square and
   (i) $z_i^m = -1$ for all $1 \leq i \leq g$, or
   (ii) $z_i^m = 1$ for all $1 \leq i \leq g$.

(2) The $\mathbb{F}_q$-*parity* $\delta(A)$ is 1 in case (i) and is -1 in case (ii).

In other words, the period is the smallest $m \in \mathbb{N}$ such that $\pi_{A/\mathbb{F}_{q^m}} \in \mathbb{Q}$ and $\pi_{A/\mathbb{F}_{q^m}} = \sqrt{q^m}$ or $-\sqrt{q^m}$. The definition of the period and parity is compatible with [38, page 144]. Note that A is maximal (resp. minimal) over $\mathbb{F}_q$ if and only if $\mu(A) = 1$ and $\delta(A) = 1$ (resp. $\delta(A) = -1$).

Let $\Theta(A/K)$ be the set of K-isomorphism classes of twists A'/K of A, see Definition 3.1.

Definition 4.2. A principally polarized supersingular abelian variety A/K is of one of the following *types* over K:

(1) *fully maximal* if A'/K has K-parity $\delta = 1$ for all $A' \in \Theta(A/K)$;
(2) *fully minimal* if A'/K has K-parity $\delta = -1$ for all $A' \in \Theta(A/K)$;
(3) *mixed* if there exist $A', A'' \in \Theta(A/K)$ with K-parities $\delta(A') = 1$ and $\delta(A'') = -1$.

If A/K has K-period 1, then A/K is maximal or minimal and so A is mixed over K since A_ι has the opposite parity. For this reason, the terminology is better suited for curves than for abelian varieties, see Lemmas 5.4 and 5.5. Also, it is most interesting to study the type of A/K over small fields of definition.

Example 4.3. Let $p \equiv 3 \bmod 4$ with $p > 3$. The supersingular elliptic curve $E : y^2 = x^3 - x$ has $\mathrm{Aut}_k(E) \simeq \mathbb{Z}/4\mathbb{Z}$. Then $\mathrm{NWN}(E/\mathbb{F}_p) = \{\pm i\}$ and $\mathrm{NWN}(E/\mathbb{F}_{p^2}) = \{-1, -1\}$. So E has two $\mathbb{F}_p$-twists and is fully

maximal over $\mathbb{F}_p$. It has four $\mathbb{F}_{p^2}$-twists and is mixed over $\mathbb{F}_{p^2}$ since an automorphism of order 4 acts on $\mathrm{NWN}(E/\mathbb{F}_{p^2})$ by multiplication by $\pm i$. Cf. Lemma 6.5.

Let n be odd. The parity is preserved under a degree n extension, i.e., $\delta(A \times_K K_n) = \delta(A)$. Hence, if A/K is mixed, then $A \times_K K_n$ is also mixed: if A'/K is a twist with opposite parity from A/K, then $A' \times_K K_n$ is a twist of opposite parity from $A \times_K K_n$. Motivated by this, we measure the 2-divisibility of the orders of the period in the next section.

4.2. Relationship between types and Weil numbers

By Theorem 2.8, the normalized Weil numbers $\{z_1, \ldots, z_g\}$ of a supersingular abelian variety A/K are roots of unity in $\mathbb{C}^*$. If $z \in \mathbb{C}^*$ is a root of unity, let $o(z)$ denote its multiplicative order in $\mathbb{C}^*$. We measure the 2-divisibility of $o(z_i)$ in the next definition.

Definition 4.4. Let $e_i = \mathrm{ord}_2(o(z_i))$. The 2-*valuation vector* of A/K is the multiset $\underline{e} = \underline{e}(A/K) := \{e_1, \ldots, e_g\}$. The notation $\underline{e} = \{e\}$ means that $e_i = e$ for $1 \le i \le g$.

Write $o(z_i) = 2^{e_i} c_i$ with c_i odd. Then $z_i^m = -1$ for some $m \in \mathbb{N}$ if and only if $e_i \ge 1$. Also:

$$\mathrm{ord}_2(o(z)) = 1 \Leftrightarrow \mathrm{ord}_2(o(-z)) = 0; \text{ if } \mathrm{ord}_2(o(z)) \ge 2, \text{ then } \mathrm{ord}_2(o(-z)) \ge 2; \tag{9}$$

$$\text{If } r \text{ is odd, then } \underline{e} \ne \{0\}, \{1\}, \text{ because } P(A/K, T) \in \mathbb{Z}[T]. \tag{10}$$

Remark 4.5. For the $\mathbb{F}_q$-parity, note that $\delta(A) = 1$ if and only if $\underline{e} = \{e\}$ with $e \ge 1$ (or $e \ge 2$ when r is odd). For the $\mathbb{F}_q$-period, write $\mu(A) = 2^E \bar{\mu}$ where $\bar{\mu}$ is odd. If $\underline{e} = \{e\}$, then $E = \max(e-1, 0)$. If $\underline{e}$ is not constant, then $E = \max\{e_i \mid 1 \le i \le g\}$.

Lemma 4.6. *Let $\underline{e} = \underline{e}(A/K)$.*

(1) *If A/K is fully maximal, then (i) $\underline{e} = \{e\}$ with $e \ge 2$;*
(2) *If A/K is fully minimal, then (ii) the e_i are not all equal;*
(3) *If (iii) $\underline{e} = \{e\}$ with $e \in \{0, 1\}$ and r is even, then A/K is mixed.*

Proof. (1) If A/K is fully maximal, then it has K-parity $+1$; so $\underline{e} = \{e\}$ for some $e \ge 1$ (with $e \ge 2$ if r is odd by (10)). Suppose that r is even and $\underline{e} = \{1\}$. By (9), the twist A_ι has the property that $\underline{e} = \{0\}$. So A_ι has K-parity -1, which contradicts the fact that A/K is fully maximal. Thus condition (i) holds.
(2) If A/K is fully minimal, then it has K-parity -1. By (10), either $\underline{e} = \{0\}$ with r even or the e_i are not all the same. If r is even and $\underline{e} = \{0\}$, then the twist by ι is maximal, giving a contradiction. Thus condition (ii) holds.
(3) This is the contrapositive of parts (1) and (2). □

Proposition 4.7. *If $A/\mathbb{F}_q$ is simple and $q = p^r$ with r even, then $A/\mathbb{F}_q$ is not fully minimal.*

Proof. If $A/\mathbb{F}_q$ is simple, the Weil numbers $\{\sqrt{q} z_i\}$ are all conjugate over $\mathbb{Q}$. Let $n = o(z_1)$ and $e = \mathrm{ord}_2(n)$. Since r is even, $\sqrt{q} \in \mathbb{Q}$, so the conjugates of $\sqrt{q} z_1$ are precisely the $\phi(n)$ values $\sqrt{q}\zeta_n^j$ for $j \in (\mathbb{Z}/n\mathbb{Z})^*$. So $\underline{e} = \{e\}$. By Lemma 4.6(2), $A/\mathbb{F}_q$ is not fully minimal. □

4.3. Types of abelian varieties with small automorphism group

Corollary 4.8. *Suppose that $|\mathrm{Aut}_k(A)| = 2$. Then*

(1) *A/K is fully maximal if and only if (i) $\underline{e} = \{e\}$ with $e \geq 2$;*
(2) *A/K is fully minimal if and only if (ii) the e_i are not all equal;*
(3) *A/K is mixed if and only if (iii) $\underline{e} = \{e\}$ with $e \in \{0, 1\}$ and r is even.*

Proof. One set of implications is Lemma 4.6. Conversely, if $|\mathrm{Aut}_k(A)| = 2$, then A_K has at most one nontrivial twist, which is A_ι. Thus, A/K is fully maximal (resp. fully minimal) if and only if A and A_ι both have K-parity $+1$ (resp. -1). The result follows because negation of $\{z_i\}$ preserves each of the conditions $(i), (ii), (iii)$ for $\underline{e}$, by (9). □

By Corollary 4.8, if $|\mathrm{Aut}_k(A)| = 2$, then the type of A/K is preserved under odd degree extensions of K.

Remark 4.9. Let S be an irreducible component of the supersingular locus of the moduli space of principally polarized abelian varieties of dimension g. Among the abelian varieties A represented by $\mathbb{F}_q$-points of S, the typical structure of $\mathrm{Aut}_k(A)$ is not known in general. For $g \geq 2$ and p odd, one might expect that typically $\mathrm{Aut}_k(A) \simeq \mathbb{Z}/2\mathbb{Z}$. For $g = 2$ and p odd, we prove that this is true in Proposition 7.6.

Remark 4.10. Let S and A be as in Remark 4.9 and $K = \mathbb{F}_q$. If p is odd, one expects the proportion of A with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset \mathrm{Aut}_K(A)$ to be small. The reason is that if $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset \mathrm{Aut}_K(A)$, then A is not simple over K by [18, Theorem B]. So this condition implies that the a-number of A is at least two, by [7, Proposition 4]. However, for all g and p, it is known that A generically has a-number 1 [23, Section 4.9].

4.4. Parity-changing twists of abelian varieties

Suppose that $A'/K \in \Theta(A/K)$ is a K-twist of A of order T. Then there is an isomorphism $\phi : A \times_K K_T \xrightarrow{\simeq} A' \times_K K_T$ defined over K_T. Denote $\mathrm{NWN}(A/K) = \{z_i, \bar{z}_i\}_{1 \leq i \leq g}$ and $\mathrm{NWN}(A'/K) = \{w_i, \bar{w}_i\}_{1 \leq i \leq g}$. After possibly reordering, $z_i^T = w_i^T$ and hence

$$w_i = \lambda_i z_i \tag{11}$$

for some (not necessarily primitive) T-th root of unity λ_i. Let $t = \mathrm{lcm}\{o(\lambda_i) \mid 1 \leq i \leq g\}$. By definition, $t \mid T$. In particular, if A'/K is a trivial twist, then $t = 1$ and $z_i = w_i$ for all i. If $t \neq T$, it means that A and A' are isogenous but not isomorphic over $\mathbb{F}_{q^t}$.

Conversely, if $A'/K \in \Theta(A/K)$ is a K-twist of A of some order and if (11) holds, then A and A' are isogenous, but not necessarily isomorphic, over K_T.

Lemma 4.11. *Let $\underline{e}$ be the 2-valuation vector of A/K. Suppose that A'/K is a K-twist of A/K of order T. Let $\epsilon = \mathrm{ord}_2(T)$. If $\epsilon < \min\{e_i \mid 1 \leq i \leq g\}$, then $\underline{e}(A'/K) = \underline{e}$.*

Proof. If $w_i = \lambda_i z_i$, then $\mathrm{ord}_2(o(w_i)) \leq \max(\mathrm{ord}_2(o(\lambda_i)), \mathrm{ord}_2(o(z_i)))$, with equality if the two values are not equal. Then $\mathrm{ord}_2(o(\lambda_i)) \leq \mathrm{ord}_2(T) = \epsilon$ so the hypothesis implies that $\mathrm{ord}_2(o(w_i)) = \mathrm{ord}_2(o(z_i))$. □

Proposition 4.12. *Suppose that A/K has K-period M and K-parity $+1$ and its K-twist A'/K has K-period N and K-parity -1. Let $e_M = \mathrm{ord}_2(M)$ and $e_N = \mathrm{ord}_2(N)$. If $e_N \leq e_M$, then $\mathrm{ord}_2(t) = 1 + e_M$; if $e_N > e_M$, then $\mathrm{ord}_2(t) = e_N$.*

Proof. Write $L = \mathrm{lcm}(M, N)$. Recall that $z_i^M = -1$ and $w_i^N = 1$ for $1 \leq i \leq g$.

Suppose that $e_N \leq e_M$. Then $\ell_2 = L/M$ is odd and $\mathrm{ord}_2(L) = e_M$. Then

$$1 = w_i^L = \lambda_i^L z_i^L = \lambda_i^L (z_i^M)^{\ell_2} = \lambda_i^L (-1)^{\ell_2}.$$

This implies that $\lambda_i^L = -1$ and so $\mathrm{ord}_2(o(\lambda_i)) = 1 + e_M$ for $1 \le i \le g$.

Suppose that $e_M < e_N$. For $1 \le i \le g$, then $\mathrm{ord}_2(o(z_i)) = 1 + e_M$ and $\mathrm{ord}_2(o(w_i)) \le e_N$. The equation $w_i = \lambda_i z_i$ implies that $\mathrm{ord}_2(o(\lambda_i)) \le e_N$ for $1 \le i \le g$. To show that $\mathrm{ord}_2(t) = e_N$, it thus suffices to show that $\mathrm{ord}_2(o(\lambda_i)) = e_N$ for some i.

When $e_M < e_N$, then $rN/2$ is even, because rM is even by definition of the period. So if r is odd, then $e_N > e_M \ge 1$. By the minimality of N (such that rN is even), it cannot hold that $w_i^{N/2} = 1$ for all i. Thus, there is at least one value i_0 such that $\mathrm{ord}_2(o(w_{i_0})) = e_N$. Furthermore, since the K-parity is -1, it is not true that $w_i^{N/2} = -1$ for all i. So there is at least one value i_1 such that $\mathrm{ord}_2(o(w_{i_1})) < e_N$.

Note that $z_i = \lambda_i^{-1} w_i$. If $e_N > 1 + e_M$, then substituting $i = i_0$ shows that $\mathrm{ord}_2(o(\lambda_{i_0}^{-1})) = e_N$. If $e_N = 1 + e_M$, then substituting $i = i_1$ shows $\mathrm{ord}_2(o(\lambda_{i_1}^{-1})) = 1 + e_M$. □

Corollary 4.13.

(1) *Suppose that A/K has K-period M and K-parity $+1$. If A'/K is a K-twist of order T with $\mathrm{ord}_2(T) \le e_M$, then A'/K also has K-parity $+1$.*
(2) *Suppose that A'/K has K-period N and K-parity -1. If A/K is a twist of order T with either $\mathrm{ord}_2(T) < e_N$ or $\mathrm{ord}_2(T) = e_N = 0$, then A/K also has K-parity -1.*
(3) *In particular, if A/K and A'/K have different K-parities, then T is even.*

Proof. Note that $\mathrm{ord}_2(T) \ge \mathrm{ord}_2(t)$.

(1) Assume that A'/K has parity -1. By Proposition 4.12, $\mathrm{ord}_2(t) = 1 + e_M$ if $e_N \le e_M$ and $\mathrm{ord}_2(t) = e_N$ if $e_N > e_M$. So $\mathrm{ord}_2(T) > e_M$, which is a contradiction.
(2) Assume that A/K has parity 1. Applying Proposition 4.12 shows that $\mathrm{ord}_2(t) = 1 + e_M$ if $e_N \le e_M$ and $\mathrm{ord}_2(t) = e_N$ if $e_N > e_M$. This implies that either $\mathrm{ord}_2(T) \ge e_N$ or $\mathrm{ord}_2(T) > e_N = 0$, which is a contradiction.
(3) If T is odd, then $\mathrm{ord}_2(T) = 0$. The hypotheses of items (1) and (2) are satisfied and so A/K and A'/K have the same parity. □

5. Fully maximal, fully minimal, and mixed curves

Let $K = \mathbb{F}_q$ with $q = p^r$ and let $k = \overline{\mathbb{F}}_p$. Let X/K be a smooth projective connected supersingular curve of genus $g \ge 1$. The Jacobian $\mathrm{Jac}(X)$ of X is a principally polarized abelian variety of dimension g. If X is hyperelliptic, let ι denote its hyperelliptic involution, which acts on $\mathrm{Jac}(X)$ as the element ι defined in Definition 3.12.

5.1. Types for Jacobians

The theory of twists of X and definitions of the period and parity of X are almost identical to those of $\mathrm{Jac}(X)$, as studied in Sections 3 and 4. The normalized Weil numbers $\{z_i, \bar{z}_i\}_{1 \le i \le g}$ and the 2-valuation vector $\underline{e} = \{e_i = \mathrm{ord}_2(o(z_i))\}_{1 \le i \le g}$ are the same for X and $\mathrm{Jac}(X)$. The main difference is that X may have fewer twists than $\mathrm{Jac}(X)$.

By [22, Appendice], $\mathrm{Jac}(X)$ has the same field of definition as X and

$$\mathrm{Aut}_k(\mathrm{Jac}(X)) \simeq \begin{cases} \mathrm{Aut}_k(X) \text{ if } X \text{ is hyperelliptic,} \\ \langle \iota \rangle \times \mathrm{Aut}_k(X) \text{ if } X \text{ is not hyperelliptic.} \end{cases} \tag{12}$$

For completeness, consider the following analogue of Proposition 3.13.

Proposition 5.1. *Suppose that* $\phi : X \times_K k \xrightarrow{\sim} X' \times_K k$ *where* X/K *is maximal and* X'/K *is minimal (or vice versa). Then* X *is hyperelliptic and* $g_\phi = \iota$ *and* $X'/K \simeq X_\iota/K$ *is a quadratic twist of* X/K.

Proof. Let $A = \mathrm{Jac}(X)$ and $A' = \mathrm{Jac}(X')$. Since the normalized Weil numbers of a curve and its Jacobian are the same, A/K is maximal and A'/K is minimal (or vice-versa) by Definition 2.9. The automorphism $g_\phi \in \mathrm{Aut}_k(X)$ can be identified with an automorphism $g'_\phi \in \mathrm{Aut}_k(A)$ under the isomorphism in (12). By Proposition 3.13, $g'_\phi = \iota$ and $A'/K \simeq A_\iota/K$ is a quadratic twist. The conclusions follow since $g_\phi = \iota \in \mathrm{Aut}_k(X)$. □

Let $\Theta(X/K)$ denote the set of K-isomorphism classes of twists of X/K.

Definition 5.2. A supersingular curve X/K is of one of the following *types* over K:

(1) *fully maximal* if X'/K has K-parity $\delta = 1$ for all $X' \in \Theta(X/K)$;
(2) *fully minimal* if X'/K has K-parity $\delta = -1$ for all $X' \in \Theta(X/K)$;
(3) *mixed* if there exist $X', X'' \in \Theta(X/K)$ with K-parities $\delta(X') = 1$ and $\delta(X'') = -1$.

When X is hyperelliptic, then $\Theta(\mathrm{Jac}(X)/K) = \Theta(X/K)$, so X and $\mathrm{Jac}(X)$ have the same type over K. When X is not hyperelliptic, then X and $\mathrm{Jac}(X)$ might have different types.

Lemma 5.3. *The types of* X *and* $\mathrm{Jac}(X)$ *over* K *are not the same if and only if:* X *is not hyperelliptic,* $\mathrm{Jac}(X)$ *is mixed over* K, r *is even, and* $\underline{e}(X/K) = \{e\}$ *with* $e \leq 1$.

Proof. If the types of X and $\mathrm{Jac}(X)$ over K are not the same, then $\mathrm{Jac}(X)$ has more twists than X, so (12) implies that X is not hyperelliptic. Also, since the extra twist corresponds to ι, then $\mathrm{Jac}(X)$ is mixed, with $\mathrm{Jac}(X)$ and $\mathrm{Jac}(X)_\iota$ having different parities.

Let $\underline{e} = \underline{e}(X/K)$. If not all $e_i \in \underline{e}$ are the same, then not all $e_i \in \underline{e}(\mathrm{Jac}(X)_\iota)$ are the same. Then both $\mathrm{Jac}(X)$ and $\mathrm{Jac}(X)_\iota$ would have parity -1, a contradiction. Thus $\underline{e} = \{e\}$.

If $e \geq 2$, then $\underline{e}(\mathrm{Jac}(X)_\iota) = \{e\}$ and both $\mathrm{Jac}(X)$ and $\mathrm{Jac}(X)_\iota$ would have parity 1, a contradiction. Thus $e \leq 1$ and r must be even by (10). We omit the converse direction. □

The following results are immediate from Definition 5.2, Proposition 3.13, and the remark below Definition 4.2.

Lemma 5.4. *Suppose that* X *has* K*-period* 1. *Then* X *is mixed if and only if* X *is hyperelliptic;* X *is fully maximal if and only if it is not hyperelliptic and maximal; and* X *is fully minimal if and only if it is not hyperelliptic and minimal.*

Lemma 5.5. *If* $\mathrm{Aut}_k(X)$ *is trivial, then* X *is fully maximal over* K *if and only if it has* K*-parity* 1 *and is fully minimal if and only if it has* K*-parity* -1.

In light of Lemmas 5.4 and 5.5, it is most interesting to study the types of curves which are non-hyperelliptic, defined over small fields, or have non-trivial automorphism group.

5.2. Supersingular non-hyperelliptic curves of mixed type

Despite Proposition 3.13, the results in Sections 6 and 7 show that not all hyperelliptic curves are mixed. The next result illustrates that not all mixed curves are hyperelliptic.

Proposition 5.6. *Suppose that $s \equiv 0 \bmod 4$. Suppose that p is such that $p+1 \equiv 0 \bmod s$. Then the smooth plane curve $X/\mathbb{F}_p$ of genus $g = (s-1)(s-2)/2$ given by the equation $x^s + y^s + z^s = 0$ is supersingular and of mixed type over $\mathbb{F}_p$.*

Proof. The curve $X/\mathbb{F}_p$ is a smooth plane curve, of genus $g = (s-1)(s-2)/2$ by the Plucker formula.

The Hermitian curve $\tilde{X} : x_1^{p+1} + y_1^{p+1} + z_1^{p+1} = 0$ is maximal over $\mathbb{F}_{p^2}$. Let $\epsilon = (p+1)/s$. There is a cover $\psi : \tilde{X} \to X$ given by $(x_1, y_1, z_1) \mapsto (x_1^\epsilon, y_1^\epsilon, z_1^\epsilon)$. The cover is Galois, since there exists $\lambda \in \mathbb{F}_{p^2}^*$ with multiplicative order ϵ. So X is a quotient of $\tilde{X}$ by a group of automorphisms defined over $\mathbb{F}_{p^2}$. By a result attributed to Serre, see [10, Theorem 10.2], X is also maximal over $\mathbb{F}_{p^2}$ and thus has $\mathbb{F}_p$-parity 1. In particular, X is supersingular.

Let $\lambda_1 \in \mathbb{F}_{p^2}^*$ be an element of multiplicative order $s_1 = s/2$. Consider the automorphism $h \in \mathrm{Aut}_{\mathbb{F}_{p^2}}(X)$ given by $h(x,y,z) = (\lambda_1 y, x, z)$. Then

$$\begin{aligned} h^{\,Fr_{\mathbb{F}_p}} h(x,y,z) &= h(Fr_{\mathbb{F}_p}(h(x^{1/p}, y^{1/p}, z^{1/p}))) \\ &= h(Fr_{\mathbb{F}_p}(\lambda_1 y^{1/p}, x^{1/p}, z^{1/p})) = h(\lambda_1^p y, x, z) \\ &= (\lambda_1 x, \lambda_1^p y, z) = (\lambda_1 x, \lambda_1^{-1} y, z), \end{aligned}$$

where the last equality uses that $p \equiv -1 \bmod s$. In particular, $h^{\,Fr_{\mathbb{F}_p}} h$ has order s_1.

Consider the action of $h^{\,Fr_{\mathbb{F}_p}} h$ on $\mathrm{Jac}(X)/\mathbb{F}_{p^2}$. The next claim is that the eigenvalues for this action include both 1 and a root of unity of order s_1. To see this, it suffices to prove the same claim for the action on $H^1(X, \mathcal{O})$ (after lifting to characteristic 0, using that $\mathrm{Jac}(X) \simeq H^0(X, \Omega^1)^*/H_1(X, \mathbb{Z})$ and invoking Serre duality). Now $H^1(X, \mathcal{O})$ has a basis given by the monomials $x^{-k_1} y^{-k_2} z^{-k_3}$ where $k_1, k_2, k_3 \in \mathbb{N}$ and $k_1 + k_2 + k_3 = r$. Then $h^{\,Fr_{\mathbb{F}_p}} h$ acts via multiplication by $\lambda_1^{-k_1+k_2}$ on $x^{-k_1} y^{-k_2} z^{-k_3}$. The claim follows by taking $(k_1, k_2) = (1,1)$ and $(k_1, k_2) = (1,2)$.

The normalized Weil numbers of $X/\mathbb{F}_{p^2}$ are all -1 and so $\underline{e}(X/\mathbb{F}_{p^2}) = \{1\}$. Let X' be the twist of $X/\mathbb{F}_p$ corresponding to h. Then $X'/\mathbb{F}_{p^2}$ is the twist of $X/\mathbb{F}_{p^2}$ by $h^{\,Fr_{\mathbb{F}_p}} h$. Its set of normalized Weil numbers contains -1 and $-\lambda_1$. By hypothesis, s_1 is even. So $-\lambda_1$ has odd order if $s_1 \equiv 2 \bmod 4$ and $-\lambda_1$ has order s_1 if $s_1 \equiv 0 \bmod 4$. Thus $\underline{e}(X'/\mathbb{F}_{p^2})$ contains the values 1 and 0 if $s_1 \equiv 2 \bmod 4$ and the values 1 and $\mathrm{ord}_2(s_1) \geq 2$ if $s_1 \equiv 0 \bmod 4$. In either case, $\underline{e}(X'/\mathbb{F}_{p^2}) \neq \{e\}$ and $\underline{e}(X'/\mathbb{F}_p) \neq \{e\}$ for any e. Hence, X' has $\mathbb{F}_p$-parity -1. Thus X is mixed over $\mathbb{F}_p$. □

Example 5.7. For $p \equiv 3 \bmod 4$, the Fermat curve $X/\mathbb{F}_p : x^4 + y^4 + z^4 = 0$ is a non-hyperelliptic supersingular curve of genus 3 which is mixed over $\mathbb{F}_p$.

Remark 5.8. Let p be odd. Let $E/\mathbb{F}_p$ be a supersingular elliptic curve with $\mathrm{NWN}(E/\mathbb{F}_p) = \{i, -i\}$. In [14, Theorem 1] (resp. [12, Proposition 15]), the authors construct a smooth plane quartic $X/\mathbb{F}_p$ such that $\mathrm{Jac}(X) \simeq_{\mathbb{F}_{p^2}} E^3$ (resp. $\mathrm{Jac}(X) \sim_{\mathbb{F}_{p^2}} E^3$). In particular, X is maximal over $\mathbb{F}_{p^2}$. The polarization on $\mathrm{Jac}(X)$ induces a non-product polarization on E^3. To determine the type of X, it is necessary to determine which automorphisms of E^3 are compatible with this polarization and the field of definition of these automorphisms.

5.3. Parity-changing twists of curves

Let X/K be a supersingular curve of genus g and let $G = \mathrm{Aut}_k(X)$. The normalized Weil numbers determine the K-parity of X. To determine the type over K, it is necessary to know whether X has a parity-changing K-twist.

By Corollary 4.13, the 2-divisibility of the order T of a twist gives information about whether it can change the K-parity of X. However, this is not easy to control because the values of T depend on the K-Frobenius conjugacy classes of G and on the fields of definition of the automorphisms $g \in G$.

This section contains results that simplify the question of whether X has a parity-changing twist. This material is used in Section 8. Given $g \in G$, recall from Proposition 3.5 that $\phi_g : X \times_K k \to X' \times_K k$ is a geometric isomorphism such that $\xi_\phi(Fr_K) = g$.

Lemma 5.9. *If $h \in G$ has odd order and is defined over K, then ϕ_h is not a parity-changing twist.*

Proof. This is immediate from Lemmas 3.8 and 4.13. □

Suppose that $\tau \in \mathrm{Aut}_k(X)$ has order 2. Assume that τ is defined over K; this is true, for example, if $\tau = \iota$ or if $\mathrm{Aut}_k(X)$ has a unique element of order 2. Let $Z = X/\tau$ be the quotient of X by τ, which is also defined over K. Thus, $X \to Z$ is a geometric $\mathbb{Z}/2\mathbb{Z}$-Galois cover. Let χ be the nontrivial character of $\mathbb{Z}/2\mathbb{Z}$; it satisfies $\chi(P) = 1$ if $P \in Z$ is split in X and $\chi(P) = -1$ if P is inert in X. Consider the Artin L-series

$$L(Z/K, T, \chi) = \prod_{P \in Z} (1 - \chi(P)|P|^{-s})^{-1}, \text{ where } T = q^{-s}. \tag{13}$$

Lemma 5.10. *Suppose that $\tau \in \mathrm{Aut}_K(X)$ has order 2.*

(1) *There is a factorization $L(X/K, T) = L(Z/K, T)L(Z/K, T, \chi)$ in $\mathbb{Z}[T]$.*
(2) *The coefficient ρ_1 of T in $L(Z/K, T, \chi)$ equals $S_1 - I_1$, where I_1 (resp. S_1) is the number of K-points of Z that are inert (resp. split) in X.*
(3) *τ negates the roots of $L(Z/K, T, \chi)$ and fixes the roots of $L(Z/K, T)$.*

Proof. (1) This result follows from [31, Chapter 9, page 130].
(2) Recall that $\zeta(X/K, T) = \prod_{Q \in X}(1 - |Q|^{-s})^{-1}$, where $T = q^{-s}$. Similarly, $\zeta(Z/K, T) = \prod_{P \in Z}(1 - |P|^{-s})^{-1}$. Write

$$\zeta(X/K, T) = \prod (1 - |P_i|^{-2s})^{-1} \prod (1 - |P_{sp}|^{-s})^{-2} \prod (1 - |P_r|^{-s})^{-1}, \tag{14}$$

where P_i, P_{sp}, P_r range over points of Z that are inert, split, and ramified in X, respectively. Note that $(1 - |P|^{-2s}) = (1 - |P|^{-s})(1 + |P|^{-s})$. The result follows by comparing (13) and (14) and computing the coefficients of T.
(3) Since $Z = X/\tau$, the involution τ acts trivially on Z and thus fixes the roots of $L(Z/K, T)$. There is an isogeny $\mathrm{Jac}(X) \sim_K \mathrm{Jac}(Z) \oplus V$ where V/K is the nontrivial eigenspace for τ. Then $L(Z/K, T, \chi) = L(V/K, T)$. By Proposition 3.9, τ acts as -1 on the roots of $L(V/K, T)$ by the definition of V. □

Suppose that $\tau \in \mathrm{Aut}_K(X)$ has order 2. Write $\underline{e} = \underline{e}(Z/K) \cup \underline{e}(Z/K, \chi)$ where $\underline{e}(Z/K, \chi)$ denotes the multiset of 2-valuations of the normalized roots of $L(Z/K, T, \chi)$. If τ is the hyperelliptic involution, then $\underline{e}(Z/K)$ is empty and $\underline{e} = \underline{e}(Z/K, \chi)$.

Lemma 5.11. *If $\tau \in \mathrm{Aut}_K(X)$ has order 2, then ϕ_τ is a parity-changing twist if and only if r is even and either $\underline{e}(Z/K) = \{1\}$ and $\underline{e}(Z/K, \chi) = \{e\}$ with $e \leq 1$, or $\underline{e}(Z/K) = \{0\}$ and $\underline{e}(Z/K, \chi) = \emptyset$.*

Proof. By Lemma 5.10, τ negates the roots of $L(Z/K, T, \chi)$ and fixes the roots of $L(Z/K, T)$. This changes the parity only under the given conditions. □

Information about parity-changing twists can be determined from $\underline{e}$ in certain cases when $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \subset \mathrm{Aut}_k(X)$ using the next remark. Section 8.4 uses this material.

Remark 5.12. Suppose that $\mathrm{Aut}_k(X)$ contains a subgroup $S \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Write $S = \{\mathrm{id}, \tau_1, \tau_2, \tau_3\}$. Suppose that S is stabilized by K-Frobenius conjugation, in which case the number γ of nontrivial involutions in S defined over K is either 3, 0, or 1.

(1) When $\gamma = 3$ and X/S has genus 0, let $A_i = \mathrm{Jac}(X/\tau_i)$. Then $\mathrm{Jac}(X) \sim_K A_1 \oplus A_2 \oplus A_3$ by [18, Theorem B]. Each τ_i acts by negating $\mathrm{NWN}(A_i/K)$ for exactly two values of i. Write $\underline{e}_i = \underline{e}(A_i)$ and $\underline{e}(X) = \bigcup_{i=1}^3 \underline{e}_i$. The twist for $\tau_i \in S$ changes the parity if and only if $\underline{e}(X) = \{1\}$ or (after rearranging), $\underline{e}_1 = \{1\}$, $\underline{e}_2 = \{0\}$, and $\underline{e}_3 = \{0\}$ or $\emptyset$.
(2) When $\gamma = 0$, K-Frobenius conjugation acts via a 3-cycle on $S - \{\mathrm{id}\}$, so the twist for each τ_i has order 3. By Corollary 4.13, these do not change the parity.
(3) When $\gamma = 1$, suppose $\tau = \tau_1$ is defined over K while $\mu = \tau_2$ and $\mu\tau = \tau_3$ are not. Let $Z = X/\tau$. Note that ${}^{Fr_K}\mu = \mu\tau$ and $\mu\,{}^{Fr_K}\mu = \tau$. Using Lemma 3.8, the twist for μ has $c = 2$ and $|G| = 2$. Moreover, the twist by μ over K corresponds to the twist X_τ by τ over K_2, so it negates the roots of $L(Z/K_2, T, \chi)$ and fixes the roots of $L(Z/K_2, T)$ by Lemma 5.10(3). To find the action of μ on $\underline{e}(X/K)$, it is necessary to take the square roots of the $\mathrm{NWN}(X_\tau/K_2)$. If $e_i \leq 1$ for any i, this leads to some ambiguity in $\underline{e}(X_\mu/K)$, which can be partially resolved by the following observation.

$$\textbf{Claim}: \text{ When } \gamma = 1, \text{the coefficient } \rho_1 \text{ of } T \text{ in } L(Z/K, T, \chi) \text{ equals } 0. \tag{15}$$

Proof. By Lemma 5.10(2), it suffices to prove $S_1 = I_1$. If p is odd, $X \to Z$ has an equation of the form $y^2 = F$. Given a K-point P of Z, it suffices to show P is split in X if and only if $\mu(P)$ is inert in X. The point P splits in X if and only if $F(P)$ is a square in K^*. Since μ and τ commute, μ acts on both X and Z. By assumption, the action of μ on the equation $y^2 = F$ is defined over K_2 but not over K. The K-action of μ thus yields a quadratic twist of $y^2 = F$. So $\mu(y) = wy$ for some $w \in K_2^* \setminus K^*$ such that $z = w^2$ is in K^*, and $F(\mu(P)) = zy$. Thus, $F(P)$ is a square in K^* if and only if $F(\mu(P))$ is not.

The proof for $p = 2$ is the same, after replacing y^2 by $y^2 - y$, $\mu(y) = wy$ by $\mu(y) = y + w$ for some $w \in K_2 \setminus K$ such that $z = w^2 - w$ is in K, and $F(\mu(P)) = zF(P)$ by $F(\mu(P)) = F(P) + z$. □

6. Analysis in low dimension: elliptic curves

Let $K = \mathbb{F}_q$ with $q = p^r$ and let $k = \overline{\mathbb{F}}_p$. If $E/\mathbb{F}_q$ is an elliptic curve, then $L(E/\mathbb{F}_q, T) = 1 - \beta T + qT^2$ for some $\beta \in \mathbb{Z}$. Moreover, E is supersingular if and only if $p \mid \beta$. By Honda–Tate theory (cf. [40], [11], [39]), β determines the $\mathbb{F}_q$-isogeny class of E.

Lemma 6.1. *Let $q = p^r$. Table 6.1 lists each $\beta \in \mathbb{Z}$ which occurs for a supersingular elliptic curve $E/\mathbb{F}_q$, together with the normalized Weil numbers z and $\bar{z}$, the 2-adic valuation $e = \mathrm{ord}_2(o(z))$, the period, and the parity. We use the convention that $\zeta_n = e^{2\pi i/n}$.*

Table 6.1
Isogeny classes and invariants of supersingular elliptic curves.

Case n_E	Conditions on r and p	β	$\mathrm{NWN}(E/\mathbb{F}_q)$	$\mathrm{ord}_2(o(z))$	Period	Parity
$W1\pm$	r even	$\pm 2\sqrt{q}$	$(\pm 1, \pm 1)$	0	1	∓ 1
$W2\pm$	r even, $p \not\equiv 1 \pmod 3$	$\pm\sqrt{q}$	$(\mp\zeta_3, \mp\overline{\zeta}_3)$	1	3	± 1
$W3$	r even, $p \not\equiv 1 \pmod 4$ or r odd	0	$(i, -i)$	2	2	1
$W4a$	r odd, $p = 2$	$\pm\sqrt{2q}$	$(\pm\zeta_8, \pm\overline{\zeta}_8)$	3	4	1
$W4b$	r odd, $p = 3$	$\pm\sqrt{3q}$	$(\pm\zeta_{12}, \pm\overline{\zeta}_{12})$	2	6	1

Proof. This is a short calculation based on the values of β in [44, Theorem 4.1]. □

The number of supersingular j-invariants is $\lfloor \frac{p}{12} \rfloor + \epsilon$ (with $\epsilon = 0, 1, 1, 2$ if $p \equiv 1, 5, 7, 11 \bmod 12$) [35, Theorem V.4.1(c)].

Remark 6.2. Let $N(\beta)$ denote the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves in the $\mathbb{F}_q$-isogeny class determined by β. The values of $N(\beta)$ are found in [32, Theorem 4.6]; they depend only on p, not q, and $N(-\beta) = N(\beta)$. Using this and Table 6.1, one can determine the probability that a given supersingular elliptic curve $E/\mathbb{F}_{p^r}$ has $\mathbb{F}_{p^r}$-parity 1. If r is odd, then the $\mathbb{F}_{p^r}$-parity is always 1. If r is even, then $N(0) = 1 - \left(\frac{-4}{p}\right)$ is the difference between the number of isomorphism classes of $E/\mathbb{F}_{p^r}$ with $\mathbb{F}_{p^r}$-parity 1 and -1.

Each supersingular j-invariant is in $\mathbb{F}_{p^2}$. If $E/\overline{\mathbb{F}}_p$ is a supersingular elliptic curve, then E descends to $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$; it descends to $\mathbb{F}_p$ if and only if the j-invariant of E is in $\mathbb{F}_p$. The next result shows that in neither case is E fully minimal.

Theorem 6.3. *Let $E/\overline{\mathbb{F}}_p$ be a supersingular elliptic curve. If the j-invariant of E is in $\mathbb{F}_p$, then E is fully maximal over $\mathbb{F}_p$; if not, then E is mixed over $\mathbb{F}_{p^2}$.*

Proof. If $p = 2$, the result is proven in Lemma 6.4 (below). If $p \geq 3$ and $\mathrm{Aut}_k(E) \not\simeq \mathbb{Z}/2\mathbb{Z}$, the result is proven in Lemma 6.5 (below). This completes the proof for $p = 3$, since there is only one isomorphism class of supersingular elliptic curves over $\overline{\mathbb{F}}_3$.

Finally, suppose that $p \geq 5$ and $\mathrm{Aut}_k(E) \simeq \mathbb{Z}/2\mathbb{Z}$, so that E_ι is the only twist of E. If E is defined over $\mathbb{F}_p$, then E and E_ι are both in case W3 of Table 6.1, thus E is fully maximal over $\mathbb{F}_p$. If E is instead defined over $\mathbb{F}_{p^2}$, then E and E_ι are either in cases W1± or in cases W2± of Table 6.1; note that E cannot be in case W3 because of the condition $\mathrm{Aut}_k(E) \simeq \mathbb{Z}/2\mathbb{Z}$ (and in that case E has j-invariant in $\mathbb{F}_p$). Thus E is mixed over $\mathbb{F}_{p^2}$. □

Lemma 6.4. *If $p = 2$, the unique supersingular elliptic curve $E/\overline{\mathbb{F}}_2$ is fully maximal over $\mathbb{F}_2$.*

Proof. The uniqueness fact can be found in [35, Appendix A, Proposition 1.1]. So E is isomorphic over k to the elliptic curve $E/\mathbb{F}_2$ with affine equation $y^2 = x^3 - x$ with j-invariant 0. Then $|E(\mathbb{F}_2)| = p + 1$, so $\beta = 0$ (case W3 of Table 6.1). The $\mathbb{F}_2$-twists are also defined over $\mathbb{F}_2$, thus are in case W3, W4a or W4b of Table 6.1, which each have $\mathbb{F}_2$-parity $+1$. □

Lemma 6.5. *Let $p \geq 3$. If $\mathrm{Aut}_k(E) \not\simeq \mathbb{Z}/2\mathbb{Z}$, then E is fully maximal over $\mathbb{F}_p$.*

Proof. If $\mathrm{Aut}_k(E) \not\simeq \mathbb{Z}/2\mathbb{Z}$, then E is isomorphic over k to either:

(1) $y^2 = x^3 - x$ (j-invariant 1728), which is supersingular if and only if $p \equiv 3 \bmod 4$; or
(2) $y^2 = x^3 + 1$, (j-invariant 0), which is supersingular if and only if $p \equiv 2 \bmod 3$.

In both cases, $\{z, \bar{z}\} = \{i, -i\}$ (case W3 of Table 6.1) with $\underline{e}(E/\mathbb{F}_p) = \{2\}$ and the curve is defined over $\mathbb{F}_p$, so we consider its type over $\mathbb{F}_p$.

For case (1), let $g \in \mathrm{Aut}_k(E)$ be the order 4 automorphism defined by $g(x, y) = (-x, iy)$.

(a) If $p > 3$, then $\mathrm{Aut}_k(E) \simeq \langle g \rangle$. Then $E/\mathbb{F}_p$ has only one nontrivial twist because the $\mathbb{F}_p$-Frobenius conjugacy classes in $\mathrm{Aut}_k(E)$ are $\{\mathrm{id}, \iota\}$ and $\{g, g^3\}$. By Lemma 3.8, the latter of these yields a quadratic twist since $c = 2$ and $G = g^{Fr} g = \mathrm{id}$. By Lemma 4.11, the twist has $\underline{e} = \{2\}$ as well.

(b) If $p = 3$, then $|\mathrm{Aut}_k(E)| = 12$ [35, Appendix A, Proposition 1.2]. Then $\mathrm{Aut}_k(A) = \langle g, \sigma \rangle$ where $\sigma(x, y) = (x + 1, y)$. The $\mathbb{F}_p$-Frobenius conjugacy classes are $\{\mathrm{id}, \iota\}$, $\{\sigma^2, \sigma\iota\}$, $\{\sigma, \sigma^2\iota, \}$, and $\{g, g^3, \sigma g, \sigma g^3, \sigma^2 g, \sigma^2 g^3\}$. The first (resp. last) of these yield a trivial (resp. quadratic) twist as in (a). Since σ and σ^2 have order 3 and are defined over $\mathbb{F}_p$, these yield twists of order 3 by Lemma 3.8 with $\underline{e} = \{2\}$ by Lemma 4.11.

For case (2), $\mathrm{Aut}_k(E) = \langle h \rangle$ where h has order 6 and is defined by $h(x, y) = (\zeta_3 x, -y)$. The two $\mathbb{F}_p$-Frobenius conjugacy classes are $\{\mathrm{id}, h^2, h^4\}$ and $\{h, h^3, h^5\}$. Since $h^3 = \iota$, the latter of these yields a quadratic twist. By Lemma 4.11, the twist has $\underline{e} = \{2\}$ as well.

Thus, in both case (1) and case (2), E is fully maximal over $\mathbb{F}_p$. □

7. Analysis in low dimension: abelian surfaces

7.1. Parity table for simple supersingular abelian surfaces

Let $q = p^r$ and $k = \overline{\mathbb{F}}_p$. Suppose that $A/\mathbb{F}_q$ is a simple supersingular abelian surface, which is not necessarily principally polarized. The $\mathbb{F}_q$-isogeny class of A is determined by (the conjugacy class of) its Weil numbers or, equivalently, by the coefficients (a_1, a_2) of

$$P(A/\mathbb{F}_q, T) = T^4 + a_1 T^3 + a_2 T^2 + q a_1 T + q^2 \in \mathbb{Z}[T].$$

The next result builds on [24]. Let L be the minimal field extension of $\mathbb{F}_q$ over which A is not simple. Then $A \sim_L E \oplus E$, where E/L is a supersingular elliptic curve.

Table 7.1
Isogeny classes and invariants of simple supersingular abelian surfaces.

	(a_1, a_2)	Conditions on r and p	t_0	W	z/L	$\mathrm{NWN}(A/\mathbb{F}_q)$	μ	δ
$1a$	$(0, 0)$	r odd, $p \equiv 3 \bmod 4$ or r even, $p \not\equiv 1 \bmod 4$	2	3	i	$(\zeta_8, \zeta_8^7, \zeta_8^3, \zeta_8^5)$	4	1
$1b$	$(0, 0)$	r odd, $p \equiv 1 \bmod 4$ or r even, $p \equiv 5 \bmod 8$	4	1	-1	$(\zeta_8, \zeta_8^7, \zeta_8^3, \zeta_8^5)$	4	1
$2a$	$(0, q)$	r odd, $p \not\equiv 1 \bmod 3$	2	2	ζ_3	$(\zeta_6, \zeta_6^5, \zeta_6^2, \zeta_6^4)$	6	-1
$2b$	$(0, q)$	r odd, $p \equiv 1 \bmod 3$	6	1	-1	$(\zeta_{12}, \zeta_{12}^{11}, \zeta_{12}^5, \zeta_{12}^7)$	6	1
$3a$	$(0, -q)$	r odd and $p \equiv 2 \bmod 3$ or r even and $p \not\equiv 1 \bmod 3$	2	2	$-\zeta_3$	$(\zeta_{12}, \zeta_{12}^{11}, \zeta_{12}^5, \zeta_{12}^7)$	6	1
$3b$	$(0, -q)$	r odd and $p \equiv 1 \bmod 3$ or r even and $p \equiv 4, 7, 10 \bmod 12$	3	3	i	$(\zeta_{12}, \zeta_{12}^{11}, \zeta_{12}^5, \zeta_{12}^7)$	6	1
$4a$	$(\sqrt{q}, q)$	r even and $p \not\equiv 1 \bmod 5$	5	1	1	$(\zeta_5, \zeta_5^4, \zeta_5^2, \zeta_5^3)$	5	-1
$4b$	$(-\sqrt{q}, q)$	r even and $p \not\equiv 1 \bmod 5$	5	1	-1	$(\zeta_{10}, \zeta_{10}^9, \zeta_{10}^3, \zeta_{10}^7)$	5	1
$5a$	$(\sqrt{5q}, 3q)$	r odd and $p = 5$	10	1	1	$(\zeta_{10}^3, \zeta_{10}^7, \zeta_5^2, \zeta_5^3)$	10	-1
$5b$	$(-\sqrt{5q}, 3q)$	r odd and $p = 5$	10	1	1	$(\zeta_{10}, \zeta_{10}^9, \zeta_5, \zeta_5^4)$	10	-1
$6a$	$(\sqrt{2q}, q)$	r odd and $p = 2$	4	2	$-\zeta_3$	$(\zeta_{24}^{13}, \zeta_{24}^{11}, \zeta_{24}^{19}, \zeta_{24}^5)$	12	1
$6b$	$(-\sqrt{2q}, q)$	r odd and $p = 2$	4	2	$-\zeta_3$	$(\zeta_{24}, \zeta_{24}^{23}, \zeta_{24}^7, \zeta_{24}^{17})$	12	1
$7a$	$(0, -2q)$	r odd	2	1	1	$(1, 1, -1 - 1)$	2	-1
$7b$	$(0, 2q)$	r even and $p \equiv 1 \bmod 4$	2	2	-1	$(i, -i, i, -i)$	2	1
$8a$	$(2\sqrt{q}, 3q)$	r even and $p \equiv 1 \bmod 3$	3	1	1	$(\zeta_3, \zeta_3^2, \zeta_3, \zeta_3^2)$	3	-1
$8b$	$(-2\sqrt{q}, 3q)$	r even and $p \equiv 1 \bmod 3$	3	1	-1	$(\zeta_6, \zeta_6^5, \zeta_6, \zeta_6^5)$	3	1

Proposition 7.1. *Table 7.1 classifies all (a_1, a_2) which occur as the coefficients of $P(A/\mathbb{F}_q, T)$ for a simple supersingular abelian surface $A/\mathbb{F}_q$, together with the data:*

- $t_0 = \deg(L/\mathbb{F}_q)$;
- *W, labeling E/L as in the first column of Table 6.1;*

- *z/L, one of the normalized Weil numbers $(z, \overline{z}, z, \overline{z})$ of A/L (again $\zeta_n = e^{2\pi i/n}$);*
- *$\mathrm{NWN}(A/\mathbb{F}_q)$, the normalized Weil numbers of $A/\mathbb{F}_q$;*
- *μ and δ, the period and parity respectively of $A/\mathbb{F}_q$.*

Proof. The list of (a_1, a_2), conditions on r and p, and t_0 are found in [24, Table 1, page 325].[1] Applying [24, Lemma 2.13, Theorem 2.9], we compute the coefficients of $P(A/L, T)$ where $L = \mathbb{F}_{q^{t_0}}$ and determine W. Then the values of z/L, the period, and the parity can be found using Table 6.1. The period is the product of t_0 and the period of E over $\mathbb{F}_q$ and the parities of A and E are the same. To determine $\mathrm{NWN}(A/\mathbb{F}_q)$, we solve $P(A/\mathbb{F}_q, T) = 0$ directly. □

We now give a full classification of the types of supersingular simple principally polarized abelian surfaces with $\mathrm{Aut}_k(A) \simeq \mathbb{Z}/2\mathbb{Z}$, using Proposition 7.1.

Proposition 7.2. *Let A be a supersingular simple principally polarized abelian surface defined over $K = \mathbb{F}_q$. Assume that $\mathrm{Aut}_k(A) \simeq \mathbb{Z}/2\mathbb{Z}$. In Proposition 7.1:*

(1) *if r is odd, then A/K is not mixed; cases (1), (2b), (3a), (6) are fully maximal and cases (2a), (5), (7a) are fully minimal.*
(2) *if r is even, then A/K is not fully minimal; cases (1), (3a), and (7b) are fully maximal and cases (4) and (8) are mixed.*

Proof. By [13, Theorem 1], the principal polarization restriction excludes exactly case (3b). Since $\mathrm{Aut}_k(A) \simeq \mathbb{Z}/2\mathbb{Z}$, the type of A over K is determined from $\underline{e}(A/K)$ by Corollary 4.8. This can be computed from the normalized Weil numbers found in Proposition 7.1. □

Remark 7.3. The sizes of the isogeny classes listed in Table 7.1 are not known. From [47], one could conjecture that a supersingular abelian surface over $\mathbb{F}_q$ most likely has mixed type.

7.2. Curves of genus 2 with extra automorphisms

By [17], there are six equations that describe all genus 2 curves X/K such that $\mathrm{Aut}_k(X) \not\simeq \mathbb{Z}/2\mathbb{Z}$. The number of k-isomorphism classes of these X/K which are supersingular is known [16, Theorem 3.3]. The twists of X/K are studied in [3] and [4]. We determine the type for all supersingular genus 2 curves X with $\mathrm{Aut}_k(X) \not\simeq \mathbb{Z}/2\mathbb{Z}$, over the smallest field $K = \mathbb{F}_q$ containing the coefficients of their defining equation. Let $|\Theta|$ denote the number of K-twists of X. We first analyze the three equations which have no moduli parameters.

Proposition 7.4. *Let $p > 5$. The types over $\mathbb{F}_p$ of the following genus 2 curves $X/\mathbb{F}_p$ with $\mathrm{Aut}_k(X) \not\simeq \mathbb{Z}/2\mathbb{Z}$, which are supersingular under the listed condition on p, are as follows.*

	Equation	Condition	$\mathrm{Aut}_k(X)$	$\lvert\Theta\rvert$	Type
1	$y^2 = x^5 - 1$	$p \not\equiv 1 \bmod 5$	$\mathbb{Z}/10\mathbb{Z}$	2	fully maximal
2	$y^2 = x^6 - 1$	$p \equiv 2 \bmod 3$	$2D_{12}$	7	mixed
3	$y^2 = x^5 - x$	$p \equiv 5, 7 \bmod 8$	$\tilde{S}_4$	6	mixed

Here D_n is the dihedral group of order n and $\tilde{S}_4$ is a 2-covering of S_4.

[1] We would like to thank a referee for pointing out that the value of t_0 in Case 5 is incorrect in [24].

Proof. The equations and automorphism groups are found in [4, Theorem 3.1]. The supersingular condition is found in [16, 1.11–1.13]. For equation (1), $|\Theta| = 2$ by [3, Proposition 11]. For equation (2), when $p \equiv 2 \bmod 3$, then $-3 \notin (\mathbb{F}_p^*)^2$, so $|\Theta| = 7$ by [3, Proposition 16]. For equation (3), when $p \equiv 5, 7 \bmod 8$, then $-2 \notin (\mathbb{F}_p^*)^2$, so $|\Theta| = 6$ by [3, Proposition 17].

The pairs (a_1, a_2) which occur for the twists of X are in [4, Sections 3.1–3.3, Tables 5, 9, 6, 7]. If $(a_1, a_2) = (0, 2p)$, note that $\mathrm{Jac}(X) \sim_{\mathbb{F}_p} E \oplus E$ where $E/\mathbb{F}_p$ is in case $W3$ of Lemma 6.1, which has parity 1. Also, $(a_1, a_2) = (0, -2p)$ has parity -1 by case $(7a)$ of Proposition 7.1.

(1) When $p \equiv 2, 3 \bmod 5$, then $(a_1, a_2) = (0, 0)$ for X and X_ι; thus X is fully maximal. When $p \equiv -1 \bmod 5$, then $(a_1, a_2) = (0, 2p)$ for X and X_ι; thus X is fully maximal.
(2) When $p \equiv 2 \bmod 3$, let $\epsilon = (-1/p)$. The first two rows of [4, Table 9] show that the parity 1 case $(a_1, a_2) = (0, 2p)$ occurs for X or one of its $\mathbb{F}_p$-twists, regardless of the value of ϵ. The third and fourth lines of [4, Table 9] show that the parity -1 case $(a_1, a_2) = (0, -2p)$ occurs for X or one of its $\mathbb{F}_p$-twists, regardless of the value of ϵ, as long as there exists $t \in \mathbb{F}_p$ such that $t^2 + 4$ is not a square in $\mathbb{F}_p^*$; the existence of such a t can be verified using a Jacobi sum argument. So X is mixed.
(3) If $p \equiv 5, 7 \bmod 8$, then both $(0, 2p)$ and $(0, -2p)$ occur as (a_1, a_2) among the twists of X, so X is mixed. □

Next, we analyze the three equations with moduli parameters.

Proposition 7.5. *Let $p > 5$. Any genus 2 curve $X/\mathbb{F}_q$ with $\mathrm{Aut}_k(X) \not\cong \mathbb{Z}/2\mathbb{Z}$ is isomorphic over k to one of equations (1)–(3) in Proposition 7.4 or one of equations (4)–(6) below:*

(4) $y^2 = x^6 + ax^4 + bx^2 + 1$ *where $a, b \in k$ are chosen such that $P(c, d) \neq 0$, where $c = ab$, $d = a^3 + b^3$, and $P(c, d) = (4c^3 - d^2)(c^2 - 4d + 18c - 27)(c^2 - 4d - 110c + 1125)$;*
(5) $y^2 = x^5 + x^3 + ax$, *for $a \neq 0$, $1/4$, $9/100$;*
(6) $y^2 = x^6 + x^3 + a$ *for $p \neq 3$, $a \neq 0$, $1/4$, $-1/50$.*

Let $q = p^r$ be such that $a, b \in K = \mathbb{F}_q$. The types over $\mathbb{F}_q$ for equations (4)–(6) are as follows:

	$\mathrm{Aut}_k(X)$	$\lvert\Theta\rvert$	Type	
4	V_4	4	fully maximal mixed	if r is odd if r is even
5	D_8	3 or 5	fully maximal mixed	if r odd, $a \notin (K^*)^2$ otherwise
6	D_{12}	4 or 6	fully maximal mixed	if $q \equiv 2 \bmod 3$ and $a \in (K^*)^2$ otherwise

Proof. The equations and automorphism groups can be found in [4, Theorem 3.1]. In cases (5) and (6), the number $|\Theta|$ of twists of X is determined in [3, Propositions 12–13]. In case (4), by [4, Section 3.6], when X is supersingular, then $|\Theta| = 4$. The pairs (a_1, a_2) for the twists of X are in [4, Sections 3.4–3.6, Tables 11–17]. We determine the types over $\mathbb{F}_q$ below:

(4) Since $\mathrm{Jac}(X) \sim_k E_1 \oplus E_2$, the 4 twists of X correspond to quadratic twists of either E_1 or E_2, or both. When r is odd, E_1 and E_2 are both in case $W3$ of Lemma 6.1, so X is fully maximal. When r is even, E_1 and E_2 are either both in case $W1+$ (so X is minimal) or both in case $W1-$ (so X is maximal), depending on the L-polynomial of E_1. Then X is mixed since the quadratic twist swaps the two cases.

(5) When r is odd and $a \notin (K^*)^2$, then X and its twists have (a_1, a_2) equal to $(0,0)$ or $(0, 2q)$. Since both cases have parity 1, the curve X is fully maximal.
When r is odd and $a \in (K^*)^2$, there are twists of X with (a_1, a_2) being both $(0, 2q)$ (parity 1) and $(0, -2q)$ (parity -1), so X is mixed. When r is even, a similar argument shows that X is mixed.

(6) When $q \equiv 2 \bmod 3$, note that $p \equiv 2 \bmod 3$ as well and r is odd. Then X and its twists have (a_1, a_2) among $(0, 2q)$, $(0, 2\epsilon q)$ and $(0, -\epsilon q)$, where $\epsilon = 1$ if $a \in (K^*)^2$ and $\epsilon = -1$ otherwise. These curves have respective parities 1, ϵ, and ϵ. So if $\epsilon = 1$, then X is fully maximal and if $\epsilon = -1$, then X is mixed.
When $q \equiv 1 \bmod 3$ and r is odd, then the coefficients (a_1, a_2) of the twists include $(0, 2q)$ and $(0, q)$ of parity 1 and $(0, -2q)$ of parity -1, so X is mixed.
When $q \equiv 1 \bmod 3$ and r is even, let $\epsilon = \left(\frac{-3}{\sqrt{q}}\right)$. Then the possibilities for (a_1, a_2) are $(\pm 4\epsilon\sqrt{q}, 6q)$ of parity $\pm\epsilon$, $(\pm 2\epsilon\sqrt{q}, 3q)$ of parity $\mp\epsilon$, and $(0, -2q)$ of parity -1. So X is mixed. □

7.3. The condition $\mathrm{Aut}_k(A) \simeq \mathbb{Z}/2\mathbb{Z}$ *is not restrictive when* p *is odd*

For general p, r, and g, the structure of the typical automorphism group of a g-dimensional supersingular abelian variety A over $K = \mathbb{F}_{p^r}$ is unknown (cf. Remark 4.9). In this section, we resolve this question for $g = 2$ and p odd.

Let $g = 2$ and let $A = (A, \lambda)$ be a principally polarized abelian surface. For $p \geq 3$, we prove that the proportion of A over $\mathbb{F}_{p^r}$ with $\mathrm{Aut}_k(A) \not\simeq \mathbb{Z}/2\mathbb{Z}$ tends to zero as $r \to \infty$.

Let $\mathcal{A}_2 = \mathcal{A}_2 \otimes \mathbb{F}_p$ denote the moduli space whose points represent the objects (A, λ) in characteristic p. Let $\mathcal{A}_{2,ss} \subset \mathcal{A}_2$ denote the supersingular locus whose points represent supersingular A. Recall that A is superspecial if and only if $A \simeq_k E_1 \oplus E_2$.

Proposition 7.6. *If $p \geq 3$, then the proportion of $\mathbb{F}_{p^r}$-points in $\mathcal{A}_{2,ss}$ which represent A with $\mathrm{Aut}_k(A) \not\simeq \mathbb{Z}/2\mathbb{Z}$ tends to zero as $r \to \infty$.*

Proof. As observed in [1, Section 9], $|\mathcal{A}_{2,ss}(\mathbb{F}_{p^r})| \ll p^{r+2}$, where the notation $f(q) \ll g(q)$ means that there is a constant $C > 0$ such that $|f(q)| \leq C|g(q)|$ for all sufficiently large q. This is because each irreducible component of $\mathcal{A}_{2,ss}$ is geometrically isomorphic to $\mathbb{P}^1$ [29, proof of Corollary 4.7], and the number of irreducible components of $\mathcal{A}_{2,ss}$ equals the class number $H_2(1, p)$ [19, Theorem 5.7], which is $\ll p^2$ by [9], see also [16, Remark 2.17].

By [8, Theorem 3.1], an $\mathbb{F}_{p^r}$-point A in $\mathcal{A}_{2,ss}$ is one of the following canonically principally polarized objects: (i) the Jacobian of a smooth supersingular curve X over $\mathbb{F}_{p^r}$ of genus 2; (ii) the sum $E_1 \oplus E_2$ of two supersingular elliptic curves over $\mathbb{F}_{p^r}$; (iii) the restriction of scalars $\mathrm{Res}_{\mathbb{F}_{p^{2r}}/\mathbb{F}_{p^r}}(E)$ of a supersingular elliptic curve $E/\mathbb{F}_{p^{2r}}$. By [1, Section 9], the number of objects in cases (ii) and (iii) is $\ll p^2$.

Thus, it suffices to restrict to case (i). Since X is hyperelliptic, the isomorphism $A \cong_k \mathrm{Jac}(X)$ descends to $\mathbb{F}_{p^r}$ by [22, Appendix]. By (12), $\mathrm{Aut}_k(\mathrm{Jac}(X)) \simeq \mathrm{Aut}_k(X)$. The arithmetic Torelli map is injective on $\mathbb{F}_{p^r}$-points representing smooth curves [28, Corollary 12.2]. So for case (i), it suffices to bound the number of supersingular curves X of genus 2 with $\mathrm{Aut}_k(X) \not\simeq \mathbb{Z}/2\mathbb{Z}$, which are described in cases (1)–(6) of Propositions 7.4 and 7.5 when $p > 5$; the cases $p = 3$ and $p = 5$ can be handled similarly. In case (1), there is at most one k-isomorphism class of curves, with at most four twists over $\mathbb{F}_{p^r}$.

In cases (2)–(6), the curves are superspecial by [16, Proposition 1.3]. The singularities of $\mathcal{A}_{2,ss}$ are ordinary $(p+1)$-points which occur precisely at the superspecial points [20, page 193]. There are $\ll p^2$ irreducible components of $\mathcal{A}_{2,ss}$, each containing p^2+1 superspecial points by [19, page 154]. So the number of superspecial points in $\mathcal{A}_{2,ss}(k)$ is $\ll p^2(p^2+1)/(p+1) \ll p^3$. (See [15, Theorem 2] for an exact formula in terms of class numbers.)

Applying [1, Lemma 9.1], the number of $\mathbb{F}_q$-models for superspecial curves of genus 2 is also $\ll p^3$. This completes the proof since $\lim_{r\to\infty} p^3/p^r = 0$. □

Remark 7.7. The conclusion of Proposition 7.6 is false when $p = 2$ by [41, Theorem 3.1].

8. Analysis in low dimension: genus 3 curves for $p = 2$

Let $p = 2$ and $k = \overline{\mathbb{F}}_2$. For $c, d \in k^*$, consider the generalized Artin–Schreier curve $X_{c,d}$ with affine equation

$$X_{c,d} : Z^4 + (1 + c)Z^2 + cZ = dS^3. \tag{16}$$

The cover $\gamma : X_{c,d} \to \mathbb{P}^1$, taking $(Z, S) \mapsto S$ is ramified only above $S = \infty$, where it is totally ramified. The filtration of higher ramification groups trivializes at index 3. So by the Riemann–Hurwitz formula, $X_{c,d}$ has genus 3. By Lemma 8.3, $X_{c,d}$ is supersingular. Let $q = 2^r$ be such that $c, d \in K = \mathbb{F}_q$.

In the main result of the section, we determine the type of $X_{c,d}$ over K. To state this, we set some notation. Let $K' = \mathbb{F}_q(h)$, where $h \in \mathbb{F}_{q^2}$ is such that $h^2 + h = c$. Then $h \in \mathbb{F}_q$ if and only if $\mathrm{Tr}_r(c) = 0$, where $\mathrm{Tr}_r : \mathbb{F}_{2^r} \to \mathbb{F}_2$ is the trace map. Let $q' = 2^{r'} = |K'|$.

Theorem 8.1. *Let $X_{c,d}$, r and h be as defined above.*

(1) *If r is odd, then $X_{c,d}/K$ is fully maximal if $h \in \mathbb{F}_q$ and mixed if $h \notin \mathbb{F}_q$.*
(2) *If $r \equiv 2 \bmod 4$, then $X_{c,d}/K$ is mixed if $h \in \mathbb{F}_q$ and fully minimal if $h \notin \mathbb{F}_q$.*
(3) *If $r \equiv 0 \bmod 4$, then $X_{c,d}/K$ is fully minimal.*

Moreover, $\mathrm{Jac}(X_{c,d})$ *has the same type as $X_{c,d}$ over K, unless $r \equiv 0 \bmod 4$ and $h \in \mathbb{F}_q$, in which case* $\mathrm{Jac}(X_{c,d})$ *is mixed.*

Remark 8.2.

(1) If $d = d_1 d_2^3$ with $d_1, d_2 \in K$, there is an $\mathbb{F}_q$-isomorphism $X_{c,d} \xrightarrow{\simeq} X_{c,d_1}$, taking $(Z, S) \mapsto (Z, S/d_2)$. So d can be replaced by any representative of the coset $d(K^*)^3$ in K^*; if r is odd, then one can set $d = 1$.
(2) The supersingular locus S_3 of the moduli space $\mathcal{M}_3 \otimes \mathbb{F}_2$ has dimension 2. By part (1), the curves in the family $X_{c,d}$ are represented by a 1-dimensional subspace of S_3. This 1-dimensional family is the same as the one given in [43, pages 56–57] by

$$X'_{a,b} : x + y + a(x^3y + xy^3) + bx^2y^2 = 0,$$

via the change of coordinates: $c = a/b,\ d = a^3/b,\ S = 1/a(x + y),\ Z = x/(x + y)$.
(3) The proportion of $c \in \mathbb{F}_q^*$ for which $X_{c,d}$ is mixed is a bit larger than $\frac{1}{2}$ when r is odd and a bit smaller than $\frac{1}{2}$ when $r \equiv 2 \bmod 4$ since $\#\{c \in \mathbb{F}_q^* \mid \mathrm{Tr}_r(c) = 1\} = \frac{q}{2}$.

8.1. Decomposition of the Jacobian

Define the values

$$c_1 = d/c^2,\ c_2 = d/(h + 1)^2, \text{ and } c_3 = d/h^2, \tag{17}$$

and corresponding elliptic curves

$$E_1 : R^2 + R = c_1 S^3,\ E_2 : T^2 + T = c_2 S^3,\ E_3 : U^2 + U = c_3 S^3. \tag{18}$$

Also, define commuting order 2 automorphisms on $X_{c,d}$ by:

$$\tau : (S, Z) \mapsto (S, Z + 1) \text{ and } \upsilon : (S, Z) \mapsto (S, Z + h). \tag{19}$$

Note that τ is defined over $K = \mathbb{F}_q$ and υ is defined over K'.

Lemma 8.3.

(1) *Over K, the quotient of $X_{c,d}$ by τ is E_1.*
Over K', the quotient of $X_{c,d}$ by υ (resp. $\tau\upsilon$) is E_2 (resp. E_3).
(2) *Hence,* $\mathrm{Jac}(X_{c,d}) \sim_{K'} E_1 \oplus E_2 \oplus E_3$ *and $X_{c,d}$ is supersingular.*
(3) *Thus* $L(X_{c,d}/K', T) = L(E_1/K', T)L(E_2/K', T)L(E_3/K', T)$.

Proof. (1) The involution τ fixes the function $R_1 = Z(Z + 1)$. Similarly, the involutions υ and $\tau\upsilon$ fix the functions $T_1 = Z(Z + h)$ and $U_1 = Z(Z + (h + 1))$ respectively. Direct calculations show that:

$$\begin{aligned} R_1^2 + cR_1 &= Z^4 + (1 + c)Z^2 + cZ = dS^3; \\ T_1^2 + (h + 1)T_1 &= Z^4 + h^2Z^2 + (h + 1)(Z^2 + hZ) = dS^3; \\ U_1^2 + hU_1 &= Z^4 + (h + 1)^2Z^2 + h(Z^2 + (h + 1)Z) = dS^3. \end{aligned}$$

Setting $R_1 = cR$, $T_1 = (h + 1)T$, and $U_1 = hU$, then

$$R^2 + R = (d/c^2)S^3,\ T^2 + T = (d/(h + 1)^2)S^3,\ U^2 + U = (d/h^2)S^3.$$

(2) The decomposition is immediate from part (1) and [18, Theorem B]. By the Deuring–Shafarevich formula, E_1, E_2, E_3 have 2-rank 0 and hence are supersingular. Thus $X_{c,d}$ is supersingular by Theorem 2.8.
(3) This is immediate from part (2). □

8.2. The normalized Weil numbers of E_1, E_2, and E_3

Lemma 8.4. *The elliptic curve $E_\circ : R^2 + R = S^3$ is maximal over $\mathbb{F}_{2^2}$ and*

$$L(E_\circ/\mathbb{F}_2, T) = 1 + 2T^2 = (1 - (\sqrt{2}i)T)(1 - (-\sqrt{2}i)T).$$

Lemma 8.5.

(1) *If c_1 is a cube in K^*, then* $\mathrm{NWN}(E_1/K) = \{i^r, (-i)^r\}$.
(2) *For $j = 2, 3$, if c_j is a cube in $(K')^*$, then* $\mathrm{NWN}(E_j/K') = \{i^{r'}, (-i)^{r'}\}$.

Proof. If c_1 is a cube in K^*, then there is an isomorphism $w : E_1 \to E_\circ$ defined over K, so part (1) follows from Lemmas 2.10 and 8.4. The proof for part (2) is similar. □

Lemma 8.6.

(1) *Suppose that c_1 is not a cube in K^*. If $r \equiv 2 \bmod 4$, then* $\mathrm{NWN}(E_1/K)$ *is* $\{\zeta_6, \bar{\zeta}_6\}$ *or* $\{-1, -1\}$. *If $r \equiv 0 \bmod 4$, then* $\mathrm{NWN}(E_1/K)$ *is* $\{\zeta_3, \bar{\zeta}_3\}$ *or* $\{1, 1\}$.
(2) *Suppose that c_j is not a cube in $(K')^*$ for $j = 2, 3$. If $r' \equiv 2 \bmod 4$, then* $\mathrm{NWN}(E_j/K')$ *is* $\{\zeta_6, \bar{\zeta}_6\}$ *or* $\{-1, -1\}$. *If $r' \equiv 0 \bmod 4$, then* $\mathrm{NWN}(E_j/K')$ *is* $\{\zeta_3, \bar{\zeta}_3\}$ *or* $\{1, 1\}$.

Proof. For part (1), if c_1 is not a cube in K^*, then it is a cube in K_3^*, where $K_3 \simeq \mathbb{F}_{q^3}$. By Lemma 8.5(1), $\mathrm{NWN}(E_1/K_3) = \{i^{3r}, (-i)^{3r}\} = \{i^r, (-i)^r\}$. If $r \equiv 2 \bmod 4$, then $\mathrm{NWN}(E_1/K_3) = \{-1, -1\}$, while if $r \equiv 0 \bmod 4$, then $\mathrm{NWN}(E_1/K_3) = \{1, 1\}$. By Lemma 2.10, $\mathrm{NWN}(E_1/K)$ are the cube roots of $\mathrm{NWN}(E_1/K_3)$ and are complex conjugates. The proof for part (2) is similar. □

Lemmas 8.3(3), 8.5, and 8.6 determine $\underline{e}(X_{c,d}/K')$. When $h \notin \mathbb{F}_q$, this is not quite strong enough to prove Theorem 8.1, because it only gives information about the normalized Weil numbers over $\mathbb{F}_{q^2}$. We now determine more information using the Artin L-series $L(E_1/\mathbb{F}_q, T, \chi)$, where χ is the nontrivial character of $\mathbb{Z}/2\mathbb{Z}$. By Lemma 5.10(1) ([31, Chapter 9, page 130]),

$$L(X_{c,d}/\mathbb{F}_q, T) = L(E_1/\mathbb{F}_q, T)L(E_1/\mathbb{F}_q, T, \chi). \tag{20}$$

Let ρ_1 be the coefficient of T in $L(E_1/K, T, \chi)$. Let I_1 (resp. S_1) be the number of K-points of E_1 that are inert (resp. split) in $X_{c,d}$. By Lemma 5.10(2), $\rho_1 = S_1 - I_1$. The conditions of Remark 5.12(3) are satisfied if $\mathrm{Tr}_r(c) = 1$, so $\rho_1 = 0$ by (15).

Proposition 8.7. *Let $K = \mathbb{F}_q$ where $q = 2^r$. Let $K' = K(h)$ where h is such that $h^2 + h = c$. The 2-valuation vector $\underline{e}(X_{c,d}/K) = \{e_1, e_2, e_3\}$ is determined below.*

$\underline{e}$	r odd	$r \equiv 2 \bmod 4$	$r \equiv 0 \bmod 4$
if $h \in \mathbb{F}_q$	$\{2,2,2\}$	$\{1,1,1\}$	$\{0,0,0\}$
if $h \notin \mathbb{F}_q$	$\{2,2,2\}$	$\{1,0,1\}$	$\{0,0,1\}$

Proof. When $h \in \mathbb{F}_q$, then $K' = K$. By Lemmas 8.5 and 8.6, $\mathrm{NWN}(X_{c,d}/K)$ are among the values $(\pm i)^r$ if r is odd, $\zeta_6, \bar{\zeta}_6, -1$ if $r \equiv 2 \bmod 4$, and $\zeta_3, \bar{\zeta}_3, 1$ if $r \equiv 0 \bmod 4$. Thus $\underline{e}(X_{c,d}/K)$ equals $\{2\}$ if r is odd, $\{1\}$ if $r \equiv 2 \bmod 4$, and $\{0\}$ if $r \equiv 0 \bmod 4$.

Suppose that $h \notin \mathbb{F}_q$. Then $\mathrm{NWN}(E_1/K)$ are the same as before; in particular, $e_1 = 2$ if r is odd, $e_1 = 1$ if $r \equiv 2 \bmod 4$, and $e_1 = 0$ if $r \equiv 0 \bmod 4$. By Lemmas 8.5 and 8.6, $\mathrm{NWN}(E_2/K')$ and $\mathrm{NWN}(E_3/K')$ are among -1 and $\zeta_6^{\pm 1}$ if r is odd, and 1 and $\zeta_3^{\pm 1}$ if r is even. Since K' is a quadratic extension of K, $\mathrm{NWN}(E_2/K)$ and $\mathrm{NWN}(E_3/K)$ are among the square roots of these. The ambiguity in taking the square root is resolved by the fact that the four sum to zero by (15) and are invariant under complex conjugation. If r is odd, then $\mathrm{NWN}(E_2/K) \cup \mathrm{NWN}(E_3/K)$ is either $\{\pm i, \pm i\}$ or $\{\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}\}$, which both yield $\{e_2, e_3\} = \{2, 2\}$. If r is even, then $\mathrm{NWN}(E_2/K) \cup \mathrm{NWN}(E_3/K)$ is either $\{1, 1, -1, -1\}$ or $\{\zeta_6, \zeta_6^{-1}, \zeta_3, \zeta_3^{-1}\}$ which both yield $\{e_2, e_3\} = \{0, 1\}$. □

8.3. The automorphism group of $X_{c,d}$ and K-Frobenius conjugacy classes

Let $G = \mathrm{Aut}_k(X_{c,d})$. Recall τ and υ from (19). Let $S_0 = \langle \tau, \upsilon \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Consider the order 3 automorphism of $X_{c,d}$, given by $\sigma : (S, Z) \mapsto (\zeta_3^2 S, Z)$. Note that σ is defined over $\mathbb{F}_q$ if r is even and over $\mathbb{F}_{q^2}$ if r is odd. Furthermore, σ centralizes S_0.

Lemma 8.8. *If $c \neq 1$, then $G = S_0 \times \langle \sigma \rangle$ is an abelian group of order 12. If $c = 1$, then G is a semidirect product of the form $S_0 \rtimes H$ where H is a cyclic group of order 9.*

Proof. The degree 4 equation (16) for $X_{c,d}$ is of the type whose automorphism group is studied in [36], see also [10, Section 12.1]. By [10, Theorem 12.11], G fixes the unique point of $X_{c,d}$ lying above $S = \infty$. Thus $G \simeq S_1 \rtimes H$ where S_1 is the normal Sylow 2-subgroup of G and H is a cyclic group of odd order. By [10, Theorem 12.7], $|S_1| = 4$ (so $S_1 = S_0$) and $|H|$ divides 9. Then $|H| = 3$ or 9 since $\sigma \in G$.

If H contains an element κ of order 9, then $\kappa(S) = \zeta_9 S$. Hence, κ acts on the right hand side of (16) by multiplication by ζ_3. However, κ can only act on the left hand side of (16) by multiplication by ζ_3 if the monomial $(1 + c)x^2$ vanishes. Thus, κ lifts to an automorphism of $X_{c,d}$ if and only if $c = 1$, in which case $\kappa(Z) = \zeta_3 Z$ and $\kappa : (S, Z) \mapsto (\zeta_9 S, \zeta_3 Z)$. □

If $c = 1$ and $|H| = 9$, note that $\kappa^3 = \sigma^2$; also G is non-abelian, since $\kappa\tau\kappa^{-1}(Z) = Z + \zeta_3^{-1}$, so $\kappa\tau\kappa^{-1}$ is either υ or $\upsilon\tau$, depending on the choice of $h \in \{\zeta_3, \zeta_3^2\}$. In this case, κ permutes the three quotients E_1, E_2, E_3 of $X_{c,d}$ by the non-trivial involutions in S_0.

Let $Fr = Fr_K$ where $K = \mathbb{F}_q$. We now determine the K-Frobenius conjugacy classes of G.

Lemma 8.9. *Let f be the number of K-Frobenius conjugacy classes in G.*

(1) *Suppose that $c \neq 1$. Then G is an abelian group of order* 12.
   (a) *If r is even and $h \in \mathbb{F}_q$, then $f = 12$.*
   (b) *If r is even and $h \notin \mathbb{F}_q$, then $f = 6$.*
   The classes are $\{\mathrm{id}, \tau\}$, $\{\upsilon, \upsilon\tau\}$, $\{\sigma, \sigma\tau\}$, $\{\upsilon\sigma, \upsilon\tau\sigma\}$, $\{\sigma^2, \sigma^2\tau\}$, $\{\upsilon\sigma^2, \upsilon\tau\sigma^2\}$.
   (c) *If r is odd and $h \in \mathbb{F}_q$, then $f = 4$.*
   The classes are $\{\mathrm{id}, \sigma, \sigma^2\}$, $\{\upsilon, \upsilon\sigma, \upsilon\sigma^2\}$, $\{\tau, \tau\sigma, \tau\sigma^2\}$, *and* $\{\upsilon\tau, \upsilon\tau\sigma, \upsilon\tau\sigma^2\}$.
   (d) *If r is odd and $h \notin \mathbb{F}_q$, then $f = 2$.*
   The classes are $\{\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ *and* $\{\upsilon, \upsilon\sigma, \upsilon\sigma^2, \upsilon\tau, \upsilon\tau\sigma, \upsilon\tau\sigma^2\}$.

(2) *If $c = 1$, then G is a non-abelian group of order* 36 *and $h \in \mathbb{F}_4 - \mathbb{F}_2$.*
   (a) *If r is even, then $h \in \mathbb{F}_q$ and $f = 10$.*
   The classes are $\{\mathrm{id}\}$, $\{\upsilon, \tau, \upsilon\tau\}$, *and* $\{\kappa^j, \upsilon\kappa^j, \tau\kappa^j, \upsilon\tau\kappa^j\}$ *for* $j = 1, \ldots, 8$.
   (b) *If r is odd, then $h \notin \mathbb{F}_q$ and $f = 2$. Also, υ is not conjugate to* id.
   The first class is $\{\mathrm{id}, \tau, \kappa^1, \ldots, \kappa^8, \upsilon\tau\kappa, \upsilon\kappa^2, \tau\kappa^3, \upsilon\tau\kappa^4, \upsilon\kappa^5, \tau\kappa^6, \upsilon\tau\kappa^7, \upsilon\kappa^8\}$.

Proof. We omit most of the long calculation. Cases (1a) and (2a) follow from the fact that K-Frobenius conjugacy classes coincide with standard conjugacy classes when all automorphisms are defined over K.

For the other cases, note that ${}^{Fr}\tau = \tau$. If $h \in \mathbb{F}_q$, then ${}^{Fr}\upsilon = \upsilon$. If $h \notin \mathbb{F}_q$, then $h^q = h + 1$ and ${}^{Fr}\upsilon = \upsilon\tau$; in this case, $\upsilon^{-1}\tau({}^{Fr}\upsilon) = \mathrm{id}$, showing that τ is K-Frobenius conjugate to id, and υ is K-Frobenius conjugate to $\upsilon\tau$.

Also, ${}^{Fr}\kappa = \kappa^q$. If r is even, then ${}^{Fr}\sigma = \sigma$. If r is odd, then ${}^{Fr}\sigma = \sigma^{-1}$; in this case, $\sigma^{-1}\mathrm{id}({}^{Fr}\sigma) = \sigma$, showing that σ is K-Frobenius conjugate to id. □

8.4. Proof of Theorem 8.1

Proof of Theorem 8.1. The results from Remark 5.12 apply here, by setting $S = S_0$. By Lemma 8.3(2), $\mathrm{Jac}(X_{c,d}) \sim_{K'} E_1 \oplus E_2 \oplus E_3$. By Lemma 8.3(1) and Remark 5.12(1), over K', the automorphism τ acts trivially on E_1 and by $[-1]$ on E_2 and E_3; similarly, υ fixes E_2 and acts by $[-1]$ on E_1 and E_3, and $\upsilon\tau$ fixes E_3 and acts by $[-1]$ on E_1 and E_2.

When $h \notin \mathbb{F}_q$, the strategy in the proof below is to analyze the situation for the base change to K', where the automorphism g acts via $g^{Fr_K} g$. The ambiguity caused by descending to K can be resolved using (15).

In each case below, the information on $\mathrm{NWN}(X_{c,d}/K)$ for $K = \mathbb{F}_q$ and their 2-adic valuations $\underline{e} = \underline{e}(X_{c,d}/K) = \{e_1, e_2, e_3\}$ is from Proposition 8.7. The data on the number and representatives of the K-twists of $X_{c,d}$ are found in Lemma 8.9.

(1) Let r be odd. Then $\underline{e} = \{2, 2, 2\}$ so $X_{c,d}$ has parity $+1$.
   (a) If $h \in \mathbb{F}_q$, then there are three nontrivial twists, each of order 2. By Lemma 5.11, none of these changes the parity, so $X_{c,d}$ is fully maximal.
   (b) If $h \notin \mathbb{F}_q$, then $K' = \mathbb{F}_{q^2}$. The nontrivial K-twist is represented by υ (which is not defined over $\mathbb{F}_q$). Then $\underline{e}(X_{c,d}/K') = \{1, 1, 1\}$. Over K', the twist for υ corresponds to $\upsilon^{Fr_K}\upsilon = \tau$, which negates the two conjugate pairs of normalized Weil numbers for E_2 and E_3, thus the twist has $\underline{e}(X'_{c,d}/K') = \{1, 0, 0\}$. By (15), $\underline{e}(X'_{c,d}/K) = \{2, 0, 1\}$, of parity -1. Thus, $X_{c,d}$ is mixed.

In addition, $\mathrm{Jac}(X_{c,d})$ and $X_{c,d}$ have the same type, by Lemma 5.3.

(2) Let $r \equiv 2 \bmod 4$.
   (a) If $h \in \mathbb{F}_q$, then $\underline{e} = \{1,1,1\}$, so $X_{c,d}$ has parity $+1$. There are either twelve K-twists (if $c \neq 1$) or ten K-twists (if $c = 1$). In both cases, the K-twist by υ has $\underline{e} = \{0,1,0\}$ and parity -1. Hence, both $X_{c,d}$ and $\mathrm{Jac}(X_{c,d})$ are mixed.
   (b) If $h \notin \mathbb{F}_q$, then $\underline{e} = \{1,0,1\}$, so $X_{c,d}$ has parity -1. Also, $\underline{e}(X_{c,d}/K') = \{0,0,0\}$. Since $c \neq 1$, there are six K-twists, represented by id, υ, σ, $\upsilon\sigma$, σ^2, and $\upsilon\sigma^2$. Twisting by $\mathrm{id}, \sigma, \sigma^2$ does not change the parity by Lemma 5.9 since these automorphisms have odd order and are defined over K. The twist of $X_{c,d}/K$ by υ (resp. $\upsilon\sigma$, $\upsilon\sigma^2$) corresponds to the twist of $X_{c,d}/K'$ by τ (resp. $\tau\sigma^2$, $\tau\sigma$), which changes $\underline{e}(X_{c,d}/K')$ to $\{0,1,1\}$. So the K-twist for υ (resp. $\upsilon\sigma$, $\upsilon\sigma^2$) has $\underline{e}(X_{c,d}/K)$ either $\{1,2,2\}$ or $\{0,2,2\}$, which both have parity -1. Thus $X_{c,d}$ is fully minimal over K. The twist by $[-1]$ has $\underline{e} = \{0,1,0\}$, thus $\mathrm{Jac}(X_{c,d})$ is fully minimal as well.

(3) Let $r \equiv 0 \bmod 4$.
   (a) If $h \in \mathbb{F}_q$, then $\underline{e} = \{0,0,0\}$, so $X_{c,d}$ has parity -1. There are either twelve K-twists (if $c \neq 1$) or ten K-twists (if $c = 1$). The nontrivial elements of S_0 yield twists such that $\underline{e} = \{1,1,0\}$, of parity -1, cf. Remark 5.12(1). The odd order automorphisms σ^j do not change the parity by Lemma 5.9. If $c \neq 1$, then all automorphisms are defined over K and the group is abelian, so no other twist changes the parity either. If $c = 1$, then the twists by κ^j permute E_1, E_2, E_3 and thus do not change the parity either. So $X_{c,d}$ is fully minimal. Since $\mathrm{Jac}(X_{c,d})$ has a twist with $\underline{e} = \{1,1,1\}$ and parity $+1$, it is mixed.
   (b) If $h \notin \mathbb{F}_q$, then $\underline{e} = \{0,0,1\}$, so $X_{c,d}$ has parity -1. The proof that both $X_{c,d}$ and $\mathrm{Jac}(X_{c,d})$ are fully minimal is very similar to case (2b). □

References

[1] Jeffrey D. Achter, Everett W. Howe, Split abelian surfaces over finite fields and reductions of genus-2 curves, Algebra Number Theory 11 (1) (2017) 39–76.
[2] Irene Bouw, Wei Ho, Beth Malmskog, Renate Scheidler, Padmavathi Srinivasan, Christelle Vincent, Zeta Functions of a Class of Artin–Schreier Curves with Many Automorphisms, Directions in Number Theory, Assoc. Women Math. Ser., vol. 3, Springer, Cham, 2016, pp. 87–124, MR 3596578.
[3] Gabriel Cardona, On the number of curves of genus 2 over a finite field, Finite Fields Appl. 9 (4) (2003) 505–526.
[4] Gabriel Cardona, Enric Nart, Zeta Function and Cryptographic Exponent of Supersingular Curves of Genus 2, Pairing-Based Cryptography—Pairing 2007, Lecture Notes in Comput. Sci., vol. 4575, Springer, Berlin, 2007, pp. 132–151.
[5] Jean-Marc Couveignes, Emmanuel Hallouin, Global descent obstructions for varieties, Algebra Number Theory 5 (4) (2011) 431–463.
[6] Pierre Deligne, La conjecture de Weil. I, Publ. Math. IHÉS 43 (1974) 273–307.
[7] Darren Glass, Rachel Pries, Hyperelliptic curves with prescribed p-torsion, Manuscr. Math. 117 (3) (2005) 299–317.
[8] Josep González, Jordi Guàrdia, Victor Rotger, Abelian surfaces of GL_2-type as Jacobians of curves, Acta Arith. 116 (3) (2005) 263–287.
[9] Ki-ichiro Hashimoto, Tomoyoshi Ibukiyama, On class numbers of positive definite binary quaternion Hermitian forms. II, J. Fac. Sci., Univ. Tokyo, Sect. 1A, Math. 28 (3) (1981) 695–699.
[10] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008, MR 2386879.
[11] Taira Honda, Isogeny classes of abelian varieties over finite fields, J. Math. Soc. Jpn. 20 (1968) 83–95.
[12] Everett W. Howe, Franck Leprévost, Bjorn Poonen, Large torsion subgroups of split Jacobians of curves of genus two or three, Forum Math. 12 (3) (2000) 315–364.
[13] Everett W. Howe, Daniel Maisner, Enric Nart, Christophe Ritzenthaler, Principally polarizable isogeny classes of abelian surfaces over finite fields, Math. Res. Lett. 15 (1) (2008) 121–127.
[14] Tomoyoshi Ibukiyama, On rational points of curves of genus 3 over finite fields, Tohoku Math. J. (2) 45 (3) (1993) 311–329.
[15] Tomoyoshi Ibukiyama, Toshiyuki Katsura, On the field of definition of superspecial polarized abelian varieties and type numbers, Compos. Math. 91 (1) (1994) 37–46.
[16] Tomoyoshi Ibukiyama, Toshiyuki Katsura, Frans Oort, Supersingular curves of genus two and class numbers, Compos. Math. 57 (2) (1986) 127–152.
[17] Jun-ichi Igusa, Class number of a definite quaternion with prime discriminant, Proc. Natl. Acad. Sci. USA 44 (1958) 312–314.
[18] E. Kani, M. Rosen, Idempotent relations and factors of Jacobians, Math. Ann. 284 (2) (1989) 307–327.
[19] Toshiyuki Katsura, Frans Oort, Families of supersingular abelian surfaces, Compos. Math. 62 (2) (1987) 107–167.

[20] Neal Koblitz, p-adic variation of the zeta-function over families of varieties defined over finite fields, Compos. Math. 31 (2) (1975) 119–218.
[21] Serge Lang, Abelian Varieties, Interscience Tracts in Pure and Applied Mathematics, vol. 7, Interscience Publishers, Inc., Interscience Publishers Ltd., New York, London, 1959.
[22] Kristin Lauter, Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields, J. Algebraic Geom. 10 (1) (2001) 19–36, with an appendix in French by J.-P. Serre.
[23] Ke-Zheng Li, Frans Oort, Moduli of Supersingular Abelian Varieties, Lecture Notes in Mathematics, vol. 1680, Springer-Verlag, Berlin, 1998.
[24] Daniel Maisner, Enric Nart, Abelian surfaces over finite fields as Jacobians, Exp. Math. 11 (3) (2002) 321–337, with an appendix by Everett W. Howe.
[25] Ju.I. Manin, Theory of commutative formal groups over fields of finite characteristic, Uspehi Mat. Nauk 18 (6(114)) (1963) 3–90.
[26] Stephen Meagher, Jaap Top, Twists of genus three curves over finite fields, Finite Fields Appl. 16 (5) (2010) 347–368.
[27] James S. Milne, Abelian varieties (v2.00), available at: www.jmilne.org/math/, 2008.
[28] James S. Milne, Jacobian varieties, available at: http://www.jmilne.org/math/, 2012.
[29] Frans Oort, Subvarieties of moduli spaces, Invent. Math. 24 (1974) 95–119.
[30] Frans Oort, Abelian Varieties over Finite Fields, Higher-Dimensional Geometry over Finite Fields, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 16, IOS, Amsterdam, 2008, pp. 123–188.
[31] Michael Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.
[32] René Schoof, Nonsingular plane cubic curves over finite fields, J. Comb. Theory, Ser. A 46 (2) (1987) 183–211.
[33] Jean-Pierre Serre, Local Fields, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York–Berlin, 1979, translated from the French by Marvin Jay Greenberg.
[34] Jean-Pierre Serre, Galois Cohomology, Springer-Verlag, Berlin, 1997, translated from the French by Patrick Ion and revised by the author.
[35] Joseph H. Silverman, The Arithmetic of Elliptic Curves, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
[36] Henning Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern, Arch. Math. (Basel) 24 (1973) 615–631.
[37] Henning Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer-Verlag, Berlin, 1993.
[38] Henning Stichtenoth, Chao Ping Xing, On the structure of the divisor class group of a class of curves over finite fields, Arch. Math. (Basel) 65 (2) (1995) 141–150.
[39] John Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. 2 (1966) 134–144.
[40] John Tate, Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda), Séminaire Bourbaki, Vol. 1968/69: Exposés 347–363, Lecture Notes in Math., vol. 175, Springer, Berlin, 1971, pp. 95–110.
[41] Gerard van der Geer, Marcel van der Vlugt, Supersingular curves of genus 2 over finite fields of characteristic 2, Math. Nachr. 159 (1992) 73–81.
[42] Gerard van der Geer, Marcel van der Vlugt, On the existence of supersingular curves of given genus, J. Reine Angew. Math. 458 (1995) 53–61.
[43] Paulo H. Viana, Jaime E.A. Rodriguez, Eventually minimal curves, Bull. Braz. Math. Soc. (N. S.) 36 (1) (2005) 39–58.
[44] William C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. Éc. Norm. Supér. (4) 2 (1969) 521–560.
[45] André Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Actual. Sci. Ind., vol. 1041, Hermann et Cie, Paris, 1948.
[46] André Weil, Variétés abéliennes et courbes algébriques, Actual. Sci. Ind., vol. 1064, Hermann & Cie, Paris, 1948.
[47] Jiangwei Xue, Tse-Chung Yang, Chia-Fu Yu, On superspecial abelian surfaces over finite fields, Doc. Math. 21 (2016) 1607–1643, MR 3603930.