Jacobians in isogeny classes of supersingular abelian surfaces over finite fields

Everett W. Howe[1] Enric Nart[2] Christophe Ritzenthaler[3]

[1]Center for Communications Research, La Jolla

[2]Universitat Autònoma de Barcelona

[3]Institut de Mathématiques de Luminy

AMS sectional meeting, San Francisco
30 April 2006
Corrected slides

Weil polynomials of elliptic curves

Elliptic curves over finite fields.

$$\left\{ \begin{array}{c} \text{Isogeny classes of} \\ \text{elliptic curves over } \mathbb{F}_q \end{array} \right\} \hookrightarrow \{x^2 - tx + q\}$$

The image is known (Deuring, Honda-Tate, Waterhouse).

Suppose q is a power of a prime p.

The possible values of t:

- Every t with $(t, q) = 1$ and $t^2 < 4q$.
- If q is not a square: $\mathbb{Z} \cap \{0, \pm\sqrt{2q}, \pm\sqrt{3q}\}$.
- If q is a square: $\pm 2\sqrt{q}$,

$$\pm\sqrt{q} \quad (\text{if } p \not\equiv 1 \bmod 3),$$
$$0 \quad (\text{if } p \not\equiv 1 \bmod 4).$$

Weil polynomials of genus-2 curves

Genus-2 curves over finite fields.

$$\left\{\begin{array}{c}\text{Isogeny classes of}\\ \text{abelian surfaces over } \mathbb{F}_q\end{array}\right\} \leftrightarrow \quad \text{Known subset of } \{x^4+ax^3+bx^2+aqx+q^2\}$$

$$\bigcup \qquad\qquad\qquad\qquad \bigcup$$

$$\left\{\begin{array}{c}\text{Isogeny classes that}\\ \text{contain Jacobians}\end{array}\right\} \leftrightarrow \quad ???$$

Honda-Tate tells us what the upper right set is.

Rück (1990) asked for the image of the lower left in the upper right. Sixteen years later, the answer is known.

Contributions by Adleman, EWH, Huang, Lauter, Maisner, McGuire, Nart, Ritzenthaler, Rück, Serre, Voloch, . . .

The contents of this talk

As elliptic curve examples suggest, special cases arise in analysis of supersingular isogeny classes. We'll look at one.

I'll sketch a proof of the 'only if' part of the following theorem.

Theorem

Suppose E_1 and E_2 are supersingular elliptic curves over a finite field of characteristic greater than 3. Then there is a Jacobian isogenous to $E_1 \times E_2$ if and only if

$$\operatorname{trace} E_1 = \pm \operatorname{trace} E_2.$$

The assumption on the characteristic is necessary.
In characteristic 3, *neither* implication is true.

The proof relies on the structure of the p-torsion subgroup-schemes of supersingular elliptic curves.

Different isogeny classes have different p-torsion

Proposition

If E_1 and E_2 are non-isogenous supersingular elliptic curves over $\mathbb{F}_q$ (in characteristic > 3), then $E_1[p] \ncong E_2[p]$.

In fact, we will see that isogenous curves may have non-isomorphic p-torsion groups.

We'll see later how this proposition will help us prove the theorem about Jacobians isogenous to $E_1 \times E_2$.

The isogeny classes we must consider

Suppose E_1 and E_2 are supersingular elliptic curves over $\mathbb{F}_q$ with trace $E_1 \neq \pm$ trace E_2.

In characteristic $p > 3$, this implies $q =$ (square).

Possible supersingular traces over $\mathbb{F}_q$ in this case.

trace	condition on p	size of isogeny class
$-2\sqrt{q}$		$\lfloor (p+4)/6 \rfloor - \lfloor p/12 \rfloor$
$-\sqrt{q}$	$p \not\equiv 1 \bmod 3$	2
0	$p \not\equiv 1 \bmod 4$	2
$\sqrt{q}$	$p \not\equiv 1 \bmod 3$	2
$2\sqrt{q}$		$\lfloor (p+4)/6 \rfloor - \lfloor p/12 \rfloor$

Twists of p-divisible groups

Let T_pE denote the p-divisible group of E.

Waterhouse: All E with trace $2\sqrt{q}$ have same T_pE. Let M be this p-divisible group, and M_0 its p-torsion.

Every supersingular EC over $\mathbb{F}_q$ has a twist with trace $2\sqrt{q}$.

We will show that if $\operatorname{trace} E = 2\sqrt{q}$ then

$$\begin{array}{ccccc} H^1(G_{\mathbb{F}_q}, \operatorname{Aut} E) & \hookrightarrow & H^1(G_{\mathbb{F}_q}, \operatorname{Aut} M) & \hookrightarrow & H^1(G_{\mathbb{F}_q}, \operatorname{Aut} M_0) \\ \| & & \| & & \\ (\mu_2, \mu_4, \text{ or } \mu_6) & \hookrightarrow & \mathbb{F}_{p^2}^* & & \end{array}$$

where $G_{\mathbb{F}_q} = \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

Enumerating the twists

Suppose E has trace $2\sqrt{q}$. Tate showed that

$$\operatorname{End} T_p E = (\operatorname{End} E) \otimes \mathbb{Z}_p = \text{maximal order } \mathcal{O} \text{ in } \mathbb{H}_p.$$

Then $\mathcal{O}$ contains the ring R of Witt vectors over $\mathbb{F}_{p^2}$, and

$$\begin{aligned} \text{twists of } T_p E &\leftrightarrow H^1(G_{\mathbb{F}_q}, \operatorname{Aut} T_p E) \\ &\leftrightarrow \text{conj. classes of elts. of } \mathcal{O} \text{ of finite order} \\ &\leftrightarrow \text{roots of unity in } R \subset \mathcal{O} \\ &\leftrightarrow \text{elements of } \mathbb{F}_{p^2}^*. \end{aligned}$$

Not hard to write down the Dieudonné modules of these twists, and see they are all distinct mod p. So

$$H^1(G_{\mathbb{F}_q}, \operatorname{Aut} E) \hookrightarrow H^1(G_{\mathbb{F}_q}, \operatorname{Aut} M) \hookrightarrow H^1(G_{\mathbb{F}_q}, \operatorname{Aut} M_0).$$

Split Jacobians and torsion subgroups

Lemma

Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$.
Suppose $C/\mathbb{F}_q$ satisfies $\operatorname{Jac} C \sim E_1 \times E_2$.
Then there are elliptic curves $F_1 \sim E_1$ and $F_2 \sim E_2$ and an integer $n > 1$ such that $F_1[n] \cong F_2[n]$. □

Note that then

$$\operatorname{trace} E_1 \equiv \operatorname{trace} E_2 \bmod n.$$

(In our paper we use a much stronger version, due to Kani.)

Proof of ‘only if’ part of main theorem

Suppose that $\operatorname{trace} E_1 \neq \pm \operatorname{trace} E_2$ and that there is a C with $\operatorname{Jac} C \sim E_1 \times E_2$.

The lemma says that we have $F_1[n] \cong F_2[n]$ for some divisor $n > 1$ of $\operatorname{trace} E_1 - \operatorname{trace} E_2$ and some $F_1 \sim E_1$, $F_2 \sim E_2$.

The proposition shows that n cannot be divisible by p.

The gives a contradiction when $|\operatorname{trace} E_1 - \operatorname{trace} E_2| = \sqrt{q}$.

In the remaining cases, one of the E’s (say E_1) has trace $\pm 2\sqrt{q}$ and the other does not, and the n from the lemma is 2 or 3.

But Frobenius acts as an integer on $F_1[2]$ and $F_1[3]$ for every $F_1 \sim E_1$, while it does not do so for any $F_2 \sim E_2$. □

Where's the computation?

Nart, Ritzenthaler, and I used computer calculations of Weil polynomials of supersingular curves to help determine what we should be proving.

Most surprising result, that took the most work to prove:

Theorem

Let q be even power of a prime $p \not\equiv 1 \bmod 12$, so that $x^4 - qx^2 + q^2$ is the Weil polynomial of an abelian surface. Then there is a curve with this Weil polynomial if and only if $p \not\equiv 11 \bmod 12$ and $p \neq 3$.

Notes added after the talk

René Schoof asked why we computed the twists of M, when we only needed the twists of M_0.

One reason is that the automorphism group of M is ‘nicer’ than that of M_0, so that the calculation of the H^1 seems a little cleaner.

But it also just seemed like a natural thing to do.

I didn’t mention it in the talk, but in fact $H^1(G_{\mathbb{F}_q}, \operatorname{Aut} M_0)$ is also isomorphic to $\mathbb{F}_{p^2}^*$.