Unlikely intersections and curves with isogenous covers

Everett W. Howe

Center for Communications Research, La Jolla

Special Session on Arithmetic Geometry in Finite Characteristic

AMS Fall Western Sectional Meeting
UC Riverside, 9–10 November 2019

email: however@alumni.caltech.edu Web site: ewhowe.com Twitter: @howe

Acknowledgement

This talk concerns ongoing joint work with:

- Jeremy Booher — University of Canterbury (NZ)
- Drew Sutherland — Massachusetts Institute of Technology
- Felipe Voloch — University of Canterbury (NZ)

Doubly isogenous curves

Identifying isomorphic curves

Sutherland and Voloch, Proceedings of AGCT-16

Investigate easy-to-compute invariants of curves over $\mathbb{F}_q$.

- Isomorphic curves have the same number of points. . .
- Isomorphic curves have the same number of points over *every extension field*.
- Stated differently: Isomorphic curves have the same Weil polynomial (characteristic polynomial of Frobenius on the Jacobian).
- (The Weil polynomial specifies the isogeny class of the Jacobian.)
- For small genera, the Weil polynomial won't always distinguish curves.
- Why not? . . .

Curves and isogeny classes

The number of genus-g curves over $\mathbb{F}_q$

- The moduli space of genus-g curves has dimension $3g - 3$.
- A generic curve of genus $g > 2$ over $\mathbb{F}_q$ has no twists.
- So we expect about q^{3g-3} curves of genus g over $\mathbb{F}_q$.

The number of g-dimensional isogeny classes over $\mathbb{F}_q$

- Set $v_g = (2^g/g!) \prod_{j=1}^{g} \left(1 - \frac{1}{2^j}\right)^{j-g-1}$.
- $\#\{g\text{-dim'l isogeny classes over } \mathbb{F}_q\} \sim v_g \frac{\varphi(q)}{q} q^{(g^2+g)/4}$. [DiPippo–H. 1998]
- For $g \leq 8$ there are more curves than isogeny classes.
- For $g \leq 22$ the birthday paradox suggests a collision.

(Note: Mestre showed that for all g, there is a $(g+1)$-dimensional family of pairs of non-isomorphic genus-g curves with the same Weil polynomial.)

Weil polynomials of covers

Sutherland and Voloch: Get addition information from covers.

One of their strategies:

Given $C/\mathbb{F}_q$, pick $Q \in C(\mathbb{F}_q)$, and define an embedding f_Q by

$$\begin{aligned} f_Q \colon C &\longrightarrow \operatorname{Jac} C \\ P &\longrightarrow [P - Q]. \end{aligned}$$

Get a cover $C_Q^{(2)}$ of C by pulling back multiplication-by-2:

$$\begin{array}{ccc} C_Q^{(2)} & \longrightarrow & \operatorname{Jac} C \\ \downarrow & & \downarrow 2 \\ C & \xrightarrow{f_Q} & \operatorname{Jac} C \end{array}$$

Note 1: $C_Q^{(2)}/C$ is Galois $\iff$ all 2-torsion of $\operatorname{Jac} C$ is rational.

Note 2: For $P, Q \in C(\mathbb{F}_q)$, the curves $C_P^{(2)}$ and $C_Q^{(2)}$ are twists of one another.

A question, not a conjecture

Definition

Two curves C and D over $\mathbb{F}_q$ are *doubly isogenous* if

- C and D have the same Weil polynomial, and
- $C_P^{(2)}$ and $D_Q^{(2)}$ have the same Weil polynomial, for some choice of base points $P \in C(\mathbb{F}_q)$ and $Q \in D(\mathbb{F}_q)$.

Question [Sutherland–Voloch, 2017]

Are there curves C and D of genus > 2 over $\mathbb{F}_q$ such that:

- C and D are not Galois conjugates of one another, and
- C and D are doubly isogenous?

A question, not a conjecture

Definition

Two curves C and D over $\mathbb{F}_q$ are *doubly isogenous* if

- C and D have the same Weil polynomial, and
- $C_P^{(2)}$ and $D_Q^{(2)}$ have the same Weil polynomial, for some choice of base points $P \in C(\mathbb{F}_q)$ and $Q \in D(\mathbb{F}_q)$.

Question [Sutherland–Voloch, 2017]

Are there curves C and D of genus > 2 over $\mathbb{F}_q$ such that:

- C and D are not Galois conjugates of one another, and
- C and D are doubly isogenous?

Why restrict the genus to be larger than 2? Let's investigate...

The case of genus 2

Let's look at genus-2 curves with all Weierstrass points rational.

$$C\colon y^2 = f = (x - a_1)(x - a_2)(x - a_3)(x - a_4)(x - a_5).$$

Let ∞ be the point at infinity, and consider $C_\infty^{(2)}$.

Facts about $C_\infty^{(2)}$

- $C_\infty^{(2)}$ has genus 17.
- Its Weil polynomial is the Weil polynomial of C times 15 elliptic factors, one for each curve $y^2 = g$ for each monic cubic or quartic factor g of f.

How unlikely are doubly isogenous genus-2 curves?

Consider genus-2 curves over $\mathbb{F}_q$ with all Weierstrass points rational over $\mathbb{F}_q$.

$\#\{\text{such curves with a marked Weierstrass point}\} \sim q^3/60$.
$\#\{\text{Weil polynomials of such curves}\} \sim q^{3/2}/6$.
$\#\{\text{Weil polynomials of ECs with all 2-torsion rational}\} \sim q^{1/2}$.

Expected number of pairs of doubly isogenous marked curves:

$$\frac{q^6/7200}{(q^{3/2}/6)(1/15!)q^{15/2}} = \frac{15!}{1200q^3}$$

So we expect no examples for large q...

But maybe sporadic examples for q up to about 1000?

Example

Over $\mathbb{F}_{307}$, the two nonisomorphic curves

$$C\colon y^2 = x(x-1)(x-12)(x-76)(x-188)$$
$$D\colon y^2 = x(x-1)(x-14)(x-72)(x-81)$$

have Weil polynomials $t^4 + 8t^3 + 6t^2 + 2456t + 94249$.

The 15 elliptic curves in $\mathrm{Jac}\, C_\infty^{(2)}$ and $\mathrm{Jac}\, D_\infty^{(2)}$ have traces

$$-28, -24, -16, -12, -12, -8, -4, 0, 4, 8, 12, 12, 20, 28, 32.$$

Special families

The trouble with heuristics. . .

We treated the 15 elliptic curves in $\mathrm{Jac}\, C_\infty^{(2)}$ as independent random variables.

Let's force them not to be. Consider

$$C\colon y^2 = f = x(x-1)(x-b)\left(x - \frac{1}{1-b}\right)\left(x - \frac{b-1}{b}\right).$$

- C has an automorphism $(x, y) \mapsto \left(\frac{1}{1-x}, \frac{y}{(1-x)^3}\right)$ of order 3.
- This permutes the cubics and quartics dividing f.
- The 15 elliptic curves fall into four orbits, of sizes 6, 3, 3, and 3.
- Furthermore, the Weil polynomial of C is of one of the forms
$$(t^2 - at + q)^2 \quad \text{or} \quad t^4 - at^2 + q^2.$$

Heuristics for curves with order-3 automorphisms

#{Curves of the type given on the preceding slide} $\sim q/3$.

#{Pairs of such curves} $\sim q^2/18$.

#{Weil polynomials of right type for such C} $\sim q^{1/2}$.

#{Sets of four elliptic Weil polynomials, with one marked} $\sim q^2/6$.

All together, the expected number of doubly-isogenous pairs over $\mathbb{F}_q$ is:

$$\frac{q^2/18}{q^{5/2}/6} = \frac{1}{3q^{1/2}}.$$

Note: For each q expect no examples. Over *all* q, expect an infinite number.

Data

n	#examples
14	2362
15	1804
16	1358
17	1138
18	765
19	695
20	522
21	398
22	330
23	312
24	264
25	242
26	248
27	210
28	210

For each n, we looked at the 1024 primes p closest to 2^n.

The second column gives the total number, over all of these p, of geometrically nonisomorphic pairs of doubly isogenous curves with automorphisms of order 3 and with rational Weierstrass points.

If our $1/\sqrt{q}$ heuristics were correct, consecutive entries in the second column would differ by a factor of about $\sqrt{2}$.

An unlikely intersection

Genus-2 curves with reduced automorphism group S_3

Every genus-2 curve with an automorphism of order 3 also has a (non-hyperelliptic) involution, perhaps over an extension.

Universal S_3 family (up to twists, in characteristic $\neq 2$)

$$y^2 = x^6 + (r - 18)x^4 + (-2r + 81)x^2 + r$$

- We require $r \neq 0$ and $r \neq 27$.
- r and $729/r$ give isomorphic curves, otherwise different r give distinct curves.
- A non-hyperelliptic involution: $(x, y) \mapsto (-x, y)$.
- An order-3 automorphism: $(x, y) \mapsto \left(\frac{x+3}{x+1}, \frac{y}{(x+1)^3}\right)$.

Universal family, continued

$$C\colon y^2 = x^6 + (r-18)x^4 + (-2r+81)x^2 + r$$

j-invariants of the associated elliptic curves

- $\operatorname{Jac} C \cong E \times E'$ (without polarization), for two 3-isogenous curves E and E'.

$$j = -(r-3)^3(r-27)/r$$
$$j' = -(r-243)^3(r-27)/r^3$$

- Elliptic curve with multiplicity six in $\operatorname{Jac} C^{(2)}$:

$$j_6 = -16(r-27)^2/r$$

Universal family, continued

$$C\colon y^2 = x^6 + (r-18)x^4 + (-2r+81)x^2 + r$$

- C has rational Weierstrass points $\iff r = \dfrac{-u^2(u-3)^2(u+3)^2}{(u-1)^2(u+1)^2}$.
- $r \neq 0, 27, \infty \iff u \neq 0, \pm 1, \pm 3, \pm\sqrt{-3}, \infty$

Elliptic curves with multiplicity three in Jac $C^{(2)}$

$$j_{3,a} = \frac{(u^8-4u^6+214u^4-36u^2+81)^3}{u^4(u^2+3)^4(u-3)^2(u-1)^2(u+1)^2(u+3)^2}$$

$$j_{3,b} = \frac{16(u^8-4u^7+20u^6+52u^5-26u^4-156u^3+180u^2+108u+81)^3}{u^2(u^2+3)^4(u-3)^4(u-1)^2(u+1)^4(u+3)^2}$$

$$j_{3,c} = \frac{16(u^8+4u^7+20u^6-52u^5-26u^4+156u^3+180u^2-108u+81)^3}{u^2(u^2+3)^4(u-3)^2(u-1)^4(u+1)^2(u+3)^4}$$

Pairs of curves

Suppose we have two such curves C and D, corresponding to parameters r and s, with

$$r = \frac{-u^2(u-3)^2(u+3)^2}{(u-1)^2(u+1)^2} \qquad s = \frac{-v^2(v-3)^2(v+3)^2}{(v-1)^2(v+1)^2},$$

and with elliptic curve j-invariants $j, j', j_6, j_{3,*}$ and $k, k', k_6, k_{3,*}$.

As we noted, j and j' are 3-isogenous, as are k and k'.

How many more isogeny conditions can we impose?

Imposing isogeny conditions

Counting relations between u and v

- Asking that j and k be n-isogenous gives a relation between u and v.
- Asking that j_6 and k_6 be m-isogenous gives one more relation.
- That should limit us to a finite set of (u, v) pairs.
- And we don't expect any further isogeny relations by accident.

This is what happens when we try various n and m.

Same thing if we ask that other pairs of j's and k's be isogenous.

The preceding slide was not telling the whole truth

That is what happens . . . with one exception

- Asking that j and k be 5-isogenous gives a relation between u and v.
- Asking that j_6 and k_6 be 7-isogenous gives us one more relation.
- That limits us to a finite set of (u, v) pairs.
- Find that $r + s = 27$ and $rs = 1$.

The preceding slide was not telling the whole truth

That is what happens . . . with one exception

- Asking that j and k be 5-isogenous gives a relation between u and v.
- Asking that j_6 and k_6 be 7-isogenous gives us one more relation.
- That limits us to a finite set of (u, v) pairs.
- Find that $r + s = 27$ and $rs = 1$.
- But: $j_{3,a}$ and $k_{3,a}$ are 7-isogenous. A free relation!

The preceding slide was not telling the whole truth

That is what happens . . . with one exception

- Asking that j and k be 5-isogenous gives a relation between u and v.
- Asking that j_6 and k_6 be 7-isogenous gives us one more relation.
- That limits us to a finite set of (u, v) pairs.
- Find that $r + s = 27$ and $rs = 1$.
- But: $j_{3,a}$ and $k_{3,a}$ are 7-isogenous. A free relation!
- And: $j_{3,b}$ and $k_{3,b}$ are 7-isogenous. Another free relation!

The preceding slide was not telling the whole truth

That is what happens . . . with one exception

- Asking that j and k be 5-isogenous gives a relation between u and v.
- Asking that j_6 and k_6 be 7-isogenous gives us one more relation.
- That limits us to a finite set of (u, v) pairs.
- Find that $r + s = 27$ and $rs = 1$.
- But: $j_{3,a}$ and $k_{3,a}$ are 7-isogenous. A free relation!
- And: $j_{3,b}$ and $k_{3,b}$ are 7-isogenous. Another free relation!
- And!: $j_{3,c}$ and $k_{3,c}$ are 7-isogenous. A *third* free relation!

The preceding slide was not telling the whole truth

That is what happens . . . with one exception

- Asking that j and k be 5-isogenous gives a relation between u and v.
- Asking that j_6 and k_6 be 7-isogenous gives us one more relation.
- That limits us to a finite set of (u, v) pairs.
- Find that $r + s = 27$ and $rs = 1$.
- But: $j_{3,a}$ and $k_{3,a}$ are 7-isogenous. A free relation!
- And: $j_{3,b}$ and $k_{3,b}$ are 7-isogenous. Another free relation!
- And!: $j_{3,c}$ and $k_{3,c}$ are 7-isogenous. A *third* free relation!

We found a point in the intersection of five curves in the plane.

An *amazing* coincidence

Theorem [Booher, H., Sutherland, Voloch 2019]

Over $\overline{\mathbb{Q}}$, the curve

$$y^2 = x^6 + \left(\tfrac{-9+5\sqrt{29}}{2}\right)x^4 + (54 - 5\sqrt{29})x^2 + \left(\tfrac{27+5\sqrt{29}}{2}\right)$$

is doubly-isogenous to its Galois conjugate, and these curves are not isomorphic.

An *amazing* coincidence

Theorem [Booher, H., Sutherland, Voloch 2019]

Over $\overline{\mathbb{Q}}$, the curve

$$y^2 = x^6 + \left(\tfrac{-9+5\sqrt{29}}{2}\right)x^4 + (54 - 5\sqrt{29})x^2 + \left(\tfrac{27+5\sqrt{29}}{2}\right)$$

is doubly-isogenous to its Galois conjugate, and these curves are not isomorphic.

Corollary

Over every finite field that contains $\sqrt{-1}$, $\sqrt{29}$, and the roots of $t^3 - t - 2$, the two curves in the theorem reduce to a pair of non-isomorphic doubly-isogenous curves with all Weierstrass points rational and with automorphisms of order 3.

Back to positive characteristic

Data, revisited

n	total	red.	rem.
14	2362	176	2186
15	1804	176	1628
16	1358	176	1182
17	1138	176	962
18	765	164	601
19	695	206	489
20	522	178	344
21	398	146	252
22	330	160	170
23	312	172	140
24	264	174	90
25	242	172	70
26	248	204	44
27	210	168	42
28	210	198	12

Second column: Total number of doubly-isogenous pairs (each with an order-3 automorphism and rational Weierstrass points) for the 1024 primes closest to 2^n.

Third column: Number explained by reduction of the global example. (Expected value is $170\frac{2}{3}$.)

Fourth column: The remainder, presumably examples that happen by chance.

Do these entries go down by factor of $\sqrt{2}$?

Closing observations

Rate of random examples

- Our crude heuristics suggest: Random doubly-isogenous curves over $\mathbb{F}_q$ with rational Weierstrass points and automorphisms of order 3 should occur with probability $\frac{2}{3\sqrt{q}}$.

  (The extra 2 comes from accounting for twists.)

- The data indicates something more like $344/\sqrt{q}$.

- If we model the distribution of elliptic curves in isogeny classes better, will we predict a better constant?

The remarkable curve

The curve C given by

$$y^2 = x^6 + \left(\frac{-9+5\sqrt{29}}{2}\right)x^4 + (54 - 5\sqrt{29})x^2 + \left(\frac{27+5\sqrt{29}}{2}\right)$$

simply popped out of our analysis.

Interesting fact: The discriminant of the right-hand side is 2^{22} times a unit.

Therefore this model has good reduction at all odd primes in $\mathbb{Z}\left[\frac{1+\sqrt{29}}{2}\right]$.

The remarkable curve

The curve C given by

$$y^2 = x^6 + \left(\frac{-9+5\sqrt{29}}{2}\right)x^4 + (54 - 5\sqrt{29})x^2 + \left(\frac{27+5\sqrt{29}}{2}\right)$$

simply popped out of our analysis.

Interesting fact: The discriminant of the right-hand side is 2^{22} times a unit.

Therefore this model has good reduction at all odd primes in $\mathbb{Z}\left[\frac{1+\sqrt{29}}{2}\right]$.

If we twist by -1 we get good reduction everywhere:

$$y^2 + \left(\frac{-1+\sqrt{29}}{2}\right)(x^2 - x)y = -x^6 + 3x^5 - \left(\frac{9+\sqrt{29}}{2}\right)x^4 + (4 + \sqrt{29})x^3 - \left(\frac{9+\sqrt{29}}{2}\right)x^2 + 3x - 1$$

Final questions inspired by the remarkable curve

Is there some satisfying explanation for why this curve exists?

Are there more such unlikely intersections coming from higher-degree isogenies?

(They would have to be defined over number fields large enough not to influence the data we've collected on doubly-isogenous curves.)