Fully maximal and minimal supersingular abelian varieties

Valentijn Karemaker (University of Pennsylvania)

Joint with R. Pries

Journées Arithmétiques, Caen

July 4, 2017

Motivation

Let $X/\mathbb{F}_q$ be a smooth projective connected curve of genus g. For many applications, we want to find $X(\mathbb{F}_q)$, or $|X(\mathbb{F}_q)|$. The zeta function of $X/\mathbb{F}_q$ is

$$Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{m\geq 1} |X(\mathbb{F}_{q^m})|\frac{T^m}{m}\right) = \frac{L(X/\mathbb{F}_q, T)}{(1-T)(1-qT)};$$

the roots $\alpha_1, \overline{\alpha}_1, \ldots, \alpha_g, \overline{\alpha}_g$ of $P(X/\mathbb{F}_q, T) = T^{2g}L(X/\mathbb{F}_q, T^{-1})$ are the *Weil numbers* of X. These all have absolute value $\sqrt{q}$.

The Weil conjectures imply the Hasse-Weil bound:

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

In particular, $|X(\mathbb{F}_q)|$ is

$$\begin{cases} \text{maximal iff } P(X/\mathbb{F}_q, T) = (T+\sqrt{q})^{2g} \text{ iff } \alpha_i/\sqrt{q} = -1 \ \forall i, \\ \text{minimal iff } P(X/\mathbb{F}_q, T) = (T-\sqrt{q})^{2g} \text{ iff } \alpha_i/\sqrt{q} = 1 \ \forall i. \end{cases}$$

Maximal and minimal abelian varieties

Let $A/\mathbb{F}_q$ be a g-dimensional abelian variety.
(We will always assume A to be principally polarised.)

$$Z(A/\mathbb{F}_q, T) = \exp\left(\sum_{m\geq 1} |A(\mathbb{F}_{q^m})| \frac{T^m}{m}\right)$$

is determined by $P(A/\mathbb{F}_q, T)$, the characteristic polynomial of the relative Frobenius endomorphism π_A of A.
Its roots $\{\alpha_1, \overline{\alpha}_1, \ldots, \alpha_g, \overline{\alpha}_g\}$ are the *Weil numbers* of $A/\mathbb{F}_q$.
Let $\{z_i = \frac{\alpha_i}{\sqrt{q}}, \overline{z}_i\}_{1\leq i\leq g}$ be the *normalised Weil numbers* of $A/\mathbb{F}_q$.

Definition (maximal/minimal)

$$A/\mathbb{F}_q \text{ is } \begin{cases} \text{maximal if all its NWN are } -1; \\ \text{minimal if all its NWN are } 1. \end{cases}$$

Supersingular abelian varieties

$A/\mathbb{F}_q$ is *maximal* (*minimal*) if all its NWN are -1 (1).

Definition (supersingular)

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

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 $A/\mathbb{F}_q$ 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

Let $K = \mathbb{F}_q$ and $k = \overline{\mathbb{F}}_q$.
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:

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "\pi_A"'] & A' \arrow[d, "\pi_{A'}"] \\ A \arrow[r, "\phi"] & A' \end{tikzcd}$$

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 $A/\mathbb{F}_q$ and/or its $\mathbb{F}_q$-twists have parity $+1$?

To answer this question, we classify supersingular $A/\mathbb{F}_q$ using the following *types*:

Definition (fully maximal, fully minimal, mixed)

$A/\mathbb{F}_q$ is *fully maximal* if all its $\mathbb{F}_q$-twists have parity $+1$.
$A/\mathbb{F}_q$ is *fully minimal* if all its $\mathbb{F}_q$-twists have parity -1.
$A/\mathbb{F}_q$ is *mixed* if both parities occur.

The type of $A/\mathbb{F}_q$ depends on:

- the 2-divisibility of the orders of the normalised Weil numbers;
- the Frobenius conjugacy classes in $\mathrm{Aut}_{\overline{\mathbb{F}}_q}(A)$.

Supersingular elliptic curves

Let $\mathbb{F}_q = \mathbb{F}_{p^r}$ and let $E/\mathbb{F}_q$ be a supersingular elliptic curve.
Then $P(E/\mathbb{F}_q, T) = T^2 - \beta T + q$ for some $\beta \in \mathbb{Z}$ such that $p|\beta$.
A supersingular $E/\mathbb{F}_q$ 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 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 $\mathrm{Aut}_{\overline{\mathbb{F}}_p}(E) \not\simeq \mathbb{Z}/2\mathbb{Z}$, 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 $\mathrm{Aut}_{\overline{\mathbb{F}}_p}(E) \simeq \mathbb{Z}/2\mathbb{Z}$. If E is defined over $\mathbb{F}_p$, then it is fully maximal. Otherwise, it is mixed.

Supersingular abelian surfaces

Let $A/\mathbb{F}_q$ be a supersingular (unpolarised) abelian surface.
Then $P(A/\mathbb{F}_q, T) = T^4 + a_1T^3 + a_2T^2 + qa_1T + q^2 \in \mathbb{Z}[T]$.
Let $\mathbb{F}_q = \mathbb{F}_{p^r}$. Then A is in one of the following cases.

	(a_1, a_2)	Conditions on r and p	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 $\mathrm{Aut}_{\overline{\mathbb{F}}_p}(A) \simeq \mathbb{Z}/2\mathbb{Z}$, 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 $\mathrm{Aut}_{\overline{\mathbb{F}}_p}(A) \not\simeq \mathbb{Z}/2\mathbb{Z}$ tends to zero as $r \to \infty$.

Thank you for your attention!