Fully maximal and fully minimal abelian varieties and curves

Rachel Pries

Colorado State University
pries@math.colostate.edu

Arithmetic Aspects of Explicit Moduli Problems
May 29 - June 2, 2017

Motivating question

Let $\mathbb{F}_q$ be a finite field, with cardinality $q = p^r$.
Let $X/\mathbb{F}_q$ be a smooth projective curve of genus g.

Ill-posed question

If X is supersingular, is it more likely to be maximal or minimal?

Outline (joint with V. Karemaker).

1. Definitions of maximal, minimal, supersingular curves.
2. A twisted example.
3. Definitions of fully maximal, mixed, fully minimal curves.
4. Results
5. Arithmetic analysis for the explicit moduli space $g = 3$, $p = 2$.
6. Open questions

1. Zeta functions of curves

Let $X/\mathbb{F}_q$ be a smooth curve of genus g.

Weil Conjectures

The zeta function of $X/\mathbb{F}_q$ is a rational function

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

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

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

Note that $P(\mathrm{Jac}(X)/\mathbb{F}_q, T) = T^{2g} L(X/\mathbb{F}_q, T^{-1})$ is the characteristic polynomial of the relative Frobenius endomorphism of $\mathrm{Jac(X)}$.

Let $\{\alpha_1, \bar{\alpha}_1, \ldots, \alpha_g, \bar{\alpha}_g\}$ be the Weil numbers of $X/\mathbb{F}_q$.

1. Hasse-Weil bound and maximal/minimal

Let $\{\alpha_1, \bar{\alpha}_1, \ldots, \alpha_g, \bar{\alpha}_g\}$ be the Weil numbers of $X/\mathbb{F}_q$.
The normalized Weil numbers are $\{z_1, \bar{z}_1, \ldots, z_g, \bar{z}_g\}$ where $z_i = \alpha_i/\sqrt{q}$.

Hasse-Weil

The number of points satisfies $\#X(\mathbb{F}_q) = q + 1 - \sum_{i=1}^{g}(\alpha_i + \bar{\alpha}_i)$, which implies the *Hasse-Weil bound*: $|\#X(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$.

Definition

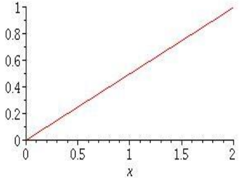
The curve $X/\mathbb{F}_q$ is *maximal* (resp. *minimal*) if its normalized Weil numbers all equal -1 (resp. 1). Need q square (r even).

Note that $X/\mathbb{F}_q$ is maximal if and only if $L(X/\mathbb{F}_q, T) = (1 + \sqrt{q}T)^{2g}$ and minimal if and only if $L(X/\mathbb{F}_q, T) = (1 - \sqrt{q}T)^{2g}$.

Fact: if $X/\mathbb{F}_q$ has NWNs $\{z_1, \bar{z}_1, \ldots, z_g, \bar{z}_g\}$,
then $X/\mathbb{F}_{q^m}$ has NWNs $\{z_1^m, \bar{z}_1^m, \ldots, z_g^m, \bar{z}_g^m\}$.

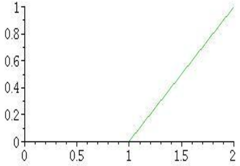
If $E/\mathbb{F}_q$ is an elliptic curve, then $\#E(\mathbb{F}_q) = q + 1 - a$.
The zeta function of E is $Z(E/\mathbb{F}_q, T) = (1 - aT + qT^2)/(1 - T)(1 - qT)$.

E supersingular if the Newton polygon of $1 - aT + qT^2$ has slopes $1/2$.



called $G_{1,1}$.

E ordinary if the Newton polygon has slopes 0 and 1.



called $G_{0,1} \oplus G_{1,0}$.

Fact: $p \mid a$ iff E supersingular.

1. Facts about supersingular elliptic curves

For all p, there exists a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ (Igusa).
The number of isomorphism classes of ss $E/\bar{\mathbb{F}}_p$ is $\lfloor \frac{p}{12} \rfloor + \varepsilon$.

E is supersingular iff $\mathrm{End}(E)$ non-commutative (order in quat. algebra)

Example: $p \equiv 3 \bmod 4$: $y^2 = x^3 - x$.
Example: $p \equiv 2 \bmod 3$: $y^2 = x^3 + 1$.

E is supersingular iff the Cartier operator annihilates $H^0(E, \Omega^1)$.

p odd: $y^2 = h(x)$, where $h(x)$ cubic with distinct roots, is supersingular iff the coefficient c_{p-1} of x^{p-1} in $h(x)^{(p-1)/2}$ is zero.
(Igusa) $y^2 = x(x-1)(x-\lambda)$ is supersingular for $\frac{p-1}{2}$ choices of $\lambda \in \overline{\mathbb{F}}_p$.

E supersingular iff its only p-torsion point is the identity:
$E[p](\bar{\mathbb{F}}_p) = \{\mathrm{id}\}$.

1. Definition of Newton polygon

Let X be a smooth projective curve defined over $\mathbb{F}_q$, with $q = p^r$.
Zeta function of X is $Z(X/\mathbb{F}_q, T) = L(X/\mathbb{F}_q, T)/(1-T)(1-qT)$

where $L(X/\mathbb{F}_q, T) = \prod_{i=1}^{2g}(1-\alpha_i T) \in \mathbb{Z}[T]$ and $|\alpha_i| = \sqrt{q}$.

The Newton polygon of X is the NP of the L-polynomial.
Find p-adic valuation v_i of coefficient of T^i in $L(X/\mathbb{F}_q, T)$.
Draw lower convex hull of $(i, v_i/r)$ where $q = p^r$.

Facts: The NP goes from $(0,0)$ to $(2g, g)$.
NP line segments break at points with integer coefficients;
If slope λ occurs with length m_λ, so does slope $1-\lambda$.

Definition

$X/\mathbb{F}_q$ is *supersingular* if the Newton polygon of $L(X/\mathbb{F}_q, t)$ is a line segment of slope $1/2$.

1. The supersingular property

Let X be a smooth projective curve defined over $\mathbb{F}_q$, with $q = p^r$.
The following are equivalent:

1. X is supersingular;
2. the Newton polygon of $L(X/\mathbb{F}_q, T)$ is a line segment of slope $1/2$;
3. each eigenvalue of the relative Frobenius morphism equals $\zeta\sqrt{q}$ for some root of unity ζ;
4. X is minimal (satisfies lower bound in Hasse-Weil bound for number of points) over $\mathbb{F}_{q^r}$ for some r;
5. $\text{Tate: End}(\text{Jac}(X \times_{\mathbb{F}_q} k)) \otimes \mathbb{Q}_p \simeq M_g(D_p)$, D_p quat alg ram at p, ∞;
6. $\text{Oort: Jac}(X)$ is geometrically isogenous to a product of supersingular elliptic curves.

6. Existence of supersingular curves?

For all p and g, there exists:
a supersingular p.p. *abelian variety* of dimension g, namely E^g;
and a supersingular *singular* curve of genus g.

Open Question 1:

Does there exist a supersingular smooth curve of genus g defined over a finite field of characteristic p, for every p and g?

Yes: $g = 1, 2, 3$ for all p. Not known for all p when $g \geq 4$.

Yes when $p = 2$ (Van der Geer/Van der Vlugt) then there exists a supersingular curve of every genus.

1. Period and parity

If $X/\mathbb{F}_q$ is supersingular, then $\{z_1, \bar{z}_1, \ldots, z_g, \bar{z}_g\}$ are roots of unity.

Definition

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

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

Then $X/\mathbb{F}_{q^{\mu(X)}}$ is maximal in case (i) and minimal in case (ii).

Better question:

If $X/\mathbb{F}_q$ is supersingular, is it more likely to have parity 1 or -1?

2. A curve of mixed type

Let $X/\mathbb{F}_p$ be plane curve $x^d + y^d + z^d = 0$. Note $g = (d-1)(d-2)/2$.

Example

If $p \equiv -1 \bmod d$, then X is maximal over $\mathbb{F}_{p^2}$. But if $d \equiv 0 \bmod 4$, then X has a twist which is not maximal over any extension of $\mathbb{F}_p$.

Proof.

The Hermitian curve $\tilde{X} : x_1^{p+1} + y_1^{p+1} + z_1^{p+1} = 0$ is maximal over $\mathbb{F}_{p^2}$.

Since $p+1 \equiv 0 \bmod d$, there exists $\lambda \in \mathbb{F}_{p^2}^*$ with order $s = (p+1)/d$.
There is a Galois cover $h : \tilde{X} \to X$ given by $(x_1, y_1, z_1) \mapsto (x_1^s, y_1^s, z_1^s)$.
So X is a quotient of $\tilde{X}$ by a subgroup of automorphisms def. over $\mathbb{F}_{p^2}$.

By Serre, X is also maximal over $\mathbb{F}_{p^2}$, proving the first claim. □

The NWNs of $X/\mathbb{F}_{p^2}$ are all -1. The NWNs of $X/\mathbb{F}_p$ are $\pm i$ (mult. g).

2. A curve $x^d + y^d + z^d = 0$ of mixed type continued

Let $p \equiv -1 \bmod d$ and $4 \mid d$.
Let $\lambda_1 \in \mathbb{F}_{p^2}^*$ have order $d_1 = d/2$.

Let $g \in \mathrm{Aut}_{\mathbb{F}_{p^2}}(X)$ be the automorphism $g(x,y,z) = (\lambda_1 y, x, z)$.
Note g has order d.

Let $X_g/\mathbb{F}_p$ be the twist of X by g.
Fact: the NWNs of $X_g/\mathbb{F}_{p^2}$ depend on the action of $g({}^{Fr}g)$.

We compute that

$$\begin{aligned} g({}^{Fr}g)(x,y,z) &= g(FrgFr^{-1})(x,y,z) \\ &= g(Fr(g(x^{1/p}, y^{1/p}, z^{1/p}))) \\ &= g(Fr(\lambda_1 y^{1/p}, x^{1/p}, z^{1/p})) = g(\lambda_1^p y, x, z) \\ &= (\lambda_1 x, \lambda_1^p y, z) = (\lambda_1 x, \lambda_1^{-1} y, z), \end{aligned}$$

where the last equality uses the fact that $p \equiv -1 \bmod d$.

2. A curve $x^d + y^d + z^d = 0$ of mixed type continued

Claim: Case 1. $d = 4$

Then $X : x^4 + y^4 + z^4 = 0$ has a twist which is not maximal over $\mathbb{F}_{p^m}$.

Proof.

Auer/Top: $\mathrm{Jac}(X) \sim_{\mathbb{F}_p} E^3$, where $E : 2y^2 = x^3 - x$ is maximal over $\mathbb{F}_{p^2}$.
The NWNs of $X/\mathbb{F}_{p^2}$ are $\{-1, \ldots, -1\}$ (maximal).

Now g has order 4 and the quotient of X by g has genus 1.
Since $i \notin \mathbb{F}_p$, g acts on $\mathrm{Jac}(X)$ via two invariant factors, with minimal polynomials $x^2 + 1$ and $x - 1$.
Note $g({}^{Fr}g) = g^2$ acts with eigenvalues $-1, -1, 1$ on $\mathrm{Jac}(X)/\mathbb{F}_{p^2}$.

Then the twist $X_g/\mathbb{F}_{p^2}$ has NWNs $\{1, 1, 1, 1, -1, -1\}$.
Thus the NWNs of the twist $X_g/\mathbb{F}_p$ are ± 1 (mult. 4) and $\pm i$.
Hence, the twist $X_g/\mathbb{F}_p$ is not maximal over any extension of $\mathbb{F}_p$. □

2. A curve $x^d + y^d + z^d = 0$ of mixed type continued

Claim:

Then $X : x^d + y^d + z^d = 0$ has a twist which is not maximal over $\mathbb{F}_{p^m}$.

Proof.

The NWNs of $X/\mathbb{F}_{p^2}$ are all -1.

The NWNs of the twist $X_g/\mathbb{F}_{p^2}$ include $-\varepsilon$ for ε eigenvalue for action of $g({}^{Fr}g)$ on $H^1(X, \mathcal{O})$. This includes $\varepsilon = 1$ and $\varepsilon = \lambda_1$.

Now -1 has order 2 but $-\lambda_1$ does not: (because $d_1 = d/2$ is even, so $-\lambda_1$ has order d_1 if $d_1 \equiv 0 \bmod 4$ and has odd order if $d_1 \equiv 2 \bmod 4$).

In either case, the twist $X_g/\mathbb{F}_p$ is not maximal over any extension of $\mathbb{F}_p$ since the 2-divisibility of the orders of its NWNs is not constant. □

3. Fully maximal/minimal abelian varieties and curves

(joint with Valentijn Karemaker)

Abstract: We introduce and study a new way to catagorize supersingular abelian varieties or curves 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 over its minimal field of definition.

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.

For supersingular curves of genus 3 in characteristic 2, we use a parametrization of a moduli space of such curves by Viana and Rodriguez to determine the L-polynomial and the type of each.

3. Definitions of fully maximal, fully minimal, mixed

Let $K = \mathbb{F}_q$ and $k = \bar{\mathbb{F}}_p$.
Let $X/\mathbb{F}_q$ be a smooth projective curve of genus g.

A twist of X/K is a curve X'/K for which there exists a geometric isomorphism $\phi : X \times_K k \to X' \times_K k$.

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

Definition of type: KP

A supersingular curve X with minimal field of definition K is of one of the following *types*:

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 $\delta(X'') = -1$.

3. Mixed is not the same as hyperelliptic

If a maximal curve has a minimal twist, then X is hyperelliptic

Suppose that $\phi : X \times_K k \overset{\simeq}{\to} X' \times_K k$ where X/K is maximal and X'/K is minimal (or vice versa). Then X is hyperelliptic and $g_\phi = \iota$ and X'/K is a quadratic twist.

Despite this:
There are mixed curves that are not hyperelliptic (example above) and hyperelliptic curves that are not mixed (examples below).

The mixed property depends on more data:
NWNs of X over minimal field of definition K
orders of twists (K-Frobenius order of elements in Frobenius conjugacy classes in $\mathrm{Aut}_k(X)$)

Analysis $g = 1$

Proposition: K/P

Let E be a supersingular elliptic curve defined over a finite field of characteristic p. If E is defined over $\mathbb{F}_p$, then it is fully maximal; otherwise, it is mixed.

Proof: (uses work of Waterhouse)
$p = 2$, all twists of $y^2 + y = x^3$ have parity 1.

p odd and $\mathrm{Aut}_k(E) \not\simeq \mathbb{Z}/2$:
All twists of $y^2 = x^3 + 1$ ($j = 0$) and $y^2 = x^3 - x$ ($j = 1728$) have parity 1.

p odd and $\mathrm{Aut}_k(E) \simeq \mathbb{Z}/2$:
If defined over $\mathbb{F}_p$ then NWNs are $\{\pm i\}$;
If not, then NWNs of E and E_ι are $\{1, 1\}$ and $\{-1, 1\}$
or $\{\zeta_3, \bar{\zeta}_3\}$ and $\{\zeta_6, \bar{\zeta}_6\}$, parity -1 and 1.

3. Twists

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

(Serre)

There are bijections:

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

Definition: $g, h \in \mathrm{Aut}_k(X)$ are *K-Frobenius conjugate* if there exists $\tau \in \mathrm{Aut}_k(X)$ such that $g = \tau^{-1} h({}^{Fr_K}\tau)$, where $({}^{Fr_K}\tau) = Fr_K \tau Fr_K^{-1}$.

Notation: X'/K a K-twist of X/K with $\phi : X \times_K k \xrightarrow{\simeq} X' \times_K k$.
Let ξ_ϕ and $g := g_\phi$ be the corresponding cocycle and automorphism.
Let K_{T_g} be the field of definition of ϕ (of degree T_g over K).

3. Facts about twists

K-Frobenius order

The degree T_g is the smallest positive integer T such that

$$g({}^{Fr_K}g)({}^{Fr_K^2}g)\cdots({}^{Fr_K^{T-1}}g) = \mathrm{id}.$$

Fact

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

$$\phi^{-1} \circ \pi' \circ \phi = \pi_X \circ G_\phi^{-1}. \quad (1)$$

3. the 2-divisibility of orders of NWNs

Suppose that $\{z_1, \bar{z}_1, \ldots, z_g, \bar{z}_g\}$ are the normalized Weil numbers of a supersingular curve X/K.
Recall that $z_1, \ldots, z_g$ are roots of unity.
We measure the 2-divisibility of their orders in the next definition.

Definition

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

Parity=1 (maximal over $\mathbb{F}_{q^m}$) iff $\underline{e} = \{e\}$ with $e \geq 1$ ($e \geq 2$ if r odd).

Twists that don't change $\vec{e}$

Suppose that X'/K is a twist of X/K of order T. Let $e_T = \mathrm{ord}_2(T)$.
If $e_T < \min\{e_i \mid 1 \leq i \leq g\}$, then $\underline{e}(X'/K) = \underline{e}$.

Characterizing the mixed case when $\mathrm{Aut}_k(A) \not\simeq \mathbb{Z}/2$

If X/K has parity $+1$ and its twist X'/K has parity -1, then the order T of the twist is even.

More precisely:

Suppose X/K has K-period M. Let $e_M = \mathrm{ord}_2(M)$.

Note that e_M is determined by the parity of X and $\underline{e}$, the 2-divisibility of the orders of the NWNs (roots of unity).

Let X'/K be a K-twist of order T. Let $e_T = \mathrm{ord}_2(T)$.

No switch of parity

If X/K has K-parity $+1$ and $e_T \leq e_M$, then X'/K also has K-parity $+1$.
If X/K has K-parity -1 and $e_T < e_M$, then X'/K also has K-parity -1.

General results: K/P

Let $q = p^r$. Let A be p.p. abelian variety of dimension g.

Corollary 1

If A is simple and r is even, then $A/\mathbb{F}_q$ is not fully minimal.

Proposition

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

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

Corollary 2

If $|\mathrm{Aut}_k(A)| = 2$, g is odd, and r is odd, then A is fully maximal.

Philosophical digression

Is the condition that $\mathrm{Aut}_k(A) \simeq \mathbb{Z}/2$ restrictive?

Open Question 2:

What is the automorphism group of A_η for η a geometric generic point of the supersingular locus $\mathcal{A}_{g,ss}$ of the moduli space of p.p. abelian varieties of dimension $g \geq 2$?

$g = 2$, p odd: Using Katsura/Oort, Achter/Howe, the proportion of supersingular p.p. $A/\mathbb{F}_{p^r}$ with $\mathrm{Aut}_k(A) \not\simeq \mathbb{Z}/2$ goes to 0 as $r \to \infty$.

(This is false when $g = 2$ and $p = 2$ by Van der Geer/Van der Vlugt).

$g = 3$, $p = 2$: we prove that automorphism group is $(\mathbb{Z}/2 \times \mathbb{Z}/2) \times \mathbb{Z}/3$ on an open, dense subset of $\mathcal{A}_{3,ss}$.

Philosophical digression continued

The proportion of $\mathbb{F}_q$-points of $\mathcal{A}_{g,ss}$ which represent abelian varieties A that are simple over K is not known in general.

Li/Oort: the generic supersingular abelian variety A_η has a-number 1 for all g and p.

If $\mathbb{Z}/2 \times \mathbb{Z}/2 \subset \mathrm{Aut}_K(A)$, then A is not simple over K by Kani/Rosen. If p is odd, this also implies that A has a-number at least 2.

So, for p odd, one expects the proportion of supersingular A/K with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset \mathrm{Aut}_K(A)$ to be small.

Analysis for $g = 2$

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

The typical situation is when $\mathrm{Aut}_k(A) \simeq \mathbb{Z}/2$. What types occur?

Proposition (KP):

Let A be a supersingular simple p.p. abelian surface with minimal field of definition $\mathbb{F}_{p^r}$. Assume $\mathrm{Aut}_k(A) \simeq \mathbb{Z}/2$.

If r is odd, then A is not mixed; Cases (1), (2b), (3a), (6) are fully maximal and Cases (2a), (5), (7a) are fully minimal.

If r is even, then A is not fully minimal; Cases (1), (3a), and (7b) are fully maximal and Cases (4) and (8) are mixed.

Cases as listed in following table.

Analysis for $g = 2$

First 4 columns from Maisner/Nart (see also HMNR)
Let $L/\mathbb{F}_q$ minimal over which $A \sim_L E_1 \times E_2$. Let $t_0 = \deg(L/\mathbb{F}_q)$. Let $n_E = n_{E_1} = n_{E_2}$ label E_1/L and E_2/L.
We compute z/L, one of the NWNs $(z, \bar{z}, z, \bar{z})$ of A/L. We compute $\mathrm{NWN}(A/\mathbb{F}_q)$. We compute the period P and parity δ of $A/\mathbb{F}_q$.

	(a_1, a_2)	r, p	t_0	n_E	z/L	$\mathrm{NWN}(A/\mathbb{F}_q)$	P	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 $p \neq 3$ 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 $p = 5$	5	1	± 1	$(\zeta_{10}^3, \zeta_{10}^7, \zeta_5^2, \zeta_5^3)$	10	-1
5b	$(-\sqrt{5q}, 3q)$	r odd and $p = 5$	5	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

Analysis when $g = 2$

Also deal with simple supersingular surfaces with $\mathrm{Aut}_k(A) \not\simeq \mathbb{Z}/2$.

Igusa: 6 equations of curves of genus 2 with $\mathrm{Aut}_k(X) \not\simeq \mathbb{Z}/2$.
Ibukiyama/Katsura/Oort - determine when these are supersingular.

Using Cardona/Nart, we determine the type for each of these.

Open Question 3:

What are the sizes of the isogeny classes listed in the table?

The answer to Open Question 3 would shed light on the probability that a supersingular abelian surface $A/\mathbb{F}_q$ is fully maximal, mixed, or fully minimal.

A procedure for studying parities of twists

The key information to retain about the normalized Weil numbers is the divisibility of their orders by 2.

We summarize this information in a multiset $\underline{e}(A/K)$.

The key information to retain about the twist is its effect on the NWNs, which can be controlled by the divisibility of its order T by 2.

If the structure of $\mathrm{Aut}_k(X)$ is complicated, then the order of the twist is not easily determined from the order of $g \in \mathrm{Aut}_k(X)$.

In particular, if G is non-abelian, then an automorphism g of order 2 can produce a twist of order 4.

5. Supersingular moduli for $g = 3$ and $p = 2$

When $p = 2$ and $g = 3$, the supersingular locus of the moduli space $\mathcal{M}_3 \otimes \mathbb{F}_2$ is irreducible of dimension 2.

Viana and Rodriguez parametrize it by the 2-dimensional family

$$X_{a,b} : x + y + a(x^3y + xy^3) + bx^2y^2 = 0. \quad (2)$$

For each supersingular curve $X_{a,b}$ of genus 3 over a finite field of characteristic 2, we determine whether $X_{a,b}$ is fully maximal, fully minimal, or mixed.

This involves an analysis of twists by $g \in \mathrm{Aut}_k(X_{a,b})$, which is a group of order either 12 or 36.

In fact, we determine $L(X_{a,b}/K, T)$ almost completely.

(See related results by Nart/Ritzenthaler).

Main result when $g = 3$ and $p = 2$

Let $K = \mathbb{F}_{2^r}$ be the smallest field containing a, b.
Let $h \in \mathbb{F}_{q^2}$ be such that $h^2 + h = \frac{a}{b}$. Note that $h \in \mathbb{F}_q$ iff $\mathrm{Tr}_r(\frac{a}{b}) = 0$, where $\mathrm{Tr}_r : \mathbb{F}_{2^r} \to \mathbb{F}_2$ denotes the trace map. Let $K' = \mathbb{F}_q(h)$.

Theorem K/P:

1. If r is odd, then $X_{a,b}$ 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 $X_{a,b}$ is fully minimal if $h \notin \mathbb{F}_q$ and mixed if $h \in \mathbb{F}_q$.
3. If $r \equiv 0 \bmod 4$, then $X_{a,b}$ is fully minimal.

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

The proportion of $(a, b) \in (\mathbb{F}_q^*)^2$ for which $X_{a,b}$ is mixed is slightly greater than $\frac{1}{2}$ when r is odd and slightly smaller than $\frac{1}{2}$ when $r \equiv 2 \bmod 4$.

The L-polynomial of $X_{a,b}$ over K'

For $K = \mathbb{F}_{2^r}$, define

$$L_{c,K}(T) = (1 - (\sqrt{2}i)^r T)(1 - (-\sqrt{2}i)^r T), \tag{3}$$

and, when r is even, define

$$L_{n,K}(T) = (1 - (2\zeta_6)^{r/2} T)(1 - (2\zeta_6^{-1})^{r/2} T). \tag{4}$$

The NWNs are $\{(\pm i)^r\}$ for $L_{c,K}(T)$ and $\{\zeta_6^{r/2}, \zeta_6^{-r/2}\}$ for $L_{n,K}(T)$.

Proposition

Let $K' = \mathbb{F}_q(h)$, where $h \in \mathbb{F}_{q^2}$ is such that $h^2 + h = \frac{a}{b}$.
Define $c_1 = ab$, $c_2 = (\frac{1}{h+1})^2 \frac{1}{b}$, $c_3 = (\frac{1}{h})^2 \frac{1}{b}$.
Then $L(X_{a,b}/K', T) = L_{c,K'}(T)^m L_{n,K'}(T)^{3-m}$, where
$m = \#\{i \in \{1,2,3\} \mid c_i \text{ is a cube in } (K')^*\}$.

Key facts about the geometry of $X_{a,b}$

$X_{a,b}$ has an involution $\tau(x,y) = (y,x)$ and the quotient is
$E_1 : R^2 + R = c_1 S^3$.
The cover $X_{a,b} \to E_1$ has equation $Z^2 + Z = \frac{a}{b} R$.
The involution $\upsilon : R \mapsto R+1$ on E_1 lifts to $X_{a,b}$, via $\upsilon(Z) = Z + h$.
Let $E_2 : T^2 + T = c_2(aS)^3$ and $E_3 : U^2 + U = c_3(aS)^3$.

Lemma

1. The cover $X_{a,b} \to E_{a,b} \to \mathbb{P}^1_S$ is Galois with group $S_0 = \langle \tau, \upsilon \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and equation
$$Z^4 + (1 + \frac{a}{b})Z^2 + \frac{a}{b} Z = \frac{1}{b} a^3 S^3.$$
2. Over K', the quotients of $X_{a,b}$ by τ, υ and $\tau\upsilon$ are E_1, E_2, and E_3.
3. Finally, $\mathrm{Jac}(X_{a,b}) \sim_{K'} E_1 \oplus E_2 \oplus E_3$.

The L-polynomial of $X_{a,b}$ over K

When $h \notin \mathbb{F}_q$, this is not quite strong enough, because it only gives information about the L-polynomial over $\mathbb{F}_{q^2}$.

This ambiguity can be partially resolved using the Artin L-series $L(E_{a,b}/\mathbb{F}_q, T, \chi)$, where χ is the nontrivial character of $\mathbb{Z}/2\mathbb{Z}$.

Note $L(X_{a,b}/\mathbb{F}_q, T) = L(E_{a,b}/\mathbb{F}_q, T)L(E_{a,b}/\mathbb{F}_q, T, \chi)$.

Let ρ_1 be the coefficient of T in $L(E_{a,b}/K, T, \chi)$.

Let I_1 (resp. S_1) be the number of K-points of $E_{a,b}$ that are inert (resp. split) in $X_{a,b}$. Then $\rho_1 = S_1 - I_1$.

Using quadratic twists, one can see that $\rho_1 = 0$.

This suffices to determine $\underline{e}(X_{a,b}/K)$.

The twists of $X_{a,b}$

Let $G = \mathrm{Aut}_k(X_{a,b})$. It contains $S_0 = \langle \tau, \upsilon \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

There is an order 3 automorphism of $X_{a,b}$, given by

$$\sigma : (x,y) \mapsto (\zeta_3 x, \zeta_3 y) \text{ or } \sigma : (S,R,Z) \mapsto (\zeta_3^2 S, R, Z).$$

Note that σ is defined over $\mathbb{F}_q$ if r is even and over $\mathbb{F}_{q^2}$ if r is odd. Also, σ centralizes S_0.

Lemma

If $a \neq b$, then $G = S_0 \times \langle \sigma \rangle$ is an abelian group of order 12.
If $a \neq b$, then G is a semidirect product $S_0 \rtimes H$ where H is a cyclic group of order 9.

Example: $X_{a,b}$ is fully maximal when r odd and $h \in \mathbb{F}_q$

Let r be odd and $h \in \mathbb{F}_q$.

The L-polynomial shows that NWNs are $\pm i$ (multiplicity 3).

So $\underline{e} = \{2,2,2\}$ and $X_{a,b}$ has parity 1.

There are 4 Frobenius conjugacy classes of twists, represented by elements of S_0, which are defined over K and thus have order $T = 2$. So $e_T = 1$.

This means the twists do not change $\underline{e}$, so all twists have parity 1.

Example: $X_{a,b}$ is mixed when r odd and $h \notin \mathbb{F}_q$

Let r be odd and $h \notin \mathbb{F}_q$.

The L-polynomial shows that the NWNs are in $\{\pm i\} \cup \mu_{12}$.
In any case, $\underline{e}(X_{a,b}/K) = \{2,2,2\}$ so $X_{a,b}$ has parity 1.

There are 2 Frobenius conjugacy classes, thus one non-trivial twist, which is represented by υ.

Over K', $\underline{e}(X_{a,b}/K') = \{1,1,1\}$.

The nontrivial twist corresponds to $\upsilon^{Fr_K}\upsilon = \tau$, which negates the two conjugate pairs of NWNs for E_2 and E_3.

Thus the twist has $\underline{e}(X'_{a,b}/K') = \{1,0,0\}$.
One checks that $\underline{e}(X'_{a,b}/K) = \{2,0,1\}$, of parity -1.

Thus, $X_{a,b}$ is mixed.

6. Why supersingular Jacobians are unlikely

Let $\mathcal{A}_g$ be the moduli space of p.p. abelian varieties of dimension g.
The image of $\mathcal{M}_g$ in $\mathcal{A}_g$ is open and dense for $g \leq 3$.
Observation (Oort 2005) $\dim(\mathcal{A}_g) = g(g+1)/2$ and
the dimension of the supersingular locus $\mathcal{A}_{g,ss}$ is $\lfloor g^2/4 \rfloor$.

The difference δ_g is length of longest chain of NPs connecting the supersingular NP σ_g to the ordinary NP ν_g.

If $g \geq 9$, then $\delta_g > 3g - 3 = \dim(\mathcal{M}_g)$.

Either (i) $\mathcal{M}_g$ does not admit a perfect stratification by NP
(i.e., there are two NPs ξ_1 and ξ_2 such that $\mathcal{A}_g[\xi_1]$ is in the closure of $\mathcal{A}_g[\xi_2]$ but $\mathcal{M}_g[\xi_1]$ is not in the closure of $\mathcal{M}_g[\xi_2]$.)

or (ii) some NPs do not occur for Jacobians of smooth curves.

Test case: $g = 11$ with NP $G_{5,6} \oplus G_{6,5}$ having slopes of $5/11, 6/11$
(does occur when $p = 2$ - Blache).

Supersingular case sometimes does not occur among wildly ramified covers

Deuring-Shafarevich formula restricts p-rank.

Oort: If $p = 2$, there does not exist a hyperelliptic supersingular curve of genus 3.

Scholten/Zhu: $p = 2$, $n \geq 2$, there is no hyperelliptic supersingular curve with $g = 2^n - 1$.

(for odd p, generalized for Artin-Schreier covers $X \stackrel{\mathbb{Z}/p}{\to} \mathbb{P}^1$ by Blache, who studied first slope of NP of more general AS curves)

But.....

Van der Geer/Van der Vlugt: If $p = 2$, then there exists a supersingular curve of every genus.

Supersingular Artin-Schreier curves

Def: $R[x] \in k[x]$ is an additive polynomial if $R(x_1 + x_2) = R(x_1) + R(x_2)$.
Then $R[x] = c_0 x + c_1 x^p + c_2 x^{p^2} + c_h x^{p^h}$.

Supersingular Artin-Schreier curves VdG/VdV

If $R(x) \in k[x]$ is an additive polynomial of degree p^h, then
$X : y^p - y = xR(x)$ is supersingular with genus $p^h(p-1)/2$.

Proof: Induction on h, starting with $h = 0$.
Key fact: $\mathrm{Jac}(X)$ is isogenous to a product of Jacobians of Artin-Schreier curves for additive polynomials of smaller degree.

Remark: BHMSSV studied L-polynomials, automorphism groups of X.

Existence of supersingular curves when $p = 2$

Van der Geer and Van der Vlugt

If $p = 2$, then there exists a supersingular curve over $\overline{\mathbb{F}}_2$ of every genus.

Proof sketch: Expand g as (with $s_i \leq s_{i-1} + r_{i-1} + 2$)
$g = 2^{s_1}(1 + 2 + \cdots + 2^{r_1}) + 2^{s_2}(1 + 2 + \cdots 2^{r_2}) + \cdots + 2^{s_t}(1 + 2 + \cdots + 2^{r_t})$.

Let $\mathbf{L} = \oplus_{i=1}^{t} L_i$ for L_i subspace of dim $d_i := r_i + 1$ in vector space of additive polynomials of deg 2^{u_i}, with $u_i = (s_i + 1) - \sum_{j=1}^{i-1}(r_j + 1)$.

If $f \in \mathbf{L}$, let $C_f : y^p - y = xf$. Let Y be fiber product of $C_f \to \mathbb{P}^1$ for all $f \in \mathbf{L}$. Then $J_Y \sim \oplus_{f \neq 0} J_{C_f}$ (thus supersingular). Also, $g_Y = \sum_{f \neq 0} g_{C_f}$.

The number of $f \in \mathbf{L}$ which have a non-zero contribution from L_i, but not from L_j for $j > i$, is $(2^{d_i} - 1)\prod_{j=1}^{i-1} 2^{d_j}$. Each adds $2^{u_i - 1}$ to g.
So $g_Y = \sum_{i=1}^{t}(2^{d_i} - 1)\prod_{j=1}^{i-1} 2^{d_j} 2^{u_i - 1} = \sum_{i=1}^{t} 2^{s_i}(1 + \cdots + 2^{r_i}) = g$.

Supersingular Artin-Schreier curves for odd p

Here is what VdG/VdV's method produces for odd p.

Proposition: K/P

Let $g = Gp(p-1)^2/2$ where $G = \sum_{i=1}^{t} p^{s_i}(1+p+\cdots p^{r_i})$. Then there exists a supersingular curve over $\overline{\mathbb{F}}_p$ of genus g.

VdG/VdV also prove that there exists a supersingular curve defined over $\mathbb{F}_2$ of every genus. The construction is a little more complicated.

An accessible open question

Open Question 4:

Determine the type (fully maximal, mixed, fully minimal) for known classes of supersingular curves:

$g = 2$, $p = 2$: Van der Geer/Van der Vlugt;

$g = p^h(p-1)/2$, $X : y^p - y = xR(x)$, Bouw/Ho/Malmskog/Scheidler/Srinivasan/Vincent;

arbitrary g, over $\mathbb{F}_2$: Van der Geer/Van der Vlugt;

the odd p generalization of the previous line;

covers of Hermitian curve: Gieulietti/Korchmáros, Garcia/Gúneri/Stichtenoth.