Fully maximal and minimal supersingular abelian varieties

Valentijn Karemaker (University of Pennsylvania)

Joint with R. Pries

Arithmetic, Geometry, Cryptography, and Coding Theory, CIRM

June 19, 2017

Supersingular abelian varieties

Let $q = p^r$, $K = \mathbb{F}_q$, $k = \overline{\mathbb{F}}_q$.
Let A be a g-dimensional abelian variety defined over K.
(We will always assume A to be principally polarised.)

Let π_A be the relative Frobenius endomorphism of A.
The roots $\{\alpha_1, \overline{\alpha}_1, \dots, \alpha_g, \overline{\alpha}_g\}$ of its characteristic polynomial $P(A/K, T)$ are the *Weil numbers* of A/K.
These have absolute value $\sqrt{q}$.
Let $\{z_i = \frac{\alpha_i}{\sqrt{q}}, \overline{z}_i\}_{1 \leq i \leq g}$ be the *normalised Weil numbers* of A/K.

Definition (supersingular)

An elliptic curve E is *supersingular* if $E[p](k) = \{0\}$.
A is *supersingular* if $A \times k \sim E^g \times k$ where E is supersingular, or equivalently, if its normalised Weil numbers are roots of unity.

Maximal and minimal abelian varieties

Definition (maximal/minimal)

A/K is *maximal* (*minimal*) if all its normalised Weil numbers are -1 (1).

If the Weil numbers of $A/\mathbb{F}_q$ are $\{\alpha_i, \overline{\alpha}_i\}_{1\leq i\leq g}$, then those of $A/\mathbb{F}_{q^m}$ are $\{\alpha_i^m, \overline{\alpha}_i^m\}_{1\leq i\leq g}$. Hence:

- If $A/\mathbb{F}_q$ is maximal or minimal, then A is supersingular.
- If $A/\mathbb{F}_q$ is supersingular, then A is minimal over some $\mathbb{F}_{q^m}$.

Question

When does a supersingular A/K become maximal before it becomes minimal?

Period and parity

Definition (period)

The ($\mathbb{F}_q$-)*period* of $A/\mathbb{F}_q$ is the smallest $m \in \mathbb{N}_{>0}$ such that $A/\mathbb{F}_{q^m}$ is either maximal ($z_i = -1\ \forall i$) or minimal ($z_i = 1\ \forall i$); rm is even.

Definition (parity)

The ($\mathbb{F}_q$-)*parity* of $A/\mathbb{F}_q$ is $+1$ (-1) if A first becomes maximal (minimal).

Example. Consider $E/\mathbb{F}_2 : y^2 + y = x^3$.
$E(\mathbb{F}_2) = \{(0,1),(0,0),\mathcal{O}\}$ so $|E(\mathbb{F}_2)| = 3$ and $\mathrm{Tr}(\pi_E) = 0$.
So $P(E/\mathbb{F}_2, T) = T^2 + 2 = (T - \sqrt{-2})(T + \sqrt{-2})$.
The normalised Weil numbers of $E/\mathbb{F}_2$ are $\{i, -i\}$.
Hence, the normalised Weil numbers of $E/\mathbb{F}_4$ are $\{-1, -1\}$.
So E has $\mathbb{F}_2$-period 2 and $\mathbb{F}_2$-parity $+1$.

Twists

A K-twist of A/K is an abelian variety A'/K such that $A \simeq_k A'$.
Twists are classified by $[\xi] \in H^1(G_K, \mathrm{Aut}_k(A))$.
A and A' may have different Weil numbers!

Example. Consider $E/\mathbb{F}_3 : y^2 = x^3 - x$. Its NWN are $\{i, -i\}$.
Let $\alpha \in \mathbb{F}_{3^3}$ such that $\alpha^3 - \alpha = 1$. Then $(x, y) \mapsto (x - \alpha, y)$ yields a twist $E'/\mathbb{F}_3 : y^2 + 1 = x^3 - x$. Its NWN are $\{\frac{\sqrt{3}+i}{2}, \frac{\sqrt{3}-i}{2}\}$.

In general:

$$\begin{array}{ccc} A & \xrightarrow{\phi} & A' \\ \Big\downarrow{\scriptstyle \pi_A} & & \Big\downarrow{\scriptstyle \pi_{A'}} \\ A & \xrightarrow{\phi} & A' \end{array}$$

satisfies
$\phi^{-1} \circ \pi_{A'} \circ \phi = \pi_A \circ g^{-1}$
for $g = \xi(Fr_K) \in \mathrm{Aut}_k(A)$
and $\langle Fr_K \rangle \simeq G_K$.

Example. If A/K is maximal and A'/K minimal, then $g = [-1]$.

Fully maximal, fully minimal, mixed

New question

When do A/K and/or its K-twists have parity $+1$?

To answer this question, we classify supersingular A/K using the following *types*:

Fully maximal, fully minimal, mixed

A/K is *fully maximal* if all its K-twists have parity $+1$.
A/K is *fully minimal* if all its K-twists have parity -1.
A/K is *mixed* if both parities occur.

The type of A/K depends on its normalised Weil numbers and its automorphism group.

From Weil numbers to types

Let $K = \mathbb{F}_q = \mathbb{F}_{p^r}$ and let A/K have NWN $\{z_1, \overline{z}_1, \ldots, z_g, \overline{z}_g\}$.
The type of A/K depends on $\underline{e}(A/K) = \{e_i = \mathrm{ord}_2(|z_i|)\}_{1 \leq i \leq g}$.
(A/K has parity 1 if and only if $e_i = e \geq 2$ (r odd) or $e_i = e \geq 1$ (r even) $\forall i$.)

Let A'/K be a twist with NWN $\{w_1, \overline{w}_1, \ldots, w_g, \overline{w}_g\}$.
Let $K_T = \mathbb{F}_{q^T}$ be the smallest extension such that $A \simeq_{K_T} A'$.
Then $w_i = \lambda_i z_i$, where λ_i is a (non-primitive) T-th root of unity.

Proposition

- If $\mathrm{ord}_2(T) < \min\{e_i\}_{1 \leq i \leq g}$, then $\underline{e}(A'/K) = \underline{e}(A/K)$.
- If A/K has parity 1 and A'/K has parity -1, then T is even.

From types to Weil numbers

Recall $K = \mathbb{F}_q = \mathbb{F}_{p^r}$ and $e_i = \mathrm{ord}_2(|z_i|)$.

Proposition

- If A is fully maximal, then $e_i = e \geq 2$ for all i.
- If A is fully minimal, then the e_i are not all equal.
- If $e_i = e \in \{0, 1\}$ for all i and r is even, then A is mixed.

The converses hold if $|\mathrm{Aut}_k(A)| = 2$. Hence:

Proposition

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

The typical structure of $\mathrm{Aut}_k(A)$ is unknown. We do have:

Proposition

If A is simple and r is even, then A is not fully minimal.

Open questions

1. What is the expected distribution of the $\{z_i\}_{1\leq i\leq g}$ on the complex unit circle, for fixed $K = \mathbb{F}_{p^r}$ and g?
2. Is it true that typically $\mathrm{Aut}_k(A) \simeq \mathbb{Z}/2\mathbb{Z}$?
(We prove this for $g = 2$.)
3. Which type occurs most often, for fixed $K = \mathbb{F}_{p^r}$ and g?
Does this vary among components of the moduli space $\mathcal{A}_{g,ss}$?
4. What are the distributions of the types as $r \to \infty$ (and g fixed) or $g \to \infty$ (and r fixed)?

Supersingular elliptic curves

Let $K = \mathbb{F}_q = \mathbb{F}_{p^r}$ and let E/K be a supersingular elliptic curve. Then $P(E/K, T) = T^2 - \beta T + q$ for some $\beta \in \mathbb{Z}$ such that $p|\beta$. A supersingular E/K is in one of the following cases.

Case n_E	Conditions on r and p	β	$\mathrm{NWN}/\mathbb{F}_q$	Parity
1a	r even	$2\sqrt{q}$	$\{1, 1\}$	-1
1b	r even	$-2\sqrt{q}$	$\{-1, -1\}$	1
2a	r even, $p \not\equiv 1 \bmod 3$	$\sqrt{q}$	$\{-\zeta_3, -\overline{\zeta}_3\}$	1
2b	r even, $p \not\equiv 1 \bmod 3$	$-\sqrt{q}$	$\{\zeta_3, \overline{\zeta}_3\}$	-1
3	r even, $p \equiv 3 \pmod 4$ or r odd	0	$\{i, -i\}$	1
4a	r odd, $p = 2$	$\sqrt{2q}$	$\{\zeta_8, \overline{\zeta}_8\}$	1
4b	r odd, $p = 2$	$-\sqrt{2q}$	$\{\zeta_8^5, \overline{\zeta}_8^5\}$	1
4c	r odd, $p = 3$	$\sqrt{3q}$	$\{\zeta_{12}, \overline{\zeta}_{12}\}$	1
4d	r odd, $p = 3$	$-\sqrt{3q}$	$\{\zeta_{12}^7, \overline{\zeta}_{12}^7\}$	1

Supersingular elliptic curves

A supersingular elliptic curve in char. p is defined over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$.

Theorem

Let E/K be a supersingular elliptic curve. If E is defined over $\mathbb{F}_p$, then it is fully maximal. Otherwise, it is mixed.

The theorem follows from the following results:

- If $p = 2$, the unique supersingular curve $E : y^2 + y = x^3$ is fully maximal.
- Let $p \geq 3$. If $\mathrm{Aut}_k(E) \not\simeq \mathbb{Z}/2\mathbb{Z}$, then E is geometrically isomorphic to either $E : y^2 = x^3 - x$ or $E : y^2 = x^3 + 1$. Both are fully maximal.
- Suppose that $p \geq 3$ and $\mathrm{Aut}_k(E) \simeq \mathbb{Z}/2\mathbb{Z}$. If E is defined over $\mathbb{F}_p$, then it is fully maximal. Otherwise, it is mixed.

Supersingular abelian surfaces

Let A/K be a supersingular (unpolarised) abelian surface.
Then $P(A/K,T) = T^4 + a_1 T^3 + a_2 T^2 + q a_1 T + q^2 \in \mathbb{Z}[T]$.
A is in one of the following cases.

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

Supersingular abelian surfaces

If we assume that $\mathrm{Aut}_k(A) \simeq \mathbb{Z}/2\mathbb{Z}$, the table implies:

- If r is odd, then A is not mixed.
  There are 6 fully maximal and 4 fully minimal cases.
- If r is even, then A is not fully minimal.
  There are 4 fully maximal and 4 mixed cases.

This assumption is not restrictive:

Proposition

If $p \geq 3$, 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 $r \to \infty$.

Supersingular abelian surfaces

Proposition

If $p \geq 3$, 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 $r \to \infty$.

The proof uses the following results:

- (Achter-Howe): $p^r \ll |\mathcal{A}_{2,ss}| \ll p^{r+2}$
- An $\mathbb{F}_{p^r}$-point A in $\mathcal{A}_{2,ss}$ is either $\mathrm{Jac}(X)$, or $E_1 \times E_2$, or $\mathrm{Res}_{\mathbb{F}_{p^{2r}}/\mathbb{F}_{p^r}}(E)$.
- (Achter-Howe): There are $\ll p^2$ of the latter two.
- So it suffices to bound the first case; $\mathrm{Aut}_k(\mathrm{Jac}(X)) \simeq \mathrm{Aut}_k(X)$ by Torelli.
- (Cardona, Cardona-Nart, Igusa, Ibukiyama-Katsura-Oort, Katsura-Oort, Koblitz): There are $\ll p^3$ supersingular curves X with $\mathrm{Aut}_k(X) \not\simeq \mathbb{Z}/2\mathbb{Z}$.

Supersingular curves of genus 3 in characteristic 2

Supersingular curves of genus 3 in char. 2 are parametrised by

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

Let $K = \mathbb{F}_q = \mathbb{F}_{2^r}$ be the smallest field containing a, b.
Let $h \in \mathbb{F}_{q^2}$ be such that $h^2 + h = \frac{a}{b}$ and $K' = \mathbb{F}_q(h)$.

Define $c_1 = ab$, $c_2 = \frac{1}{(h+1)^2}\frac{1}{b}$, $c_3 = \frac{1}{h^2}\frac{1}{b}$. Let

$$\begin{aligned} E_1 &: R^2 + R = c_1 S^3, \\ E_2 &: T^2 + T = c_s(aS)^3, \\ E_3 &: U^2 + U = c_3(aS)^3. \end{aligned}$$

Then $\mathrm{Jac}(X_{a,b}) \sim_{K'} E_1 \oplus E_2 \oplus E_3$.

Supersingular curves of genus 3 in characteristic 2

We have $\mathrm{Jac}(X_{a,b}) \sim_{K'} E_1 \oplus E_2 \oplus E_3$, where E_i depends on c_i.
Recall that $K = \mathbb{F}_{2^r}$ and $K' = K(h) = \mathbb{F}_{2^s}$ for $s \in \{r, 2r\}$.

Lemma

If c_i is a cube in K', then the NWN of E_i/K' are $\{i^s, (-i)^s\}$.
If c_i is not a cube in K', then the NWN of E_i/K' are $\{\zeta_6^{s/2}, \zeta_6^{-s/2}\}$.

This determines the valuations of the NWN of $X_{a,b}$ over K.

Lemma

If $a \neq b$, then $\mathrm{Aut}_k(X_{a,b}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
If $a = b$, then $\mathrm{Aut}_k(X_{a,b}) \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/9\mathbb{Z}$.

Supersingular curves of genus 3 in characteristic 2

Knowing $\mathrm{Aut}_k(X_{a,b})$ allows us to compute the number of twists of $X_{a,b}$ and (the valuations of) their normalised Weil numbers. Comparing these to the normalised Weil numbers of $X_{a,b}$ we obtain the main result:

Theorem

If r is odd, $X_{a,b}$ is fully maximal if $h \in \mathbb{F}_q$ and mixed if $h \notin \mathbb{F}_q$.
If $r \equiv 2 \bmod 4$, $X_{a,b}$ is fully minimal if $h \notin \mathbb{F}_q$ and mixed if $h \in \mathbb{F}_q$.
If $r \equiv 0 \bmod 4$, then $X_{a,b}$ is fully minimal.

Thank you for your attention!