Estimating the number of genus-2 curves over a finite field with split Jacobians (corrected slides)

Jeffrey D. Achter[1] Everett W. Howe[2]

[1]Colorado State University

[2]Center for Communications Research, La Jolla

SIAM Conference on Applied Algebraic Geometry
Fort Collins, 1–4 August 2013

Questions with nice answers

Curves

How many genus-2 curves are there over $\mathbb{F}_q$?

$$\sum_{\text{genus-2 } C/\mathbb{F}_q} \frac{1}{\#\operatorname{Aut} C} = q^3.$$

(Brock/Granville, *Finite Fields Appl.*, 2001)

Principally-polarized abelian surfaces

How many principally-polarized abelian surfaces (A, λ) are there over $\mathbb{F}_q$?

$$\sum_{(A,\lambda)/\mathbb{F}_q} \frac{1}{\#\operatorname{Aut}(A, \lambda)} = q^3 + q^2.$$

Why such nice answers?

Curves and principally-polarized surfaces are parametrized by nice moduli splaces.

What about objects *without* nice moduli spaces?
For example. . .

Curves with nonsimple Jacobians

How many genus-2 curves C are there over $\mathbb{F}_q$ such that Jac C is nonsimple?

Likewise, we could ask about principally-polarized surfaces where the surface is not simple.

Main result

Theorem

There exist positive constants c and d such that for all q,

$$\#\{\textit{genus-2 curves } C/\mathbb{F}_q \textit{ with } \operatorname{Jac} C \textit{ nonsimple}\}$$

is at least $\dfrac{c\,q^{5/2}}{(\log q)^5}$ *and at most* $d\,q^{5/2}(\log q)^{10}(\log\log q)^2$.

Informal interpretation

A randomly chosen genus-2 curve $C/\mathbb{F}_q$ has roughly one chance in $\sqrt{q}$ of having nonsimple Jacobian.

Does this make sense?

Let's compare to the probability that an isogeny class is split.

Isogeny classes

The number of isogeny classes of abelian surfaces over $\mathbb{F}_q$, with $q = p^e$, is

$$\sim \frac{32}{3} \frac{(p-1)}{p} q^{3/2}.$$

(DiPippo/Howe, *J. Number Theory*, 1998)

Split isogeny classes

The number of split isogeny class of abelian surfaces over $\mathbb{F}_q$, with $q = p^e$, is

$$\sim 8 \frac{(p-1)^2}{p^2} q.$$

Types of split surfaces

Split surfaces can be isogenous to…

1. $E_1 \times E_2$, with E_1 and E_2 ordinary and nonisogenous
2. E^2, with E ordinary
3. $E_1 \times E_2$, with E_1, E_2 nonisogenous, but at least one supersingular
4. E^2, with E supersingular

How many of each type?

1. We will see…
2. $O(q^2(\log q)^{\cdots})$
3. $O(q^2(\log q)^{\cdots})$, probably less
4. $O(q^2)$ … and there are this many when $q = p^2$

So the ordinary nonisogenous case is the critical one.

How curves with nonsimple Jacobians arise

Given:

- Two elliptic curves E_1, E_2 over a field k
- An isomorphism $\psi\colon E_1[n] \to E_2[n]$ for some $n > 0$, such that ψ is an anti-isometry with respect to the Weil pairing

We will produce:

A genus-2 curve C (possibly degenerate) with $\operatorname{Jac} C \sim E_1 \times E_2$.

How curves with nonsimple Jacobians arise

Given:

- Two elliptic curves E_1, E_2 over a field k
- An isomorphism $\psi\colon E_1[n] \to E_2[n]$ for some $n > 0$, such that ψ is an anti-isometry with respect to the Weil pairing

$$E_1[n] \times E_1[n] \xrightarrow{\text{Weil}} \boldsymbol{\mu}_n$$

We will produce:

A genus-2 curve C (possibly degenerate) with $\operatorname{Jac} C \sim E_1 \times E_2$.

How curves with nonsimple Jacobians arise

Given:

- Two elliptic curves E_1, E_2 over a field k
- An isomorphism $\psi\colon E_1[n] \to E_2[n]$ for some $n > 0$, such that ψ is an anti-isometry with respect to the Weil pairing

$$E_1[n] \times E_1[n] \xrightarrow{\text{Weil}} \boldsymbol{\mu}_n$$

$$E_2[n] \times E_2[n] \xrightarrow{\text{Weil}} \boldsymbol{\mu}_n$$

We will produce:

A genus-2 curve C (possibly degenerate) with $\operatorname{Jac} C \sim E_1 \times E_2$.

How curves with nonsimple Jacobians arise

Given:

- Two elliptic curves E_1, E_2 over a field k
- An isomorphism $\psi\colon E_1[n] \to E_2[n]$ for some $n > 0$, such that ψ is an anti-isometry with respect to the Weil pairing

$$\begin{array}{ccc} E_1[n] \times E_1[n] & \xrightarrow{\text{Weil}} & \boldsymbol{\mu}_n \\ \downarrow{\scriptstyle \psi\times\psi} & & \\ E_2[n] \times E_2[n] & \xrightarrow{\text{Weil}} & \boldsymbol{\mu}_n \end{array}$$

We will produce:

A genus-2 curve C (possibly degenerate) with Jac $C \sim E_1 \times E_2$.

How curves with nonsimple Jacobians arise

Given:

- Two elliptic curves E_1, E_2 over a field k
- An isomorphism $\psi\colon E_1[n] \to E_2[n]$ for some $n > 0$, such that ψ is an anti-isometry with respect to the Weil pairing

$$\begin{array}{ccc} E_1[n] \times E_1[n] & \xrightarrow{\text{Weil}} & \boldsymbol{\mu}_n \\ {\scriptstyle \psi\times\psi}\downarrow & & \downarrow{\scriptstyle \text{inv.}} \\ E_2[n] \times E_2[n] & \xrightarrow{\text{Weil}} & \boldsymbol{\mu}_n \end{array}$$

We will produce:

A genus-2 curve C (possibly degenerate) with Jac $C \sim E_1 \times E_2$.

Completing a diagram

We have:

- $\text{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\text{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map

Completing a diagram

We have:

- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map

$$E_1 \times E_2 \xrightarrow{\text{mult. by } n} \widehat{E_1} \times \widehat{E_2}$$

Completing a diagram

We have:

- $\text{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\text{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map

$$\begin{array}{ccc} E_1 \times E_2 & \xrightarrow{\text{mult. by } n} & \widehat{E_1} \times \widehat{E_2} \\ {\scriptstyle\alpha}\big\downarrow & & \\ A & & \end{array}$$

Completing a diagram

We have:

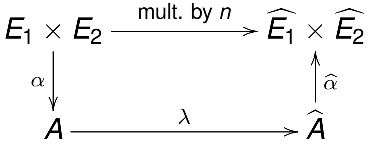
- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map

$$\begin{array}{ccc} E_1 \times E_2 & \xrightarrow{\text{mult. by } n} & \widehat{E_1} \times \widehat{E_2} \\ \downarrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \widehat{\alpha}} \\ A & & \widehat{A} \end{array}$$

Completing a diagram

We have:

- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map



Completing a diagram

We have:

- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map

$$\begin{array}{ccc}
E_1 \times E_2 & \xrightarrow{\text{mult. by } n} & \widehat{E_1} \times \widehat{E_2} \\
\downarrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \widehat{\alpha}} \\
\mathrm{Jac}\, C & \xrightarrow{\lambda} & \widehat{\mathrm{Jac}\, C}
\end{array}$$

An old story

Theorem

- *Every genus-2 curve C with non-simple Jacobian arises in this manner, perhaps in several ways.*
- *If* Jac C *is nonsimple but is not isogenous to E^2, then the E_1, E_2, n, and ψ giving C are unique up to*

$$(E_1, E_2, n, \psi) \mapsto (E_2, E_1, n, \psi^{-1}).$$

This is close to work of Kani, *J. Reine Angew. Math.* (1997).

But the results go back at least to Kowalevski's dissertation (1874, published in *Acta Math.* in 1884), using unpublished result of Weierstrass (her advisor).

Also, independently, to Picard, *Bull. Math. Soc. France* (1883).

Rephrasing the question

Don't count curves. . .

Instead, count quadruples (E_1, E_2, n, ψ), where

- E_1 and E_2 are nonisogenous elliptic curves over $\mathbb{F}_q$
- $n > 1$ is an integer
- $\psi\colon E_1[n] \to E_2[n]$ is an anti-isometry

Note that the existence of an isomorphism $E_1[n] \to E_2[n]$ implies that

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

Thus, for a given E_1 and E_2, only certain n are possible.

How not to prove the theorem

A reasonable strategy?

- We claim there are $\sim q^{5/2}$ curves with nonsimple Jacobian.
- There are $\sim q^2$ pairs (E_1, E_2).
- Should we try to show that each (E_1, E_2) gives about $q^{1/2}$ curves?

This won't work: Consider

$$\limsup_{q\to\infty} \max_{E_1,E_2/\mathbb{F}_q} \frac{\log \#\{\text{Jac } C \text{ coming from } E_1, E_2\}}{\log q}.$$

Can prove this is equal to $3/4$.

Why some pairs of elliptic curves produce many C

Given E_1 and E_2, let's count anti-isometries $E_1[\ell] \to E_2[\ell]$.

For there to be *any* anti-isometries, the Galois modules $E_1[\ell]$ and $E_2[\ell]$ must be isomorphic.

Say the characteristic polynomials of Frobenius on these modules are both $f = x^2 - tx + q \in \mathbb{F}_\ell[x]$. In that case…

…the number of anti-isometries $E_1[\ell] \to E_2[\ell]$ is:

$$\begin{cases} \ell + 1 & \text{if } f \text{ is irreducible,} \\ \ell - 1 & \text{if } f \text{ has two distinct roots in } \mathbb{F}_\ell, \\ \ell^3 - \ell & \text{if disc } f = 0 \text{ and Frobenius acts as an integer,} \\ 0 \text{ or } 2\ell & \text{if disc } f = 0 \text{ and Frobenius does not act as an integer.} \end{cases}$$

The relative conductor

Suppose the Frobenius π acts as an integer t on $E[\ell]$.
Then $(\pi - t)/\ell$ is an endomorphism of E,
So ℓ divides the index $[\operatorname{End} E : \mathbb{Z}[\pi]]$.

We define the *relative conductor* of $E/\mathbb{F}_q$ to be

$$\operatorname{rcond} E = [\operatorname{End} E : \mathbb{Z}[\pi]].$$

Theorem

The number of anti-isometries $E_1[n] \to E_2[n]$ is at most

$$2^{\nu(n)}\psi(n)(\operatorname{rcond} E_1)(\operatorname{rcond} E_2),$$

where $\nu(n) = \#\{p \mid n\}$ and $\psi(n) = n\prod_{p|n}(1 + 1/p)$.

Strata

Definition

A *stratum* (for a quadratic order R) is the set of all elliptic curves over $\mathbb{F}_q$ having endomorphism ring R.

We can get rid of the annoying $2^{\nu(n)}$ by summing over strata.

Theorem

Let S_1 and S_2 be two nonisogenous strata. The sum of the number of anti-isometries $E_1[n] \to E_2[n]$ for all $E_1 \in S_1$ and $E_2 \in S_2$ is bounded by

$$\#S_1 \, \#S_2 \, \psi(n) \, (\mathrm{rcond}\, S_1)(\mathrm{rcond}\, S_2).$$

Summing over all n dividing the difference of the traces gives:

Theorem

There exists a constant c such that for all nonisogenous strata S_1 and S_2, the number of $\operatorname{Jac} C$ coming from all $E_1 \in S_1$ and $E_2 \in S_2$ is at most

$$c\#S_1\,\#S_2\,(\operatorname{rcond} S_1)(\operatorname{rcond} S_2)q^{1/2}(\log\log q)^2.$$

Summing over strata. . .

The total number of C coming from ordinary nonisogenous elliptic curves is at most:

$$c\,q^{1/2}(\log\log q)^2 \sum_{S_1,S_2} \#S_1\,\#S_2\,(\operatorname{rcond} S_1)(\operatorname{rcond} S_2)$$

$$\le (c/2)q^{1/2}(\log\log q)^2 \Big(\sum_S \#S \cdot \operatorname{rcond} S\Big)^2$$

$$= (c/2)q^{1/2}(\log\log q)^2 \Big(\sum_E \operatorname{rcond} E\Big)^2.$$

Our goal is to give an upper bound of the form

$$d\,q^{5/2}(\log q)^{10}(\log\log q)^2.$$

The sum of the relative conductors

So our main result follows from:

Theorem

There is a constant c such that for all q,

$$\sum_{\text{ordinary } E/\mathbb{F}_q} \operatorname{rcond} E < c\, q\, (\log q)^5.$$

Why is this reasonable?

- rcond E can only be as large as the conductor of $\mathbb{Z}[\pi]$.
- On average, the rings $\mathbb{Z}[\pi]$ have small conductor.
- Even when $\mathbb{Z}[\pi]$ has large conductor, relative few curves in the isogeny class have large relative conductor.

Some data

We can estimate probability that a random genus-2 curve over $\mathbb{F}_q$ has split Jacobian by sampling.

For $q = 101$, probability is $c/\sqrt{q}$, with $c = 0.796 \pm 0.009$.

For $q = 1009$, probability is $c/\sqrt{q}$, with $c = 0.80 \pm 0.05$.

Perhaps suggests true probability is $c/\sqrt{q}$, with no log powers?

Application

Fix a genus-2 C over $\mathbb{Q}$. Consider

$$f(x) = \#\{p < x \text{ such that } C/\mathbb{F}_p \text{ has split Jacobian}\}.$$

If the suggestion on preceding slide is correct,
we expect $f(x)$ to grow like $\sqrt{x}/\log x$.
This agrees well with tests on $C\colon y^2 = x^5 + x + 6$.