Curves of genus two with maps of every degree to a fixed elliptic curve

Everett W. Howe

Unaffiliated mathematician based in San Diego, California (unceded Kumeyaay land)

17th Algorithmic Number Theory Symposium (ANTS XVII)

Rijksuniversiteit Groningen
6–10 July 2026

Email: however@alumni.caltech.edu Web site: ewhowe.com GitHub: everetthowe Bluesky: @ewhowe.com

An interesting example

An interesting example

Two curves over $K := \mathbb{Q}(i, s)$, where $i^2 = -1$ and $s^2 = 5$

$$C: \quad y^2 := x^6 - 3x^4 + (2 + r^{24})x^2 - r^{24} \qquad \text{where } r = (s+1)/2,$$
$$E: \quad w^2 := z^3 + 9sz.$$

Four functions on C

$$P_2 := (36sr^6)/(x^2 - 1) \qquad Q_2 := (-18sr^3)/(x^2 - 1)^2$$
$$P_3 := \frac{-3r(x+1)(x^2 - 6r^3x + r^{12})}{(x-1)(sx + r^6)^2} \qquad Q_3 := \frac{-9r\big((1-2s)x^2 - 2x - r^6\big)}{(x-1)^2(sx + r^6)^3}$$

Four maps from C to E that take $(1, 0) \in C(K)$ to $\infty \in E(K)$

$$\varphi_1: \quad (x, y) \to (\ P_2,\ yQ_2) \qquad \varphi_3: \quad (x, y) \to (\ P_3, iyQ_3)$$
$$\varphi_2: \quad (x, y) \to (-P_2, iyQ_2) \qquad \varphi_4: \quad (x, y) \to (-P_3,\ yQ_3)$$

An interesting example, continued

Linear combinations of the four maps

For integers a, b, c, d, we compute that

$$\deg(a\varphi_1 + b\varphi_2 + c\varphi_3 + d\varphi_4) = 2a^2 + 2b^2 + 3c^2 + 3d^2 + 2ad + 2bc\,.$$

Lemma

The above quaternary quadratic form in a, b, c, d represents all integers $n > 1$.

(This is an easy consequence of work of Dickson on a certain ternary form.)

An interesting example, continued

Linear combinations of the four maps

For integers a, b, c, d, we compute that

$$\deg(a\varphi_1 + b\varphi_2 + c\varphi_3 + d\varphi_4) = 2a^2 + 2b^2 + 3c^2 + 3d^2 + 2ad + 2bc\,.$$

Lemma

The above quaternary quadratic form in a, b, c, d represents all integers $n > 1$.

(This is an easy consequence of work of Dickson on a certain ternary form.)

The interesting consequence

For every integer $n > 1$, there is a map of degree n from C to E!

An interesting example, continued

Linear combinations of the four maps

For integers a, b, c, d, we compute that

$$\deg(a\varphi_1 + b\varphi_2 + c\varphi_3 + d\varphi_4) = 2a^2 + 2b^2 + 3c^2 + 3d^2 + 2ad + 2bc\,.$$

Lemma

The above quaternary quadratic form in a, b, c, d represents all integers $n > 1$.

(This is an easy consequence of work of Dickson on a certain ternary form.)

The interesting consequence

For every integer $n > 1$, there is a map of degree n from C to E!

Our question:

Can we find all such examples in characteristic 0?

Statement of results

Our main result

Theorem 1

Up to isomorphism, there are exactly twenty pairs (C, E) *such that*

1. C *is a curve of genus* 2 *over the complex numbers* $\mathbb{C}$;
2. E *is an elliptic curve over* $\mathbb{C}$; *and*
3. *for every* $n > 1$ *there is a map of degree* n *from* C *to* E.

The paper gives a full description of all examples:

- Models over the field of moduli
- Exact period matrices
- Discriminants of endomorphism rings of E and a related ellipic curve
- Quaternary quadratic form given by the degree function on maps $C \to E$

Humbert surfaces

Definition

A map $\varphi\colon C \to E$ from a genus-2 curve to an elliptic curve is *minimal* if it does not factor through an isogeny $E' \to E$ of degree > 1.

Humbert surface of discriminant n^2

- Subvariety H_{n^2} of $\mathcal{M}_2$, the moduli space of genus-2 curves.
- Geometric points correspond to curves with minimal degree-n maps to some elliptic curve.

Humbert surfaces

Definition

A map $\varphi\colon C \to E$ from a genus-2 curve to an elliptic curve is *minimal* if it does not factor through an isogeny $E' \to E$ of degree > 1.

Humbert surface of discriminant n^2

- Subvariety H_{n^2} of $\mathcal{M}_2$, the moduli space of genus-2 curves.
- Geometric points correspond to curves with minimal degree-n maps to some elliptic curve.

Maps $C \to E$ of prime degree are minimal. Therefore Theorem 1 shows:

Corollary

The intersection of the H_{p^2}, over all primes p, is nonempty.

(This is not new.)

Humbert surfaces are not random!

Geometry

- Each H_{n^2} is a codimension-1 subvariety of $\mathcal{M}_2$.
- $\mathcal{M}_2$ is 3-dimensional.
- The intersection of four random surfaces in $\mathcal{M}_2$ should be empty.
- Can we find four Humbert surfaces H_{n^2} with empty intersection?

Humbert surfaces are not random!

Geometry

- Each H_{n^2} is a codimension-1 subvariety of $\mathcal{M}_2$.
- $\mathcal{M}_2$ is 3-dimensional.
- The intersection of four random surfaces in $\mathcal{M}_2$ should be empty.
- Can we find four Humbert surfaces H_{n^2} with empty intersection?

Theorem 2

Let $N = 18634\,63705\,23309\,79680$

$$= 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23 \cdot 31 \cdot 37 \cdot 47 \cdot 59 \cdot 71 \cdot 131\,.$$

Then for every $k > 0$*, the intersection* $H_4 \cap H_9 \cap H_{16} \cap H_{(kN)^2}$ *is empty.*

Humbert surfaces are not random!

Geometry

- Each H_{n^2} is a codimension-1 subvariety of $\mathcal{M}_2$.
- $\mathcal{M}_2$ is 3-dimensional.
- The intersection of four random surfaces in $\mathcal{M}_2$ should be empty.
- Can we find four Humbert surfaces H_{n^2} with empty intersection?

Theorem 2

Let $N = 18634\,63705\,23309\,79680$

$$= 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23 \cdot 31 \cdot 37 \cdot 47 \cdot 59 \cdot 71 \cdot 131\,.$$

Then for every $k > 0$*, the intersection* $H_4 \cap H_9 \cap H_{16} \cap H_{(kN)^2}$ *is empty.*

Improvement from the current version of the paper

The paper has H_{169} instead of H_{16}, and has a much larger N.

Earlier work on intersections of Humbert surfaces

I had looked in the literature for explicit examples of finite sets of Humbert surfaces with trivial intersection, and asked an expert.

Came up empty-handed. But I learned on Saturday that I missed one!

Earlier work on intersections of Humbert surfaces

I had looked in the literature for explicit examples of finite sets of Humbert surfaces with trivial intersection, and asked an expert.

Came up empty-handed. But I learned on Saturday that I missed one!

Harun Kir's dissertation (2024)

- He looks at general Humbert surfaces, not just H_{n^2}.
- Uses work of Kani that we will discuss later.
- Among other examples: $H_4 \cap H_{12} \cap H_{20} \cap H_{28} \cap H_{60} \cap H_{76} \cap H_{84} \cap H_{276} \cap H_{308}$ is nonempty, but its intersection with H_n for any odd n is empty.

Sketches of proofs

Three-part strategy to obtain all pairs (C, E) as in Theorem 1

Limit examples to a finite set

- Show that C is obtained by gluing E to an elliptic curve F along their 2-torsion.
- Show that E has CM by a quadratic order with explicitly bounded discriminant.
- Show that F is isogenous to E via an isogeny of explicitly bounded degree.

Enumerate possible C and E

- Run through the finite number of possible pairs (E, F); construct possible C.
- Given a possible C and E, compute basis of $\mathrm{Hom}(E, \mathrm{Jac}\, C)$.
- Derive the quadratic form whose values are the degrees of maps $C \to E$.

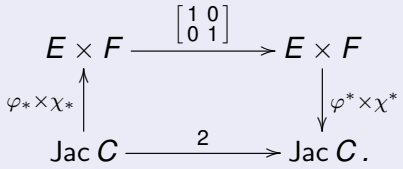
Analyze the quadratic form to see if it represents all $n > 1$

- For each form, check whether its value set contains $\{2, \ldots, 31\}$.
- If not, move to next possibility.
- If so, prove that the form represents all integers $n > 1$.

Step 1: We get C by gluing E to a curve F along 2-torsion

Proposition

Suppose C is a genus-2 curve with a degree-2 map φ to an elliptic curve E. Then there is a unique elliptic curve F and a degree-2 map $\chi\colon C \to F$ such that



Remarks

- The kernel of $\varphi^* \times \chi^*$ is the graph of an isomorphism $E[2] \xrightarrow{\sim} F[2]$.
- Given an E, F, and $E[2] \xrightarrow{\sim} F[2]$, one can construct a C and a degree-2 map $C \to E$ that give rise to them (except in one very special circumstance).
- This construction goes back to a result of Jacobi from 1828.

Interpreting other maps $C \to E$ through this construction

Recall that we have degree-2 maps $\varphi\colon C \to E$ and $\chi\colon C \to F$.

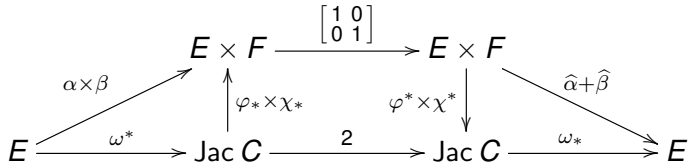
Corollary

Suppose $\omega\colon C \to E$ *is a nonconstant map.*

Define $\alpha\colon E \to E$ *and* $\beta\colon E \to F$ *by* $\alpha := \varphi_*\omega^*$ *and* $\beta := \chi_*\omega^*$.

Then:

- *We have* $\deg\alpha + \deg\beta = 2\deg\omega$.
- *We have* $\#(\ker\alpha)[2] = \#(\ker\beta)[2]$.



Consequences of a degree-3 map $\omega\colon C \to E$

Recall our goal: We want to show that E has CM and that F is isogenous to E.

Apply the corollary to a degree-3 map $\omega\colon C \to E$

We obtain $\alpha\colon E \to E$ and $\beta\colon E \to F$ such that

- $\deg \alpha + \deg \beta = 6$;
- $\#(\ker \alpha)[2] = \#(\ker \beta)[2]$.

Consequences of a degree-3 map $\omega\colon C \to E$

Recall our goal: We want to show that E has CM and that F is isogenous to E.

Apply the corollary to a degree-3 map $\omega\colon C \to E$

We obtain $\alpha\colon E \to E$ and $\beta\colon E \to F$ such that

- $\deg\alpha + \deg\beta = 6$;
- $\#(\ker\alpha)[2] = \#(\ker\beta)[2]$.

$\deg\alpha$	$\deg\beta$	Can kernels match?	Prove $\alpha \notin \mathbb{Z}$?	F isogenous to E?
0	6	no	—	—
1	5	yes	no	yes
2	4	yes	yes	yes
3	3	yes	yes	yes
4	2	yes	yes	yes
5	1	yes	yes	yes
6	0	no	—	—

Consequences of a degree-3 map $\omega\colon C \to E$

Recall our goal: We want to show that E has CM and that F is isogenous to E.

Apply the corollary to a degree-3 map $\omega\colon C \to E$

We obtain $\alpha\colon E \to E$ and $\beta\colon E \to F$ such that

- $\deg\alpha + \deg\beta = 6$;
- $\#(\ker\alpha)[2] = \#(\ker\beta)[2]$.

$\deg\alpha$	$\deg\beta$	Can kernels match?	Prove $\alpha \notin \mathbb{Z}$?	F isogenous to E?
0	6	no	—	—
1	5	yes	no	yes
2	4	yes	yes	yes
3	3	yes	yes	yes
4	2	yes	yes	yes
5	1	yes	yes	yes
6	0	no	—	—

Consequences of a degree-4 map $\omega\colon C \to E$

Apply the corollary to a degree-4 map $\omega\colon C \to E$

- Get $\alpha\colon E \to E$ and $\beta\colon E \to F$ with $\deg\alpha + \deg\beta = 8$ and $\#(\ker\alpha)[2] = \#(\ker\beta)[2]$.
- We may assume that we're in the case where there is a 5-isogeny $\gamma\colon E \to F$.
- Note that $\widehat{\gamma}\beta \in \operatorname{End} E$.

$\deg\alpha$	$\deg\beta$	Can kernels match?	Prove $\alpha \notin \mathbb{Z}$?	Prove $\widehat{\gamma}\beta \notin \mathbb{Z}$?
0	8	yes	no	yes
1	7	yes	no	yes
2	6	yes	yes	yes
3	5	yes	yes	no
4	4	yes	no	yes
5	3	yes	yes	yes
6	2	yes	yes	yes
7	1	yes	yes	yes
8	0	yes	yes	no

Consequences of a degree-4 map $\omega\colon C \to E$

Apply the corollary to a degree-4 map $\omega\colon C \to E$

- Get $\alpha\colon E \to E$ and $\beta\colon E \to F$ with $\deg\alpha + \deg\beta = 8$ and $\#(\ker\alpha)[2] = \#(\ker\beta)[2]$.
- We may assume that we're in the case where there is a 5-isogeny $\gamma\colon E \to F$.
- Note that $\widehat{\gamma}\beta \in \operatorname{End} E$.

$\deg\alpha$	$\deg\beta$	Can kernels match?	Prove $\alpha \notin \mathbb{Z}$?	Prove $\widehat{\gamma}\beta \notin \mathbb{Z}$?
0	8	yes	no	yes
1	7	yes	no	yes
2	6	yes	yes	yes
3	5	yes	yes	no
4	4	yes	no	yes
5	3	yes	yes	yes
6	2	yes	yes	yes
7	1	yes	yes	yes
8	0	yes	yes	no

So in every case, we see that E has CM.

Enumerating possibilities, evaluating possibilities

- We know that E has CM, and we can list the possible discriminants.
- We know that F is isogenous to E, via an isogeny of degree at most 5.
- So we can enumerate the possible pairs (E, F) using exact arithmetic.
- And we can enumerate the possible curves C associated to E and F.

- The Riemann matrices for E and F have entries in a known number field.
- The Riemann matrix for $\mathrm{Jac}\, C$ has entries in the same field.

- Compute the quadratic form on $\mathrm{Hom}(E, \mathrm{Jac}\, C)$ obtained from polarizations.
- Check whether it represents all integers $n > 1$.

Enumerating possibilities, evaluating possibilities

- We know that E has CM, and we can list the possible discriminants.
- We know that F is isogenous to E, via an isogeny of degree at most 5.
- So we can enumerate the possible pairs (E, F) using exact arithmetic.
- And we can enumerate the possible curves C associated to E and F.

- The Riemann matrices for E and F have entries in a known number field.
- The Riemann matrix for $\mathrm{Jac}\, C$ has entries in the same field.

- Compute the quadratic form on $\mathrm{Hom}(E, \mathrm{Jac}\, C)$ obtained from polarizations.
- Check whether it represents all integers $n > 1$.

- This gives us Theorem 1.

The refined Humbert invariant

The invariant and its properties

Given a genus-2 curve C, Kani defines an integer quadratic form q_C.

- q_C is positive definite and has rank at most 3.
- q_C primitively represents $n^2 \iff C$ has a minimal degree-n map to some E.
- The values taken by q_C are all 0 or 1 mod 4.

A integer quadratic form is *primitive* if its coefficients generate the unit ideal.

Which primitive ternary quadratics are refined Humbert invariants?

Kani: A primitive ternary quadratic is equivalent to a q_C for a curve C if and only if

- it is positive definite;
- all of its values are 0 or 1 mod 4;
- it primitively represents n^2 for some $n > 1$ coprime to its discriminant;
- it does not represent 1.

Enumerating ternary quadratic forms

Lemma

Up to isomorphism, there are 59 *integer ternary quadratic forms* q *such that*

- q *is positive definite*;
- q *only represents integers that are* 0 *or* 1 *mod* 4;
- q *primitively represents* 4, 9, *and* 16;
- q *does not represent* 1.

Idea of proof

- Let the successive minima of q be a, b, and c. They are all 0 or 1 mod 4.
- Must have $a = 4$. Since $4x^2$ does not represent 9, must have $b \leq 9$.
- Enumerate positive definite binary forms with these minima.
- None primitively represents 16, so $c \leq 16$.

Proof of Theorem 2

Lemma

Let $q := Ax^2 + By^2 + Cz^2$ be a nondegenerate form over $\mathbb{Z}_p$ for an odd prime p. Suppose that

- *at least one of A, B, and C is a unit,*
- *the parities of the valuations of A, B, and C are not all equal, and*
- *$-A/B$, $-A/C$, and $-B/C$ are all nonsquares in $\mathbb{Q}_p$.*

Then q does not primitively represent any $m \in \mathbb{Z}_p$ whose valuation is greater than those of A, B, and C.

Proof of Theorem 2

Lemma

Let $q := Ax^2 + By^2 + Cz^2$ be a nondegenerate form over $\mathbb{Z}_p$ for an odd prime p. Suppose that

- *at least one of A, B, and C is a unit,*
- *the parities of the valuations of A, B, and C are not all equal, and*
- *$-A/B$, $-A/C$, and $-B/C$ are all nonsquares in $\mathbb{Q}_p$.*

Then q does not primitively represent any $m \in \mathbb{Z}_p$ whose valuation is greater than those of A, B, and C.

Sketch of proof

- Suppose $m = Au^2 + Bv^2 + Cw^2$ for $u, v, w \in \mathbb{Z}_p$ with at least one a unit.
- Not all three summands have the same valuation, by the parity condition.
- If Au^2 and Bv^2 have smallest valuation, then $Au^2 + Bv^2$ has larger valuation.
- Then $(A/B)(u/v)^2 + 1 = 0 \bmod p$, so $-A/B$ is a square in $\mathbb{Q}_p$. Contradiction.

Proof of Theorem 2, continued

Straightforward computation

- For each of the 59 forms q, find a prime power $P = p^e$ such that q does not primitively represent any multiple of P.
- How to find such a P?
- Try to use the lemma; check odd p dividing determinant of Gram matrix of q.
- (Note that we can always diagonalize to apply the lemma, since p is odd.)
- If this fails for one of our 59 forms, check by brute force that $P = 2^{10}$ works.
- Verify that N^2 is a multiple of P.

We chose N so that the last condition is always satisfied, so Theorem 2 holds.

Remaining work

Compute the refined Humbert invariants of the curves in Theorem 1

- Up to Galois conjugacy, there are only 8 curves.
- In conversation with Harun Kir to compute the invariants. Stay tuned.

Compute explicit bases for the lattice of maps $C \to E$

- (Here we fix a base point P on C and only consider maps that take P to ∞.)
- Already done and in GitHub repository for 3 of the 8 Galois conjugacy classes.

Remaining work

Compute the refined Humbert invariants of the curves in Theorem 1

- Up to Galois conjugacy, there are only 8 curves.
- In conversation with Harun Kir to compute the invariants. Stay tuned.

Compute explicit bases for the lattice of maps $C \to E$

- (Here we fix a base point P on C and only consider maps that take P to ∞.)
- Already done and in GitHub repository for 3 of the 8 Galois conjugacy classes.

Thank you!

Questions? Anything else related to the talk that you would like to see calculated?