MATHEMATICS OF COMPUTATION
Volume 93, Number 345, January 2024, Pages 347–381
https://doi.org/10.1090/mcom/3891
Article electronically published on August 31, 2023

DOUBLY ISOGENOUS GENUS-2 CURVES WITH D_4-ACTION

VISHAL ARUL, JEREMY BOOHER, STEVEN R. GROEN, EVERETT W. HOWE, WANLIN LI, VLAD MATEI, RACHEL PRIES, AND CALEB SPRINGER

Abstract. We study the extent to which curves over finite fields are characterized by their zeta functions and the zeta functions of certain of their covers. Suppose C and C' are curves over a finite field K, with K-rational base points P and P', and let D and D' be the pullbacks (via the Abel–Jacobi map) of the multiplication-by-2 maps on their Jacobians. We say that (C, P) and (C', P') are *doubly isogenous* if $\mathrm{Jac}(C)$ and $\mathrm{Jac}(C')$ are isogenous over K and $\mathrm{Jac}(D)$ and $\mathrm{Jac}(D')$ are isogenous over K. For curves of genus 2 whose automorphism groups contain the dihedral group of order eight, we show that the number of pairs of doubly isogenous curves is larger than naïve heuristics predict, and we provide an explanation for this phenomenon.

1. Introduction

The isogeny class of the Jacobian of a (smooth, projective, geometrically connected) curve over a field K is an invariant of the curve, and it is natural to wonder whether this invariant is strong enough to always distinguish two curves from one another. The answer is no — distinct isogenous elliptic curves provide abundant counterexamples. Even when we restrict attention to curves of larger genus, the answer remains no, as over finite fields curves that are Galois conjugates of one another have the same zeta function (which in this case characterizes the isogeny class of the Jacobian). Furthermore, Smith [19] showed that even in characteristic 0 there exist nonisomorphic curves C and C' of arbitrarily large genus with $\mathrm{Jac}(C)$ isogenous to $\mathrm{Jac}(C')$. Later, Mestre [12, 13] proved that such pairs of curves exist for *every* genus in characteristic 0; in particular, for every $g \geq 1$ there is a family of dimension $g + 1$ of pairs of hyperelliptic curves of genus g with a 2-power isogeny between their Jacobians. Thus the isogeny class of the Jacobian is not an invariant that can always distinguish two curves from one another.

The question becomes more interesting when we restrict to low-dimensional families of curves. One motivation is a connection with deterministic algorithms for factoring polynomials over finite fields. Suppose there are an open subset U of $\mathbb{A}^1_{\mathbb{Z}}$

Received by the editor February 25, 2021, and, in revised form, January 27, 2023.
2020 *Mathematics Subject Classification.* Primary 11G20, 11M38, 14H40, 14K02, 14Q05; Secondary 11G10, 11Y40, 14H25, 14H30, 14Q25.
Key words and phrases. Curve, Jacobian, finite field, zeta function, isogeny, unramified cover, arithmetic statistics.
This work was supported by a grant from the Simons Foundation (546235) for the collaboration 'Arithmetic Geometry, Number Theory, and Computation', through a workshop held at ICERM. The second author was partially supported by the Marsden Fund Council administered by the Royal Society of New Zealand. The fifth author was partially funded by the Simons collaboration on 'Arithmetic Geometry, Number Theory, and Computation'. The seventh author was partially supported by NSF grant DMS-19-01819. The eighth author was partially supported by National Science Foundation Awards CNS-2001470 and CNS-1617802.

©2023 by the authors

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

and an abelian scheme $\mathcal{A}$ over U such that for all sufficiently large primes p, the zeta functions of the specialization of $\mathcal{A}$ to the elements of $U(\mathbb{F}_p)$ are distinct. Poonen [17], extending earlier work of Kayal, showed that if such a scheme $\mathcal{A}$ exists, then there is a deterministic algorithm that, given a finite field $\mathbb{F}_q$ and a polynomial $f \in \mathbb{F}_q[t]$, will produce the irreducible factors of f in time polynomial in $\log q$ and $\deg f$.

Motivated by this observation, Sutherland and Voloch [20] considered curves over finite fields, and asked whether curves could be distinguished from one another (up to Galois conjugacy) by their zeta functions together with the zeta functions of certain of their covers. If so, then the Jacobians of these curves and their covers could be used in Poonen's argument. One of the families of covers they studied was obtained by considering maximal unramified abelian 2-extensions of curves, as will now describe.

Let (C, P) be a *pointed* curve over a field K, that is, a curve over K provided with a K-rational point. Let $\widetilde{C} \to C$ be the pullback of the multiplication-by-2 map on $\mathrm{Jac}(C)$ via the embedding $C \to \mathrm{Jac}(C)$ that sends P to the identity. We say that two curves C and C' over K are *isogenous* if their Jacobians are isogenous over K, and we say that two pointed curves (C, P) and (C', P') are *doubly isogenous* if C and C' are isogenous and $\widetilde{C}$ and $\widetilde{C}'$ are isogenous. (Similar definitions can be made using pullbacks of other isogenies of the Jacobian; following Sutherland and Voloch, we focus here on the multiplication-by-2 map because it is perhaps the simplest nontrivial choice.)

As we noted above, if K is a finite field then C and C' are isogenous if and only if they have the same zeta function over K. One can use arithmetic statistics to develop heuristics for the number of pairs of pointed curves (C, P) and (C', P') that are isogenous or doubly isogenous. The hope is to identify families of curves such that no two members are expected to be doubly isogenous, and then prove that expectation and obtain a deterministic factoring algorithm. As a first step, we would like to gather data to test whether our heuristics are reasonable, and to that end we study families for which the heuristics suggest that there *do* exist doubly isogenous pairs.

In as-yet-unpublished work, Howe, Sutherland, and Voloch studied genus-2 curves having an automorphism of order 3; the full automorphism group of these curves contains the dihedral group of order 12. They gave a heuristic for the number of such curves over finite fields of characteristic not 2 or 3 that are doubly isogenous. Their data showed that the number of such pairs was larger than expected. This over-abundance was explained by the existence of a pair of doubly isogenous pointed curves over the number field $\mathbb{Q}(\sqrt{29})$; for every prime $\mathfrak{p}$ of this number field, the reductions of these curves modulo $\mathfrak{p}$ give a pair of doubly isogenous pointed curves having an automorphism of order 3.

We explore another instance of this problem, working over a field K of characteristic not 2 containing a primitive 4th root of unity. We consider curves of genus 2 with an automorphism ρ of order 4. The automorphism groups of these curves contain the dihedral group of order 8. We study their elementary abelian 2-group covers, in some cases restricting to the situation where the Weierstrass points of the genus-2 curves are K-rational. An imprecise summary of our main results is that, taking $K = \mathbb{F}_q$ for a prime $q \equiv 1 \bmod 4$:

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

(1) The number of pairs of such curves over $\mathbb{F}_q$ whose Jacobians are isogenous over $\mathbb{F}_q$ grows as expected; see Theorem 4.6 and Table 2.
(2) The number of pairs of such curves that are "$[1-\rho^*]$-isogenous" over $\mathbb{F}_q$ grows as expected; see Example 5.6 and Table 3(B). (The terminology is explained in Example 5.6, but roughly speaking, the definition of being $[1-\rho^*]$-isogenous is the same as that of being doubly isogenous, except the multiplication-by-2 map on $\mathrm{Jac}(C)$ is replaced by a degree-4 endomorphism of $\mathrm{Jac}(C)$.)
(3) The number of pairs of such curves that are doubly isogenous over $\mathbb{F}_q$ is larger than expected; see Lemma 5.4 and Table 3(A). We explain this discrepancy in Section 6 by finding unexpected relationships between the Prym varieties of certain covers.

We remark that this family of curves is Moonen's fourth special family [16]. It would be interesting to study isogenies between curves in the other special families of Moonen.

Conventions. A *curve* over a field K is a smooth projective geometrically connected 1-dimensional variety over K. If C is a curve over a field K, then $\mathrm{Aut}(C)$ is the group of K-rational automorphisms of C; if L is an extension field of K, then $\mathrm{Aut}_L(C)$ is the group of L-rational automorphisms of C.

2. The family of genus-2 curves with D_4-action

Let K be a field of characteristic not 2. In this section, we find an equation that describes every genus-2 curve over K whose automorphism group contains the dihedral group D_4 of order 8. We also show that the Jacobian of a genus-2 curve with D_4 contained in its automorphism group is isogenous to the square of an elliptic curve.

We fix a presentation of the dihedral group of order 8:

$$D_4 = \langle a, b \,|\, a^2 = b^2 = (ab)^4 = 1 \rangle.$$

We let ξ denote the automorphism of D_4 that interchanges a and b.

Notation 2.1. A *curve with D_4-action* is a curve Z together with an embedding $\epsilon\colon D_4 \hookrightarrow \mathrm{Aut}(Z)$. We say that two curves with D_4-action (Z,ϵ) and (Z',ϵ') are *isomorphic* if there is a K-rational isomorphism $\varphi\colon Z \to Z'$ such that the following diagram commutes:

$$\begin{array}{ccc} & D_4 & \\ {\scriptstyle\epsilon}\swarrow & & \searrow{\scriptstyle\epsilon'} \\ \mathrm{Aut}(Z) & \xrightarrow[\delta\mapsto\varphi\circ\delta\circ\varphi^{-1}]{} & \mathrm{Aut}(Z') \end{array}$$

Let $\mathcal{Z}$ denote the set of K-isomorphism classes of genus-2 curves with D_4-action over K. Using Igusa's classification [8, §8] of the automorphism groups of genus-2 curves, we check that if (Z,ϵ) is a genus-2 curve with D_4-action, then $\epsilon((ab)^2)$ is the hyperelliptic involution.

Remark 2.2. If (Z,ϵ) is a curve with D_4-action and α is an automorphism of Z, we let ϵ^α denote the inclusion $D_4 \hookrightarrow \mathrm{Aut}(Z)$ that sends x to $\alpha\epsilon(x)\alpha^{-1}$. Note that $\alpha\colon Z \to Z$ then gives a morphism of pairs $(Z,\epsilon) \to (Z,\epsilon^\alpha)$, which shows that

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

conjugating ϵ by an automorphism of Z does not change the isomorphism class of the pair (Z, ϵ).

2.1. **A family of genus-2 curves with D_4-action.** Let c and s be elements of K with $c \neq 0$ and $s \neq \pm 2$, and let Z be the genus-2 curve

$$Z\colon \quad y^2 = c(x^2+1)(x^4+sx^2+1). \tag{2.1}$$

The hyperelliptic involution κ of Z is given by $(x, y) \mapsto (x, -y)$. The curve Z also has other K-rational involutions, including

$$\sigma\colon (x,y) \mapsto (-x,y) \qquad \text{and} \qquad \tau\colon (x,y) \mapsto (1/x, y/x^3).$$

Let $\rho = \sigma\tau$, so that ρ takes (x, y) to $(-1/x, y/x^3)$. We note that $\rho^2 = \kappa$. The group G generated by σ and τ is isomorphic to D_4. More precisely, we specify an inclusion

$$\begin{aligned} \epsilon\colon D_4 &\hookrightarrow \mathrm{Aut}(Z), \\ a &\mapsto \sigma, \\ b &\mapsto \tau. \end{aligned} \tag{2.2}$$

Thus, Equations (2.1) and (2.2) give us a family of genus-2 curves with D_4-action.

Remark 2.3. When $s \in \{-6, -1, 14\}$, the curve (2.1) has geometric automorphism group strictly larger than D_4; using Igusa's classification [8, §8], we can show that all other values of s give curves with geometric automorphism group isomorphic to D_4.

2.2. **Classifying genus-2 curves with D_4-action up to isomorphism.**

Lemma 2.4. *Let (Z', ϵ') be a genus-2 curve over K with D_4-action. Then there are values $c, s \in K$ such that the curve with D_4-action (Z, ϵ) given by* (2.1) *and* (2.2) *is isomorphic to (Z', ϵ'). The value of s is unique, and the value of c is unique up to multiplication by elements of $K^{\times 2}$.*

Proof. Let $\alpha = \epsilon'(a)$, let $\beta = \epsilon'(b)$, and let ι be the hyperelliptic involution on Z'. The quotient of Z' by α has genus 1 because $\alpha \neq \iota$. The Riemann–Hurwitz formula shows that α has two geometric fixed points. If P is one of these fixed points, then $\iota P = \iota\alpha P = \alpha\iota P$, so ιP is fixed by α as well.

We claim that $P \neq \iota P$. To see this, consider the V_4-subgroup $H = \langle \alpha, \iota \rangle$. The stabilizer of any point under H is the decomposition group of the corresponding place in the geometric cover $Z' \to Z'/H$. This decomposition group is cyclic since the extension is tamely ramified. Hence, no fixed point of α is fixed by ι.

Consider the quotient $\mathbb{P}^1 = Z'/\langle \iota \rangle$. The two fixed points of α are P and ιP. These two points map to the same point Q in $\mathbb{P}^1$ and Q must be K-rational. Since α and β both commute with ι, they descend to automorphisms $\overline{\alpha}$ and $\overline{\beta}$ of $\mathbb{P}^1$. The point Q is one of the fixed points of the involution $\overline{\alpha}$, so both fixed points of $\overline{\alpha}$ must be K-rational. By choosing the coordinate x on $\mathbb{P}^1$ appropriately, we may assume that the fixed points of $\overline{\alpha}$ are $x = 0$ and $x = \infty$. This means that an equation for Z' is

$$y^2 = a_6x^6 + a_4x^4 + a_2x^2 + a_0,$$

for some constants $a_0, a_2, a_4, a_6 \in K$, and in this model α sends (x, y) to $(-x, y)$.

Since $(\alpha\beta)^2 = \iota$ and ι induces the trivial automorphism on $\mathbb{P}^1$, we see that $\overline{\alpha}\overline{\beta}$ is an involution of $\mathbb{P}^1$, implying that $\overline{\alpha}$ and $\overline{\beta}$ commute. This means that $\overline{\beta}$ must

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

be a linear fractional transformation of the form $x \mapsto d/x$ for some $d \in K^\times$. Since the fixed points of $\overline{\beta}$ are also K-rational, d is a square in $K^\times$. By scaling x by $\sqrt{d}$, we may assume that $d = 1$. This implies that $a_6 = a_0$ and $a_4 = a_2$, so that an equation for Z' is

$$y^2 = a_0x^6 + a_2x^4 + a_2x^2 + a_0,$$

and so that β sends (x, y) to $(1/x, y/x^3)$. Let $c = a_0$ and $s = a_2/a_0$, and let (Z, ϵ) be the genus-2 curve with D_4-action given by (2.1) and (2.2). Our model for Z' gives us an isomorphism $(Z', \epsilon') \to (Z, \epsilon)$.

Demanding that the fixed points of $\overline{\alpha}$ be 0 and ∞ and that the fixed points of $\overline{\beta}$ be 1 and -1 completely specifies the standard hyperelliptic model for Z', up to scaling y by a constant. These scalings modify c by multiplication by a square in $K^\times$. This proves the final statement of the lemma. □

Lemma 2.5. *The two curves*

$$Z\colon y^2 = c(x^2+1)(x^4+sx^2+1) \quad \textit{and} \quad Z'\colon y^2 = c'(x^2+1)(x^4+s'x^2+1)$$

are isomorphic to one another if and only if either $c' = c$ *(in* $K^\times/K^{\times 2}$*) and* $s' = s$*, or* $c' = 2c(s+2)$ *(in* $K^\times/K^{\times 2}$*) and* $(s'+2)(s+2) = 16$.

Note that Lemma 2.5 says that every curve of the form given by Equation (2.1) has exactly one other model of the same form, unless $s = -6$ and -2 is a square, in which case the lemma claims that the given model is unique.

Proof of Lemma 2.5. If either of the given relations among c, c' and s, s' hold, it is easy to check that the two curves are isomorphic to each other. The isomorphism in the second case is given by $(x, y) \mapsto \big((x+1)/(x-1), y/(x-1)^3\big)$.

On the other hand, suppose we have a curve Z as in the lemma. We would like to see how many other models it has that are also of the form given by Equation (2.1). Notation 2.1, Remark 2.2, and Lemma 2.4 show that these models correspond to the embeddings of D_4 into $\mathrm{Aut}(Z)$, up to conjugation by $\mathrm{Aut}(Z)$, so we just need to count the number of such embeddings up to conjugacy.

If $s \notin \{-6, -1, 14\}$ then $\mathrm{Aut}(Z) \cong D_4$ by Remark 2.3. The outer automorphism group of D_4 has two elements, so there are two embeddings of D_4 into $\mathrm{Aut}(Z)$ up to conjugation and hence two models of the form (2.1). These are accounted for by the two models in the lemma.

If $s \in \{-1, 14\}$, then by computing Igusa invariants and consulting [8, §8] we find that $\mathrm{Aut}_{\bar{K}}(Z)$ is a certain group of order 24, so $\mathrm{Aut}(Z)$ is a subgroup of this group that contains D_4. By enumeration, we find that for each such subgroup G there are two conjugacy classes of embedding $D_4 \hookrightarrow G$. Once again, these are accounted for by the two models in the lemma.

When $s = -6$, we find from Igusa that $\mathrm{Aut}_{\bar{K}}(Z)$ is either a certain group G_{48} of order 48 (if K has characteristic not 5) or a certain group G_{240} of order 240 (if K has characteristic 5). Both of these groups contain a unique subgroup G_{16} of order 16. For every subgroup G of G_{48} or G_{240} that contains D_4, we find that the number of conjugacy classes of embeddings $D_4 \hookrightarrow G$ is equal to 2 if G does not contain G_{16}, and is equal to 1 if G does contain G_{16}.

In terms of the model $y^2 = c(x^2+1)(x^4-6x^2+1)$ for Z, the group G_{16} is generated by the involutions σ and τ together with the automorphism υ of order 8 given by $(x, y) \mapsto ((x-1)/(x+1), 2\sqrt{-2}\,y/(x+1)^3)$. We see that G_{16} is contained in $\mathrm{Aut}(Z)$ if and only if -2 is a square in K. Combined with the results of the

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

preceding paragraph, we find two models for Z when -2 is not a square, and one otherwise. □

2.3. **An invariant of the curve Z.** Lemma 2.5 shows that two curves Z and Z' of the form given by Equation (2.1) are geometrically isomorphic to one another if and only if either $s' = s$ or $s' = (-2s + 12)/(s + 2)$. The function

$$I(s) := -\frac{(s-2)^2}{4(s+2)} = 1 - \frac{s+s'}{4} \tag{2.3}$$

is stable under the involution $s \leftrightarrow s'$ and is rational of degree 2, so it gives a geometric invariant for the curve Z.

2.4. **Structure of the Jacobian of the curve Z.** In this section, we consider the quotients of Z by the noncentral involutions of D_4.

Let E be the elliptic curve defined by

$$E: \quad y^2 = c(x+1)(x^2 + sx + 1). \tag{2.4}$$

Lemma 2.6. *The quotient of Z by each of the involutions $(x, y) \mapsto (-x, \pm y)$ is isomorphic to E, and $\mathrm{Jac}(Z)$ is isogenous to E^2.*

Proof. The quotient of Z by the involution $(x, y) \mapsto (-x, y)$ is clearly E.

To find the quotient by $(x, y) \mapsto (-x, -y)$, it helps to rewrite the equation for Z as

$$x^2y^2 = cx^2(x^2 + 1)(x^4 + sx^2 + 1).$$

Since xy and x^2 are both fixed by the involution, the quotient is given by the equation

$$y^2 = cx(x+1)(x^2 + sx + 1).$$

If we replace (x, y) with $(1/x, y/x^2)$, we obtain (2.4) and hence the second quotient is isomorphic to E.

These two involutions generate a subgroup of $\mathrm{Aut}(Z)$ isomorphic to the Klein four-group. The product of these involutions is the hyperelliptic involution κ; the quotient of Z by κ is the projective line. By [10, Theorem C], $\mathrm{Jac}(Z)$ is isogenous to the product of the Jacobians of the three quotients, thus $\mathrm{Jac}(Z) \sim \mathrm{Jac}(E)^2 \cong E^2$. □

Let $s' = (-2s + 12)/(s + 2)$ and $c' = 2c(s + 2)$, and let E' be the elliptic curve

$$E': \quad y^2 = c'(x+1)(x^2 + s'x + 1).$$

Note that there is a 2-isogeny $E \to E'$ given by

$$(x, y) \mapsto \left(\frac{1}{s+2} \frac{(2x+s)(x-1)}{(x+1)}, \frac{4}{s+2} \frac{(x^2+2x+s-1)}{(x+1)^2}\, y \right),$$

whose kernel contains the 2-torsion point $P = (-1, 0)$ of E. The kernel of the dual isogeny $E' \to E$ contains the 2-torsion point $P' = (-1, 0)$ of E'.

Lemma 2.7. *The quotient of Z by each of the involutions $(x, y) \mapsto (1/x, \pm y/x^3)$ is isomorphic to E'.*

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Proof. Replacing x with $(x+1)/(x-1)$ and y with $y/(x-1)^3$ in the equation for Z, we find that Z can also be written as

$$y^2 = c'(x^2+1)(x^4+s'x^2+1).$$

The two involutions $(x,y) \mapsto (1/x, \pm y/x^3)$ in the original model become the involutions $(x,y) \mapsto (-x, \mp y)$ in the new model. The result follows from Lemma 2.6. □

Lemma 2.6 says that there is an isogeny $E^2 \to \mathrm{Jac}(Z)$, but we can be much more precise.

Proposition 2.8. *Let E be as above, let $P = (-1,0) \in E[2]$, and let Q and R be the other two geometric points of order 2 on E. Let $\psi\colon E[2] \to E[2]$ be the automorphism that fixes P and swaps Q and R. Then there is an isogeny $\varphi\colon E \times E \to \mathrm{Jac}(Z)$ whose kernel is the graph of ψ, and the pullback via φ of the principal polarization on $\mathrm{Jac}(Z)$ is twice the product polarization on $E \times E$.*

Proof. Because there is a degree-2 map $Z \to E$, the general theory set out in [11, §2] shows that there are an elliptic curve F, an isomorphism $\psi\colon E[2] \to F[2]$, and an isogeny $E \times F \to \mathrm{Jac}(Z)$ satisfying the conclusion of the proposition. The explicit construction carried out in [5, §3] shows that $F \cong E$ and that ψ is the isomorphism specified in the statement. □

In fact, almost every pair (E,P) consisting of an elliptic curve E over K and a K-rational 2-torsion point arises in this way.

Proposition 2.9. *Let E be an elliptic curve over K with a rational point P of order 2. Then there is a genus-2 curve Z over K with D_4-action that gives rise to this (E,P) as above if and only if E does* not *have a geometric automorphism $\alpha \neq \pm 1$ that fixes P.*

Proof. Given an E and a P as in the statement of the proposition, we may choose a model $y^2 = x(x^2+ax+b)$ for E so that P is the point $(0,0)$. Let $\psi\colon E[2] \to E[2]$ be the automorphism that fixes P and swaps the other two points of order 2. If there is no geometric automorphism of E that restricts to ψ on $E[2]$, then the construction of [5, Proposition 4, p. 324] produces a genus-2 curve Z of the form (2.1), and we check that the E and P produced by this curve as above are the E and P we started with.

If there *is* a geometric automorphism α of E that restricts to ψ, then the geometric isogeny $\varphi\colon E \times E \to E \times E$ that takes (U,V) to $(U+\alpha^{-1}(V), V-\alpha(U))$ has kernel equal to the graph of ψ, and the pullback via φ of the product polarization is twice the product polarization. If there were a curve Z that gave rise to (E,P), then by Proposition 2.8 the polarized Jacobian of Z would be geometrically isomorphic to $E \times E$ with the product polarization, which is impossible. To complete the proof, we just need to observe that over fields of characteristic not 2, every automorphism $\alpha \neq \pm 1$ of an elliptic curve that fixes one point of order 2 necessarily swaps the other two. □

2.5. **Related families of genus-2 curves with D_4-action.** If K is algebraically closed, Cardona and Quer [2, Proposition 2.1] show that every genus-2 curve Y with $\mathrm{Aut}(Y) \cong D_4$ is a member of the family

$$Y_v\colon \quad y^2 = x^5 + x^3 + vx,$$

where $v \in K \setminus \{0, 1/4, 9/100\}$.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

The advantage of this family is that every geometric isomorphism class of a curve with automorphism group D_4 corresponds to exactly one value of v, as opposed to the family Z in (2.1). The disadvantage is that the automorphisms of this curve are not necessarily defined over the field generated by the parameter v.

Moonen [16] studied cyclic covers of $\mathbb{P}^1$ given by monodromy data. One of the twenty families of curves that appear in his work is the cyclic degree-4 cover of $\mathbb{P}^1$ given by

$$X_T\colon \quad z^4 = x(x-1)^2(x-T)^2.$$

The curve X_T has genus 2 and $\mathrm{Aut}_{\bar{K}}(X_T) \cong D_4$ for a generic choice of T. This model makes the order-4 automorphism very apparent, but the hyperelliptic structure is not as clearly visible.

3. The 2-torsion and unramified elementary abelian 2-covers

In this section, we study unramified elementary abelian 2-covers of the curves Z defined by (2.1). Throughout this section, we assume all Weierstrass points of Z are defined over K. Let ζ be a primitive fourth root of unity in K. Then Z can be given by

$$Z\colon \quad y^2 = c(x-\zeta)(x+\zeta)(x-t)(x+t)(x-1/t)(x+1/t), \quad \text{where} \tag{3.1}$$

$$s = -(t^4+1)/t^2. \tag{3.2}$$

3.1. **Unramified elementary abelian 2-covers.** Let $P \in Z(K)$ be the Weierstrass point $(\zeta, 0)$. Since there is a K-rational automorphism of Z taking P to $(-\zeta, 0)$, the choice of ζ does not affect the K-isomorphism class of the 2-covers we construct. Note that P and $(-\zeta, 0)$ are distinguished from the other Weierstrass points of Z by the fact that they form an orbit of size 2 under the action of D_4; the other Weierstrass points form an orbit of size 4.

Definition 3.1. Let $\iota_P\colon Z \hookrightarrow \mathrm{Jac}(Z)$ be the Abel-Jacobi embedding that sends $Q \in Z(\bar{K})$ to the divisor class $[Q-P]$. Let $\pi^{\mathbf{0}}\colon \widetilde{Z} \to Z$ be the pullback of the multiplication-by-2 map on $\mathrm{Jac}(Z)$ by $\iota_P\colon Z \hookrightarrow \mathrm{Jac}(Z)$.

Our assumption that the Weierstrass points of Z are K-rational implies that the cover $\mathrm{Jac}(Z) \to \mathrm{Jac}(Z)$ given by the multiplication-by-2 map is Galois, with Galois group isomorphic to $\mathrm{Jac}(Z)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$; the group $\mathrm{Jac}(Z)[2]$ acts on the cover by translation. Since $\pi^{\mathbf{0}}$ is defined as a pullback of this cover, $\pi^{\mathbf{0}}$ is also Galois, with Galois group canonically isomorphic to $\mathrm{Jac}(Z)[2]$. In fact, geometric class field theory shows that we can recognize $\pi^{\mathbf{0}}$ as the maximal unramified abelian extension of Z with Galois group of exponent 2 in which the base point $P = (\zeta, 0)$ splits completely.

Definition 3.2. For a subgroup H of $\mathrm{Jac}(Z)[2]$, let $\widetilde{Z}^H$ be the quotient of $\widetilde{Z}$ by H. Let $\pi^H\colon \widetilde{Z}^H \to Z$ be the quotient cover.

For example, $\widetilde{Z}^{\mathbf{0}} = \widetilde{Z}$ and $\widetilde{Z}^{\mathrm{Jac}(Z)[2]} = Z$. More generally, the degree of π^H equals the index of H in $\mathrm{Jac}(Z)[2]$. Since $\mathrm{Jac}(Z)[2]$ is abelian, π^H is Galois with Galois group isomorphic to $\mathrm{Jac}(Z)[2]/H$. Furthermore, the genus of $\widetilde{Z}^H$ equals $[\mathrm{Jac}(Z)[2] : H] + 1$ by the Riemann–Hurwitz formula.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Remark 3.3. If we pick a different basepoint P' instead of P and keep track of the basepoint dependence by labeling the 2-covers as $\widetilde{Z}_P$ and $\widetilde{Z}_{P'}$, and if we let $Q \in \mathrm{Jac}(Z)(\bar{K})$ be a point with $2Q = P - P'$, then translation by Q on $\mathrm{Jac}(Z)(\bar{K})$ yields a geometric isomorphism from $\widetilde{Z}_P$ to $\widetilde{Z}_{P'}$. We will prove in the following paragraph that there exists an elementary abelian 2-extension L of K of degree at most 2^4 such that $Q \in \mathrm{Jac}(Z)(L)$, so this translation isomorphism will be defined over L. In particular, when K is a finite field, then L is at worst a quadratic extension of K, and the curve $\widetilde{Z}_{P'}$ is a (possibly trivial) quadratic twist of $\widetilde{Z}_P$. From now on, we fix the base point to be $P = (\zeta, 0)$ for all π^H.

The following argument was provided by Bjorn Poonen. The obstruction to dividing a point of $\mathrm{Jac}(Z)(K)$ by 2 lies in $H^1(K, \mathrm{Jac}(Z)[2])$. Since all the Weierstrass points are defined over K, we know that $\mathrm{Jac}(Z)[2] \cong \mu_2^4$ as a Galois module. Hence, the obstruction to dividing $P' - P$ by 2 lies in $H^1(K, \mathrm{Jac}(Z)[2]) \cong (H^1(K, \mu_2))^4 = (K^\times/K^{\times 2})^4$, so there exists an elementary abelian 2-extension L/K of degree at most 2^4 such that the image of this class in $H^1(L, \mathrm{Jac}(Z)[2]) = (L^\times/L^{\times 2})^4$ is trivial. When K is a finite field of characteristic not 2, over its unique elementary abelian 2-extension L, this obstruction class vanishes. Thus $\widetilde{Z}_{P'}$ is a quadratic twist of $\widetilde{Z}_P$.

3.2. **Decomposition of the Jacobian.** In this section, we determine the isogeny decomposition of $\mathrm{Jac}(Z^H)$ over K.

Definition 3.4. Given a cover $\pi\colon V \to Z$, let Prym^π denote the Prym variety of π, that is, the identity component of the kernel of the induced norm homomorphism $\mathrm{Jac}(V) \to \mathrm{Jac}(Z)$. There is a K-isogeny $\mathrm{Jac}(V) \sim \mathrm{Jac}(Z) \times \mathrm{Prym}^\pi$.

Definition 3.5. For a subgroup H of $\mathrm{Jac}(Z)[2]$, we set $\mathrm{Prym}^H := \mathrm{Prym}^{\pi^H}$, where π^H is the cover defined in Definition 3.2.

Proposition 3.6. *Let Z be a genus-2 curve with D_4-action whose Weierstrass points are defined over K. For every $H \subseteq \mathrm{Jac}(Z)[2]$, there is an isogeny*

$$\mathrm{Jac}(\widetilde{Z}^H) \sim E^2 \times \prod_{\substack{H \subseteq H' \subseteq \mathrm{Jac}(Z)[2] \\ [\mathrm{Jac}(Z)[2]:H']=2}} \mathrm{Prym}^{H'}. \tag{3.3}$$

Proof. Let $G = \mathrm{Jac}(Z)[2]$ and $r = [G : H]$, and enumerate the index-2 subgroups of G containing H by $H'_1, \cdots, H'_{r-1}$. We apply [10, Theorem C] to the $\{H'_i\}$ together with H and G. More precisely, we define

$$H_i := \begin{cases} H'_i & \text{for } i = 1, \dots r-1, \\ H & \text{for } i = r, \\ G & \text{for } i = r+1, \end{cases} \quad \text{and} \quad n_i := \begin{cases} -1 & \text{for } i = 1, \dots r-1, \\ 1 & \text{for } i = r, \\ r-2 & \text{for } i = r+1. \end{cases}$$

Let g_{ij} be the genus of $Z^{H_i H_j}$. The group $H_i H_j$ must be one of $H'_1, \cdots, H'_{r-1}, H, G$. We know from Riemann–Hurwitz that the genus of $\widetilde{Z}^H$ is $r+1$, the genus of each $\widetilde{Z}^{H'_i}$ is 3, and the genus of $\widetilde{Z}^G$ is 2. Using this information and some casework, we see that

$$g_{ij} = \begin{cases} 2 & \text{if } i \neq j \text{ and } i, j \leq r-1, \\ 3 & \text{if } i = j \leq r-1, \\ 3 & \text{if } i \leq r-1 \text{ and } j = r, \text{ or } i = r \text{ and } j \leq r-1, \\ r+1 & \text{if } i = j = r, \\ 2 & \text{if } i \text{ or } j \text{ is } r+1. \end{cases}$$

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

We check the conditions to apply [10, Theorem C]: first, $H_iH_j = H_jH_i$ is satisfied because G is abelian; and second, $\sum_i n_i g_{ij} = 0$ for all $j \in \{1, \dots, r+1\}$ by our computations above. Therefore the conclusion of [10, Theorem C] holds, namely, there exists a K-isogeny

$$\prod_{n_i>0} \mathrm{Jac}(\widetilde{Z}^{H_i})^{n_i} \sim \prod_{n_j<0} \mathrm{Jac}(\widetilde{Z}^{H_j})^{-n_j},$$

which for us becomes

$$\mathrm{Jac}(\widetilde{Z}^{H}) \times (\mathrm{Jac}(Z))^{r-2} \sim \prod_{\substack{H \subseteq H' \subseteq \mathrm{Jac}(Z)[2] \\ [\mathrm{Jac}(Z)[2]:H']=2}} \mathrm{Jac}(\widetilde{Z}^{H'}).$$

Now we substitute $\mathrm{Jac}(\widetilde{Z}^{H'}) \sim \mathrm{Jac}(Z) \times \mathrm{Prym}^{H'}$, cancel $(\mathrm{Jac}(Z))^{r-2}$ from both sides, and substitute $\mathrm{Jac}(Z) \sim E^2$ (from Lemma 2.6) to finish. □

3.3. **The Weil pairing.**

Definition 3.7. Let $R = \{\zeta, -\zeta, t, -t, 1/t, -1/t\}$. For $r \in R$, let W_r denote the Weierstrass point $(r, 0)$ of Z.

Lemma 3.8. *If $D \in \mathrm{Jac}(Z)[2]$, then there exist $u, v \in R$ such that $D = [W_u - W_v]$.*

Proof. We know $\mathrm{Jac}(Z)[2]$ is generated by $[W_r - W_\zeta]$ for $r \in R \setminus \{\zeta\}$ with the single relation $\sum_r [W_r - W_\zeta] = 0$. The conclusion follows from a straightforward computation. □

Definition 3.9. Let $e_2(\cdot, \cdot)$ denote the Weil pairing on $\mathrm{Jac}(Z)[2]$, which takes values in $\{\pm 1\} \subset K^\times$. For every subgroup H of $\mathrm{Jac}(Z)[2]$, define $H^\perp$ by

$$H^\perp := \{S \in \mathrm{Jac}(Z)[2] \ : \ e_2(Q, S) = 1 \text{ for all } Q \in H\}.$$

For later use, we give an explicit description of the Weil pairing on 2-torsion points.

Lemma 3.10. *For nonzero elements $[W_{u_1} - W_{v_1}]$ and $[W_{u_2} - W_{v_2}]$ of $\mathrm{Jac}(Z)[2](K)$, we have $e_2([W_{u_1} - W_{v_1}], [W_{u_2} - W_{v_2}]) = -1$ if and only if $\#(\{u_1, v_1\} \cap \{u_2, v_2\}) = 1$.*

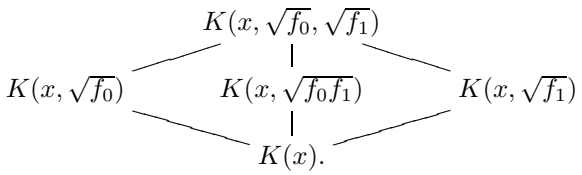
Proof. This is a direct calculation using a well-known formula for the Weil pairing (see [4, Theorem 1]). □

Proposition 3.11. *Let H' be an index-2 subgroup of $\mathrm{Jac}(Z)[2]$ and let $U = [W_u - W_v]$ be the generator of $(H')^\perp$. Define $a \in K^\times / K^{\times 2}$ by*

$$a := \begin{cases} c(\zeta - u)(\zeta - v) & \text{if } \zeta \notin \{u, v\}, \\ \prod_{r \in R \setminus \{u,v\}} (\zeta - r) & \text{if } \zeta \in \{u, v\}. \end{cases}$$

Let E' be the genus-1 curve given by the equation $y^2 = a \prod_{r \in R \setminus \{u,v\}} (x - r)$. Then there is a K-isogeny $\mathrm{Prym}^{H'} \sim \mathrm{Jac}(E')$.

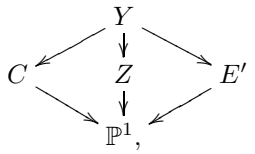
Proof. Let $f_0 = ac(x - u)(x - v)$ and $f_1 = a \prod_{r \in R \setminus \{u,v\}} (x - r)$, and consider the V_4-diagram of function fields



This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

If we let C be the genus-0 curve $y^2 = f_0$, the diagram above gives us a V_4-diagram of curves

(3.4)



where Y is the curve with function field $K(x, \sqrt{f_0}, \sqrt{f_1})$. The value of a was chosen so that the point $x = \zeta$ of $\mathbb{P}^1$ splits in one of the extensions $C \to \mathbb{P}^1$ and $E' \to \mathbb{P}^1$ and ramifies in the other, and it follows that the Weierstrass point $P = (\zeta, 0)$ of Z splits in the quadratic extension $Y \to Z$. Since $Y \to Z$ is a Galois extension with group of exponent 2 in which P splits completely, it must be a subextension of $\widetilde{Z} \to Z$, which as we noted earlier is the maximal such extension. This tells us that the element f_0 of $K(Z)^\times$ is a square in $K(\widetilde{Z})^\times$.

In fact, we see that the map $U \mapsto f_0$ defines an injective homomorphism

$$\gamma\colon \operatorname{Jac}(Z)[2] \to (K(Z)^\times \cap K(\widetilde{Z})^{\times 2})/K(Z)^{\times 2}.$$

If we let G be the latter group, then Kummer theory says that there is a perfect pairing

$$\operatorname{Gal}(\widetilde{Z}/Z) \times G \to \{\pm 1\} \subset K^\times.$$

In particular, $\#G = \#\operatorname{Gal}(\widetilde{Z}/Z) = \#\operatorname{Jac}(Z)[2]$, so the injective homomorphism γ is an isomorphism. This isomorphism, together with the canonical isomorphism $\operatorname{Jac}(Z)[2] \cong \operatorname{Gal}(\widetilde{Z}/Z)$, turns the Kummer pairing into a perfect pairing

$$\operatorname{Jac}(Z)[2] \times \operatorname{Jac}(Z)[2] \to \{\pm 1\}.$$

As is observed in [4, §2], this pairing is in fact the Weil pairing; this can be seen by using the explicit formula for the natural pairing of the m-torsion of an abelian variety with that of its dual [14, §16] and the fact that the pullback of the Abel–Jacobi map $Z \to \operatorname{Jac}(Z)$ is equal to $-\lambda^{-1}\colon \widehat{\operatorname{Jac}(Z)} \to \operatorname{Jac}(Z)$, where $\lambda\colon \operatorname{Jac}(Z) \to \widehat{\operatorname{Jac}(Z)}$ is the canonical polarization on $\operatorname{Jac}(Z)$ [15, Lemma 6.9 and Remark 6.10(c)].

From this we conclude the cover $Y \to Z$ is $\pi^{H'}$. Furthermore, we see from Diagram (3.4) and [10, Theorem C] that $\operatorname{Jac}(Y) \sim \operatorname{Jac}(Z) \times \operatorname{Jac}(E')$, so $\operatorname{Prym}^{H'} \sim \operatorname{Jac}(E')$. □

3.4. **The D_4-action on the factors of $\operatorname{Jac}(\widetilde{Z})$.** Applying Proposition 3.11 to the fifteen index-2 subgroups of $\operatorname{Jac}(Z)[2]$ yields fifteen elliptic curves.

Definition 3.12. Given a nonzero $U \in \operatorname{Jac}(Z)[2]$, let E_U be the elliptic curve obtained by applying Proposition 3.11 to the index-2 subgroup $\langle U \rangle^\perp$. If u and v are the unique elements of R such that U is equal to the divisor class $[W_u - W_v] = [W_v - W_u]$, we also write $E_{\{u,v\}}$ for E_U.

Corollary 3.13. *There is a K-isogeny*

$$\operatorname{Jac}(\widetilde{Z}) \sim E^2 \times \prod_U E_U,$$

where the product is over nonzero $U \in \operatorname{Jac}(Z)[2]$.

Proof. Combine Proposition 3.6 with $H = \mathbf{0}$ and Proposition 3.11. □

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Proposition 3.14. *The set of nonzero elements of* $\mathrm{Jac}(Z)[2]$ *breaks up into six orbits under the action of* D_4*, as listed in Table* 1*. For each* U *in an orbit, the table presents a value* $a \in K^\times$ *as in Proposition* 3.11*, and values of* λ *and* d *such that* E_U *is isomorphic to* $y^2 = dx(x-1)(x-\lambda)$*.*

TABLE 1. The fifteen elliptic curves E_U for nonzero $U \in \mathrm{Jac}(Z)[2]$, labeled as in Definition 3.12, grouped in their orbits under the action of D_4. The value of a is as in Proposition 3.11, and the values of λ and d are such that E_U is also isomorphic to $y^2 = dx(x-1)(x-\lambda)$. Recall that each E_U can be recovered as the Prym variety of the double cover of Z associated, as in Proposition 3.11, to the subgroup $H' \subseteq \mathrm{Jac}(Z)[2]$ that pairs trivially with U under the Weil pairing.

Orbit label	Point label	a	λ	d
1	$\{\zeta, -\zeta\}$	1	$4t^2/(t^2+1)^2$	1
2A	$\{t, -t\}$	$c(t^2+1)$	$4\zeta t/(t+\zeta)^2$	$c(t^2+1)$
	$\{1/t, -1/t\}$	$c(t^2+1)$		
2B	$\{-t, -1/t\}$	$\zeta ct(t^2+1)$	$2(t^2-1)/(t+\zeta)^2$	$c(t^2+1)$
	$\{t, 1/t\}$	$\zeta ct(t^2+1)$		
2C	$\{t, -1/t\}$	ζct	-1	$c(t^2+1)$
	$\{-t, 1/t\}$	ζct		
4A	$\{\zeta, 1/t\}$	$\zeta t(t+\zeta)$	$-2\zeta t/(t-\zeta)^2$	ζ
	$\{\zeta, -t\}$	$(t+\zeta)$		
	$\{-\zeta, -1/t\}$	$\zeta ct(t-\zeta)$	$-2\zeta t/(t-\zeta)^2$	$\zeta c(t^2+1)$
	$\{-\zeta, t\}$	$c(t-\zeta)$		
4B	$\{\zeta, t\}$	$(t-\zeta)$	$2\zeta t/(t+\zeta)^2$	ζ
	$\{\zeta, -1/t\}$	$\zeta t(t-\zeta)$		
	$\{-\zeta, -t\}$	$c(t+\zeta)$	$2\zeta t/(t+\zeta)^2$	$\zeta c(t^2+1)$
	$\{-\zeta, 1/t\}$	$\zeta ct(t+\zeta)$		

Proof. The generators σ and τ of the D_4 subgroup of $\mathrm{Aut}(Z)$ act on the curve labels via

$$\sigma(\{u,v\}) = \{-u,-v\} \quad \text{and} \quad \tau(\{u,v\}) = \{1/u, 1/v\},$$

so the grouping into orbits is clear. The value of a is determined via Proposition 3.11, and the associated λ and d are computed by applying a linear fraction transformation to put the curve E' from Proposition 3.11 into Legendre form. □

Remark 3.15. Suppose an element $\alpha \in \mathrm{Aut}(Z)$ takes $U \in \mathrm{Jac}(Z)[2]$ to V. If α does not fix the base point $(\zeta, 0)$ by which we embedded Z into $\mathrm{Jac}(Z)$, then α does not necessarily provide a K-rational isomorphism between E_U and E_V, because the base point determines the appropriate twist of the elliptic curve associated to a

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

2-torsion point. We see this, for example, in Orbits 4A and 4B: each of these orbits has two different values of d.

Remark 3.16. The order-4 automorphism of Z induces an order-4 automorphism ζ of $\mathrm{Jac}(Z)$, such that multiplication by 2 factors as $(1-\zeta)(1+\zeta)$. A natural object of study is the degree-4 cover of Z whose Jacobian contains orbits 1 and 2C; it arises as $\widetilde{Z}^H$ when $H := \mathrm{Ker}(1-\zeta)$. See Sections 5 and 6 for more details.

4. Heuristics for isogenous curves

Let q be a power of an odd prime p and let $K \cong \mathbb{F}_q$ be a finite field of order q. In this section, we consider genus-2 curves Z over K having the property that $D_4 \subseteq \mathrm{Aut}(Z)$. We study unordered pairs of nonisomorphic curves of this type whose Jacobians are isogenous to one another. The main result of this section is Theorem 4.6, which gives upper and lower bounds for the number of these unordered pairs in terms of q.

4.1. **The moduli space of genus-2 curves with D_4-action.** Recall from Notation 2.1 that $\mathcal{Z}$ is the set of K-isomorphism classes of objects (Z,ϵ), where Z is a genus-2 curve over K and where $\epsilon\colon D_4 \hookrightarrow \mathrm{Aut}(Z)$ is an embedding. Let $\overline{\mathcal{Z}}$ denote the set of K-isomorphism classes of genus-2 curves over K such that $D_4 \subseteq \mathrm{Aut}(Z)$, and let $\nu\colon \mathcal{Z} \to \overline{\mathcal{Z}}$ be the forgetful morphism taking the object (Z,ϵ) to the curve Z. At the beginning of Section 2 we defined ξ to be the involution of D_4 that swaps the generators a and b. We can define an involution on $\mathcal{Z}$ as well, by sending (Z,ϵ) to $(Z,\epsilon\xi)$.

Notation 4.1. Let $\mathcal{X}$ be the set of isomorphism classes of objects (E,P), where E is an elliptic curve over K and P is a K-rational point of order 2 on E. Two such objects (E_1,P_1) and (E_2,P_2) are isomorphic if there is a K-rational isomorphism $E_1 \to E_2$ taking P_1 to P_2.

Let χ be the involution on $\mathcal{X}$ that sends a pair (E,P) to the pair (E',P'), where $E' = E/\langle P\rangle$ and where P' is the generator of the kernel of the dual isogeny $E' \to E$. Let $\mathcal{X}_{-8} \subset \mathcal{X}$ be the subset consisting of those objects (E,P) such that E has a *K-rational* endomorphism β with $\beta^2 = -2$ for which $\beta(P) = 0$. Let $\mathcal{X}_{-4} \subset \mathcal{X}$ be the subset consisting of those (E,P) such that E has a *geometric* automorphism α satisfying $\alpha^2 = -1$ for which $\alpha(P) = P$. Finally, let $\mathcal{X}' = \mathcal{X} \setminus \mathcal{X}_{-4}$. The involution χ on $\mathcal{X}$ restricts to an involution on $\mathcal{X}'$.

In Section 2.4, we associated to every genus-2 curve with D_4-action (Z,ϵ) an elliptic curve E and a 2-torsion point P on E. Thus there is a map $\mu\colon \mathcal{Z} \to \mathcal{X}$ that sends the isomorphism class of (Z,ϵ) to that of (E,P).

Proposition 4.2. *The map μ is injective and has image $\mathcal{X}'$. It takes the involution $(Z,\epsilon) \mapsto (Z,\epsilon\xi)$ of $\mathcal{Z}$ to the involution χ on $\mathcal{X}'$. The map $\nu\colon \mathcal{Z} \to \overline{\mathcal{Z}}$ that sends (Z,ϵ) to Z is 2-to-1, unless (Z,ϵ) is fixed by ξ or, equivalently, unless $\mu(Z,\epsilon) \in \mathcal{X}_{-8}$.*

Proof. Let $(E,P) \in \mathcal{X}$. By Proposition 2.9, there exists $(Z,\epsilon) \in \mathcal{Z}$ such that $\mu(Z,\epsilon) = (E,P)$ if and only if there is no automorphism $\alpha \neq \pm 1$ of E that fixes P. Combining this with the observation that an automorphism $\alpha \neq \pm 1$ of an elliptic curve in characteristic not 2 that fixes a 2-torsion point must have order 4, we find that (E,P) is in the image of μ if and only if it lies in $\mathcal{X}'$.

Next we show that a genus-2 curve with D_4-action (Z,ϵ) can be recovered from its image (E,P) under μ. To see this, we first write down a short Weierstrass

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

model for E such that P is the point $(0,0)$. Such a model is of the form $y^2 = x(x^2+dx+e)$, and the model is unique up to scaling x and y. The coefficient e is nonzero because the model is nonsingular, and d is also nonzero, because otherwise the map $(x,y) \mapsto (\zeta x, -y)$ would be an automorphism of order 4 that fixes P, and E has no such automorphisms because (E,P) lies in $\mathcal{X}'$. There is a unique way to scale x so that the model becomes $y^2 = cx(x^2+fx-f)$ for $c, f \in K^\times$ with $f \neq -4$; the value of f is unique, and the value of c is unique up to squares. Replacing x with $x+1$ transforms the model into $y^2 = c(x+1)(x^2+sx+1)$, where $s = f+2 \neq \pm 2$ and where $P = (-1,0)$. We have shown that (E,P) determines unique values of $s \in K$ and $c \in K^\times/K^{\times 2}$, and these values determine a unique genus-2 curve with D_4-action, via Equations (2.1) and (2.2), so μ is injective.

Lemmas 2.6 and 2.7 show that if $\mu(Z,\epsilon) = (E,P)$ then $\mu(Z,\epsilon\xi) = (E',P')$, so μ takes the involution $(Z,\epsilon) \mapsto (Z,\epsilon\xi)$ to χ.

The fact that ν is 2-to-1 except for the objects (Z,ϵ) that are isomorphic to $(Z,\epsilon\xi)$ follows from Lemma 2.5 and its proof. By the preceding statements, (Z,ϵ) and $(Z,\epsilon\xi)$ are isomorphic if and only if (E,P) is fixed by χ, meaning that (E,P) and (E',P') are isomorphic. This is true if and only if E has an endomorphism β, whose kernel is generated by P, such that $\beta^2 = 2u$ for a unit u in $\mathrm{End}(E)$. The only possibilities are that: (i) $\beta = \pm 1 \pm \zeta$ where $\zeta \in \mathrm{Aut}(E)$ with $\zeta^2 = -1$, in which case $(E,P) \notin \mathcal{X}'$, or (ii) β satisfies $\beta^2 = -2$. □

Remark 4.3. As the preceding proof shows, the curves $Z \in \overline{\mathcal{Z}}$ that have only one preimage in $\mathcal{Z}$ correspond to the exceptional curves in Lemma 2.5, that is, the curves with $s = -6$ when -2 is a square. We note that when $s = -6$ the associated elliptic curve E has j-invariant 8000, which is the unique root of the Hilbert class polynomial for $\mathbb{Z}[\sqrt{-2}]$. The endomorphisms $\beta \in \mathrm{End}(E)$ with $\beta^2 = -2$ kill the 2-torsion point $P = (-1,0)$, and these endomorphisms are K-rational if and only if -2 is a square.

Remark 4.4. We can view $\mathcal{Z}$ as the coarse moduli space for objects (Z,ϵ) as in Notation 2.1. Similarly, we can view $\mathcal{X}$ as the coarse moduli space $Y_1(2) \cong Y_0(2)$, namely the modular curve $X_1(2)$ with its cusp removed. Then, under the embedding $\mathcal{Z} \hookrightarrow Y_0(2)$ the involution associated to $\mathcal{Z} \to \overline{\mathcal{Z}}$ is the Fricke involution on $Y_0(2)$. The language of moduli spaces is not useful to us here since these are not fine moduli spaces and we need to keep track of the field of definition of the objects.

4.2. **Counting isogenous pairs of curves with D_4-action.**

Definition 4.5. Let $P(q)$ denote the number of unordered pairs $\{Z_1, Z_2\}$, where $Z_1, Z_2 \in \overline{\mathcal{Z}}$ are not isomorphic to one another and $\mathrm{Jac}(Z_1)$ and $\mathrm{Jac}(Z_2)$ are isogenous.

Theorem 4.6 determines the rate of growth of $P(q)$ up to logarithmic factors.

Theorem 4.6. *There are constants $d_1, d_2 > 0$ such that for all odd prime powers $q > 7$,*

$$d_1 q^{3/2} \leq P(q) \leq d_2 q^{3/2} (\log q)^2 (\log\log q)^4.$$

If the generalized Riemann hypothesis holds, there is a constant $d_3 > 0$ such that

$$P(q) \leq d_3 q^{3/2} (\log\log q)^6.$$

Remark 4.7. Direct calculation shows that $P(q) = 0$ for $q = 3$, 5, and 7, so the hypothesis that $q > 7$ in Theorem 4.6 is necessary.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Before we get to the proof of Theorem 4.6, we present some definitions and lemmas that we will need.

Proposition 2.8 shows that if Z is a genus-2 curve over K with D_4-action, then $\mathrm{Jac}(Z)$ is isogenous to E^2, where E is an elliptic curve with a rational 2-torsion point. Since E has a rational point of order 2, $\#E(K)$ is even, and since q is odd, the trace of Frobenius for E must also be even. This shows that the Weil polynomial of $\mathrm{Jac}(Z)$ is of the form $(x^2 - tx + q)^2$, for an even integer t with $t^2 \le 4q$.

Definition 4.8. For each even integer t with $t^2 \le 4q$, let $M(q,t)$ denote the number of $Z \in \overline{\mathcal{Z}}$ whose Weil polynomial is $(x^2-tx+q)^2$, and let $N(q,t)$ denote the number of elliptic curves over K with trace t.

Lemma 4.9. *For all odd prime powers q and even integers t with $t^2 \le 4q$ we have $M(q,t) \le 3N(q,t)$.*

Proof. For each curve $Z \in \overline{\mathcal{Z}}$ with Weil polynomial $(x^2 - tx + q)^2$, choose an embedding $\epsilon\colon D_4 \hookrightarrow \mathrm{Aut}(Z)$. Proposition 4.2 shows that (Z,ϵ) gives rise to a unique pair (E,P) with $\mathrm{trace}(E) = t$, so $M(q,t)$ is at most the number of such pairs. Since an elliptic curve has at most three rational points of order 2, we have $M(q,t) \le 3N(q,t)$. □

Lemma 4.10. *There is a constant d_4 such that for all odd prime powers q and even integers t with $t^2 \le 4q$, we have*

$$N(q,t) < d_4\sqrt{q}(\log q)(\log\log q)^2.$$

If the generalized Riemann hypothesis holds, there is a constant d_5 such that for all odd prime powers q and even integers t with $t^2 \le 4q$, we have

$$N(q,t) < d_5\sqrt{q}(\log\log q)^3.$$

Proof. This follows from the formulas for $N(q,t)$ found in [18, Theorem 4.6, pp. 194–196]), combined with the bounds on Kronecker class numbers found in [1, Lemma 4.4, p. 49]. □

Proof of Theorem 4.6. Clearly,

$$P(q) = \sum_{\substack{t^2\le 4q\\ t \text{ even}}} \binom{M(q,t)}{2} = \sum_{\substack{t^2\le 4q\\ t \text{ even}}} M(q,t)^2/2 - \sum_{\substack{t^2\le 4q\\ t \text{ even}}} M(q,t)/2.$$

The number of even t with $t^2 \le 4q$ is at most $2\sqrt{q}+1$. By the Cauchy–Schwarz inequality,

$$\sum M(q,t)^2 \ge \frac{\left(\sum M(q,t)\right)^2}{(2\sqrt{q}+1)},$$

where each sum is over the set of even t with $t^2 \le 4q$. By Lemma 2.5, the sum of the $M(q,t)$ is either $q-2$ or $q-3$, so

$$P(q) \ge \frac{(q-3)^2}{2(2\sqrt{q}+1)} - \frac{q-2}{2}.$$

From this we can show that $P(q) \ge q^{3/2}/23$ for $q \ge 17$. By direct computation we find that $P(9) = 6$, $P(11) = 3$, and $P(13) = 6$, so we have $P(q) \ge q^{3/2}/23$ for all $q > 7$.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

To prove the upper bounds on $P(q)$, we use Lemmas 4.9 and 4.10 to see that

$$P(q) = \sum_{\substack{t^2 \le 4q \\ t \text{ even}}} \binom{M(q,t)}{2} < \frac{81}{2} \sum_{\substack{t^2 \le 4q \\ t \text{ even}}} N(q,t)^2$$

$$\le \frac{81}{2}(2\sqrt{q}+1) \begin{cases} d_4^2\, q(\log q)^2(\log\log q)^4 & \text{in general;} \\ d_5^2\, q(\log\log q)^6 & \text{if GRH holds.} \end{cases}$$

The upper bounds in the theorem follow. □

4.3. **Gathering data.** Proposition 4.2 and the ideas in Section 4.2 allow us to quickly compute the exact value of $P(q)$ when q is not too large. The subtleties in the computation include computing the objects (E, P) that lie in $\mathcal{X}_{-8}$ and in $\mathcal{X}_{-4}$, and, for each even trace t, determining the number of elliptic curves with trace t that have exactly one point of order 2 and the number that have exactly three points of order 2. This latter question is answered by noting that an elliptic curve with Frobenius endomorphism π has three rational points of order 2 if and only if $(\pi - 1)/2$ lies in its endomorphism ring, and by noting that the number of curves with trace t and with a given endomorphism ring can be computed from a class number; see [18, Theorem 4.5, p. 194].

Further details of our method of computing $P(q)$ can be found in the comments of the Magma code we used to do so, which can be found as supplementary material with the arXiv version of this paper as well as on the fourth author's web page: `http://ewhowe.com/papers/paper51.html`.

For $15 \le n \le 24$, we computed the values of $P(q)/q^{3/2}$ for the 1024 odd prime powers q closest to 2^n. For each of these sets of 1024 prime powers we also computed the standard deviation and the minimum and maximum values of $P(q)/q^{3/2}$. These values are presented in Table 2. From Theorem 4.6 and this data, it seems reasonable to model $P(q)$ as growing like a constant times $q^{3/2}$.

TABLE 2. Data for isogenous curves. For each n, we give the mean, standard deviation, and extremal values of $P(q)/q^{3/2}$, where q ranges over the 1024 odd prime powers closest to 2^n.

n	Mean	S.d.	Max	Min
15	0.42025	0.01958	0.45974	0.38473
16	0.42188	0.01949	0.45828	0.38732
17	0.42270	0.01953	0.45792	0.38845
18	0.42394	0.01939	0.45914	0.38996
19	0.42406	0.01955	0.45865	0.39078
20	0.42464	0.01917	0.45862	0.39105
21	0.42514	0.01942	0.45851	0.39203
22	0.42577	0.01922	0.45830	0.39248
23	0.42527	0.01937	0.45843	0.39262
24	0.42557	0.01938	0.45853	0.39276

Remark 4.11. The quantity $P(q)$ was defined so that it counts the number of unordered pairs $\{Z_1, Z_2\}$ of *nonisomorphic* curves with D_4-action and with isogenous

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Jacobians, because clearly Z_1 and Z_2 will have isogenous Jacobians if in fact they are the same curve. There's another "easy" way that two curves can have isogenous Jacobians: If Z_1 and Z_2 are curves over a proper extension $\mathbb{F}_q$ of $\mathbb{F}_p$ that are Galois conjugates of one another, their Jacobians will be isogenous to one another via some power of the Frobenius isogeny. If $q = p^e$, these Galois conjugate pairs account for $\Theta(e^2 q)$ of all the isogenous pairs over $\mathbb{F}_q$, which is an increasingly small fraction of the value of $P(q)$ as $q \to \infty$. However, when we consider the more uncommon doubly isogenous pairs in later sections, we will want to specifically exclude Galois conjugate pairs from our counts.

5. Initial heuristics and data for doubly isogenous curves

By Theorem 4.6, the number of unordered pairs $\{Z_1, Z_2\}$ of genus-2 curves over $K = \mathbb{F}_q$ with D_4-action and with isogenous Jacobians is proportional to $q^{3/2}$, up to logarithmic factors. The frequency naturally decreases if, in addition, we require that Z_1 and Z_2 be doubly isogenous. In this section, we present our initial heuristic about the expected number of doubly isogenous curves over $\mathbb{F}_q$ and some data that we use to test the heuristic.

Remark 5.1. Recall that we associate to a pointed curve (C, P) the cover $\widetilde{C} \to C$ obtained as the pullback of the multiplication-by-2 map on $\mathrm{Jac}(C)$ by the Abel–Jacobi map corresponding to the base point P. We say that two pointed curves (C_1, P_1) and (C_2, P_2) are doubly isogenous if (the Jacobians of) C_1 and C_2 are isogenous and (the Jacobians of) $\widetilde{C}_1$ and $\widetilde{C}_2$ are isogenous. When we are considering a genus-2 curve with D_4-action and with all Weierstrass points rational, there is a natural choice for a base point: one of the two Weierstrass points whose stabilizer under the D_4 action has size 4. (As we saw in Section 3.1, it does not matter which of these two Weierstrass points we choose, because they give isomorphic covers.) Throughout the rest of this paper, in accordance with Remark 3.3, when we say without further comment that two genus-2 curves with D_4-action are doubly isogenous, we mean *with respect to this choice of base point.*

5.1. **An initial heuristic for doubly isogenous curves.**

As we noted in Remark 4.11, two curves Z_1 and Z_2 over a finite field K are trivially doubly isogenous if they are Galois conjugates of one another. This observation influences Definition 5.2.

Definition 5.2. Let $\delta(q)$ be the number of unordered pairs $\{Z_1, Z_2\}$ of doubly isogenous curves over $\mathbb{F}_q$, where Z_1 and Z_2 are genus-2 curves with D_4-action and all Weierstrass points rational, and where Z_1 and Z_2 are not Galois conjugates of one another.

We formulate a heuristic to estimate $\delta(q)$ that we label as "naïve" because it turns out not to match the data we gathered. Later in the paper, we explain this discrepancy and improve the heuristic.

Naïve Heuristic 5.3. *For a fixed odd prime power q, we model the double-isogeny class of Z as a six-tuple of independent random elliptic curves over $\mathbb{F}_q$.*

Justification. By Corollary 3.13, if all of the Weierstrass points of Z are rational then $\mathrm{Jac}(\widetilde{Z})$ decomposes into a sum of 17 elliptic curves, two of which are E. The remaining 15 elliptic curves fall into six orbits under the action of D_4, as in Table 1. The elliptic curve in Orbit $2C$ does not depend on s.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Suppose Z_1 and Z_2 are genus-2 curves with D_4-action, lying over elliptic curves E_1 and E_2 as in Lemma 2.6. For Z_1 and Z_2 to be doubly isogenous over $\bar{K}$, there must be six geometric isogenies of elliptic curves, one between E_1 and E_2 and an additional five for the nonconstant orbits. (These five isogenies may be between orbits with different labels; for example, orbit 2A for one curve may be isogenous to orbit 2B for the other. This only affects the probability that that the five isogenies exist by a constant factor.) With positive probability, a geometric isogeny $\mathrm{Jac}(\widetilde{Z}_1) \sim \mathrm{Jac}(\widetilde{Z}_2)$ comes from a K-rational isogeny, because all the elliptic curves have a bounded number of twists. Thus it is reasonable to model the double-isogeny class of Z as six random elliptic curves. □

Let n be the number of isomorphism classes of genus-2 curves over K with D_4-action and rational Weierstrass points. It follows from the parametrization in terms of the variable t given in (3.1) that $n \asymp q$; the exact count is irrelevant for our purposes. Choose n six-tuples of random elliptic curves over $\mathbb{F}_q$, and denote them by $(E_{i,1}, \dots E_{i,6})$ for $i \in \{1, \dots, n\}$. Define the set

$$S_q := \{(i,j) : i \neq j \text{ and } E_{i,a} \sim E_{j,a} \text{ for } a = 1, 2, \dots, 6\} \subseteq \{1, \dots, n\}^2.$$

Lemma 5.4. *The expected value of $\#S_q$ (which is the prediction of Naïve Heuristic* 5.3 *for the number of pairs of doubly isogenous curves) satisfies*

$$\mathbb{E}(\#S_q) \asymp 1/q.$$

Proof. There are $\Theta(q^2)$ pairs of (i,j), and in Section 4 we showed the probability of two random elliptic curves over $\mathbb{F}_q$ being isogenous is $\Theta(q^{-1/2})$. □

Thus Naïve Heuristic 5.3 predicts that the "expected value" of $\delta(q)$ is $\asymp 1/q$. As we will see, this does not match the data we gathered; the assumption that the 6 elliptic curves are independent does not turn out to be completely accurate.

5.2. **Data that does not support the naïve heuristic.** In order to calculate $\delta(q)$ for specific values of q, we first want to enumerate all isomorphism classes of genus-2 curves Z over $K \cong \mathbb{F}_q$ with D_4-action and with all Weierstrass points rational. To do so, we vary t in (3.1). Letting $s = -(t^4+1)/t^2$ and taking into account the involution $s \leftrightarrow s'$, we see that the following values of t give isomorphic curves:

$$\pm t, \quad \pm\left(\frac{1}{t}\right), \quad \pm\left(\frac{t-1}{t+1}\right), \quad \pm\left(\frac{t+1}{t-1}\right). \tag{5.1}$$

To enumerate isomorphism classes, we fix an ordering of the elements of K and only consider values of t for which $s \neq \pm 2$ (so Z is nonsingular) and for which t is the smallest of the values in (5.1). We then include the curve Z from (3.1) and its standard quadratic twist in our enumeration. If w is a fixed quadratic nonresidue of K, that means we look at

$$y^2 = (x^2+1)(x^4+sx^2+1) \quad \text{and} \quad y^2 = w(x^2+1)(x^4+sx^2+1).$$

(Recall from Lemma 2.5 that if $s = -6$ and -2 is not a square in K, the curve Z is isomorphic to its standard quadratic twist. However, when $s = -6$ we have $t = \pm 1 \pm \sqrt{2}$, so when the Weierstrass points of Z are rational, the exceptional case in Lemma 2.5 does not occur.)

In Table 3(A), we present some data that we collected by enumerating doubly isogenous pairs. For n ranging from 15 to 23, we considered the 1024 primes

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

TABLE 3. The total number of unordered pairs of doubly isogenous curves and $[1-\rho^*]$-isogenous curves over $\mathbb{F}_q$ for the 1024 primes $q \equiv 1 \bmod 4$ closest to 2^n, restricting to curves with all Weierstrass points rational

A Data for doubly isogenous curves

n	Examples
15	820
16	580
17	407
18	282
19	218
20	138
21	100
22	58
23	42

B Data for $[1-\rho^*]$-isogenous curves

n	Examples
15	11690160
16	23837994
17	48443688
18	97608276
19	196343212
20	394584130
21	793839836
22	1588282776
23	3172154548

$q \equiv 1 \bmod 4$ closest to 2^n and computed the sum of $\delta(q)$ over these values of q. According to Naïve Heuristic 5.3 and Lemma 5.4, we would expect this sum to have rate of growth of the form $c/2^n$ for some constant c. In particular, we would expect the sum to approximately halve as we increase n by 1. This is not what we observe. We explain this discrepancy in the next section by finding several families of coincidences that cause doubly isogenous pairs to occur more often than predicted.

We can similarly develop heuristics for covers corresponding to subgroups of $\mathrm{Jac}(Z)[2]$.

Definition 5.5. Let H be a subgroup of $\mathrm{Jac}(Z)[2]$. We say that Z_1 and Z_2 are *H-isogenous* if $\mathrm{Jac}(Z_1)$ and $\mathrm{Jac}(Z_2)$ are isogenous and $\mathrm{Jac}(\widetilde{Z}_1^H)$ and $\mathrm{Jac}(\widetilde{Z}_2^H)$ are isogenous, where $\widetilde{Z}_1^H$ and $\widetilde{Z}_2^H$ are as defined in Definition 3.2.

(When $H = 0$ we recover the definition of doubly isogenous curves.)

Proposition 3.6 gives a decomposition of $\mathrm{Jac}(\widetilde{Z}^H)$, and Table 1 lets us identify the elliptic curves appearing in this decomposition. In particular, if m is the number of different nonconstant orbits of elliptic curves corresponding to the 2-torsion points in $H^\perp$, then we expect

$$\#\{H\text{-isogenous pairs } /\mathbb{F}_q\} \asymp q^{(3-m)/2}. \tag{5.2}$$

Example 5.6. For example, take $H := \mathrm{Ker}(1-\rho^*)$, where ρ is the automorphism of order 4 defined in Section 2.1. The cover $\widetilde{Z}^H \to Z$ has degree four, and since $(1-\rho^*)^2 = -2\rho^*$, it is isomorphic to the pullback of the endomorphism $1-\rho^*$ on $\mathrm{Jac}(Z)$ via the embedding $Z \to \mathrm{Jac}(Z)$. When Z_1 and Z_2 are H-isogenous for this H, we say that Z_1 and Z_2 are *$[1-\rho^*]$-isogenous*. The Jacobian $\mathrm{Jac}(\widetilde{Z}^H)$ contains orbits 1 and 2C (in addition to E^2). Since Orbit 2C is constant, $m = 1$ and we only need a single coincidence for $\mathrm{Jac}(\widetilde{Z}_1^H)$ and $\mathrm{Jac}(\widetilde{Z}_2^H)$ to be isogenous. Thus we

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

expect

$$\#\{[1-\rho^*]\text{-isogenous pairs } /\mathbb{F}_q\} \asymp q. \tag{5.3}$$

We expect the total number of pairs of $[1-\rho^*]$-isogenous curves for the 1024 primes $q \equiv 1 \bmod 4$ closest to 2^n to have rate of growth $c \cdot 2^n$ for some constant c, and this is supported by the data in Table 3(B), as the number of pairs roughly doubles as we increase n by 1.

6. Families with unexpected coincidences

Naïve Heuristic 5.3 predicts that the "expected value" of $\delta(q)$ is on the order of $1/q$, where $\delta(q)$ is the number of nonconjugate pairs $\{Z_1, Z_2\}$ of doubly isogenous curves over a finite field $\mathbb{F}_q$ with Z_1 and Z_2 genus-2 curves with D_4-action and all Weierstrass points rational. As seen in Table 3(A), the data we collected does not seem to reflect this rate of growth. In this section, we find a number of families of coincidences that explain this discrepancy and we formulate a more sophisticated heuristic for the number of such pairs, which will be supported by the data in Section 7.

6.1. j-Invariants for orbits.

We begin by computing the j-invariants of the elliptic curves appearing in Table 1; the middle column of Table 4 gives these j-invariants in terms of the parameter t. For our computations, it will be convenient to note that we can also express these j-invariants in terms of the quantity

$$u := (1/2)(t - 1/t),$$

as is shown in the third column of Table 4. This new parametrization simplifies our computations in Section 6.2, because $I = (u + 1/u)^2$ is a quartic function of u instead of a degree-8 function of t. We omit the proofs of the following two facts.

Table 4. The j-invariants for the elliptic curves in Table 1 in terms of t and $u = \frac{1}{2}(t - 1/t)$

Orbit	j-invariant, in terms of the variable t	j-invariant, in terms of the variable u
1	$\dfrac{2^4(t^8+14t^4+1)^3}{(t^5-t)^4}$	$\dfrac{2^8(u^4+u^2+1)^3}{u^4(u^2+1)^2}$
2A	$\dfrac{-2^4(t^4-14t^2+1)^3}{t^2(t^2+1)^4}$	$\dfrac{-2^6(u^2-3)^3}{(u^2+1)^2}$
2B	$\dfrac{2^6(3t^4-10t^2+3)^3}{(t^2-1)^2(t^2+1)^4}$	$\dfrac{2^6(3u^2-1)^3}{(u^3+u)^2}$
2C	1728	1728
4A	$\dfrac{-2^6(t^4-2\zeta t^3-6t^2+2\zeta t+1)^3}{(t^3-t)^2(t-\zeta)^4}$	$\dfrac{-2^8(u^2-\zeta u-1)^3}{(u^2-\zeta u)^2}$
4B	$\dfrac{-2^6(t^4+2\zeta t^3-6t^2-2\zeta t+1)^3}{(t^3-t)^2(t+\zeta)^4}$	$\dfrac{-2^8(u^2+\zeta u-1)^3}{(u^2+\zeta u)^2}$

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Lemma 6.1. *Replacing u with $-u$, $1/u$, or $-1/u$ does not change the value of I.*

Lemma 6.2. *The elliptic curve E defined by Equation (2.4) has j-invariant*

$$\frac{2^8(t^4-t^2+1)^3}{t^4(t^2-1)^2} = \frac{2^6(4u^2+1)^3}{u^2},$$

and is isomorphic to $y^2 = dx(x-1)(x-\lambda)$, where $\lambda = t^2$ and $d = c(t^2+1)$.

6.2. **Finding generic geometric isogenies.** In this subsection, we work over an algebraically closed field K of characteristic not 2. Our goal is to find families of ordered pairs (Z_1, Z_2) of genus-2 curves over K with D_4-action that have a higher-than-expected chance of being doubly isogenous. For example, we might search for families where the elliptic curves in some of the orbits listed in Table 1 for Z_1 are automatically isogenous to those in some of the orbits for Z_2. We carry out this search by using classical modular polynomials $\Phi_n \in \mathbb{Z}[x,y]$. (Recall that the polynomial Φ_n has the property that there is a geometric cyclic n-isogeny between two elliptic curves over an arbitrary field K if and only if the j-invariants j_1 and j_2 of the two curves satisfy $\Phi_n(j_1,j_2) = 0$; see [7], [9].)

Let Z_1 and Z_2 be two genus-2 curves over K with D_4-action, and let I_1 and I_2 be their respective invariants; see Section 2.3. We can write each Z_i in the form (3.1); that is, there are $c_i, t_i \in K$ such that Z_i is given by

$$\begin{aligned} Z_i\colon \quad y^2 &= c_i(x-\zeta)(x+\zeta)(x-t_i)(x+t_i)(x-1/t_i)(x+1/t_i) \\ &= c_i(x^2+1)(x^4+s_ix^2+1), \end{aligned} \tag{6.1}$$

where $s_i = -(t_i^4+1)/t_i^2$. Since K is algebraically closed, we may take $c_1 = c_2 = 1$.

As we observed in Section 6.1, the orbit labels for Z_1 and Z_2 are determined by the values of $u_i = (1/2)(t_i - 1/t_i)$, which satisfy $I_i = (u_i + 1/u_i)^2$. It follows that u_1 and u_2 are reasonable parameters to use for the families we construct.

To find families of ordered pairs (Z_1, Z_2) with a cyclic isogeny of degree n between specified orbits, we work over the algebraic closure K of the 2-variable function field $\mathbb{Q}(\zeta)(u_1,u_2)$, and consider the curves Z_1 and Z_2 with parameters $t_1, t_2 \in K$ such that $u_i = (1/2)(t_i - 1/t_i)$. Given an orbit for Z_1 and an orbit for Z_2, we can plug the appropriate formulas for the j-invariants of the orbits into Φ_n in order to obtain an expression in u_1 and u_2 which is zero if and only if there is a cyclic n-isogeny between the curves in the given orbits.

Example 6.3. Let us calculate conditions under which the Orbit 1 elliptic curve for Z_1 is geometrically isomorphic to the Orbit 1 elliptic curve for Z_2. This calculation is simpler than most, because the j-invariants of the Orbit 1 elliptic curves can in fact be expressed directly in terms of the invariants of Z_1 and Z_2; namely, the Orbit 1 j-invariant for each curve is $256 \cdot (I_i - 1)^3/I_i$. We see that the two j-invariants are equal if and only if

$$(I_1-1)^3 I_2 - (I_2-1)^3 I_1 = 0.$$

The expression on the left-hand side factors as the product of $I_1^2I_2 + I_1I_2^2 - 3I_1I_2 + 1$ and $I_1 - I_2$.

We compute that the condition $I_1^2I_2 + I_1I_2^2 - 3I_1I_2 + 1 = 0$ is equivalent to

$$(u_1^2+u_2^2+1)(u_1^2u_2^2+u_1^2+1)(u_1^2u_2^2+u_2^2+1)(u_1^2u_2^2+u_1^2+u_2^2) = 0.$$

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Example 6.4. Let us consider the relation between u_1 and u_2 that is satisfied exactly when the elliptic curves in Orbit 2A of Z_1 are 2-isogenous to the elliptic curves in Orbit 2B of Z_2. We will not write down the full polynomial relation in u_1 and u_2 because it involves 94 terms. We do observe that it factors over $\mathbb{Q}(\zeta)$ into nine irreducible polynomials; one of these irreducible factors is $u_1^2u_2^2+u_1^2+1$, which also appears in Example 6.3! Thus, if the single relation $u_1^2u_2^2 + u_1^2 + 1 = 0$ holds, the Orbit 1 curve for Z_1 is isomorphic to the Orbit 1 curve for Z_2, *and* the Orbit 2A curve for Z_1 is 2-isogenous to the Orbit 2B curve for Z_2. This is an unexpected coincidence!

In the following subsection we report on what we found by systematically searching for such coincidences. The ideal but computationally intensive calculation would be to work over K and consider every pair (F_1, F_2) of elliptic curves, where each F_i is either the quotient of Z_i given by (2.4) or one of the curves in an orbit for Z_i. For each positive integer n in some a predetermined set of values (see Remark 6.5 for our choice), we would compute an expression in u_1 and u_2 that equals zero if and only if there is a cyclic n-isogeny between the curves in the two orbits. Then, for every pair of such expressions, we would compute their greatest common divisor. Whenever this greatest common divisor was not 1, we would find a family of pairs (Z_1, Z_2) of curves associated to a pair of parameters (u_1, u_2) where there are multiple isogenies between the elliptic factors of $\mathrm{Jac}(\widetilde{Z}_1)$ and those of $\mathrm{Jac}(\widetilde{Z}_2)$.

It is computationally difficult to implement the above strategy because when we substitute the rational functions for the j-invariants into all but the smallest modular polynomials, the expressions become quite large. To reduce the size of the coefficients in the expressions, and to reduce the number of monomials involved, we instead work modulo a prime $p \equiv 3 \bmod 4$ and specialize u_1 to a value in $\mathbb{F}_p(\zeta)$. This yields rational functions in $\mathbb{F}_p(\zeta)(u_2)$ which fit much more easily in memory. We are therefore looking for cyclic n-isogenies between fibers (over u_2) of the family Z_2 and a fixed fiber of Z_1, after reducing modulo p.

There are two risks associated to making these reductions. The first is that we may find spurious relations, nonzero greatest common divisors that occur only modulo p. As it happens, none of the relations we found involved modular polynomials of high degree, so we were subsequently able to verify the relations we found over the full ring $\mathbb{Q}(\zeta)(u_1, u_2)$.

The second risk is that we might miss a family. This could happen, for example, if there is a relation that involves a polynomial in $\mathbb{Q}(\zeta)(u_1, u_2)$ that reduces modulo p to a constant, or to a polynomial like u_1u_2 whose solutions require one of the u_i to be equal to one of the forbidden values 0 or ζ. It could also happen if we specialize to a value of u_1 that makes the polynomial constant. Without knowing more about the geometry of the possible families in characteristic zero, we are not sure how to rule out these possibilities. We did, however, run our computation several times, with different choices for the prime p and different choices for the values of u_1, and the results did not vary. Thus, we believe we found all of the families of coincidences involving isogenies of the degrees we considered. As we will see in Section 7, we have found enough families to formulate an improved heuristic that is supported by our data.

Remark 6.5. We are left to specify the degrees n of the cyclic isogenies we will consider. We choose to look for cyclic n-isogenies for all values of n for which the modular curve $X_0(n)$ has genus 0 (namely, $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18,$

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

and 25) or genus 1 (namely, $n = 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36$, and 49). We chose these values so that we would find all families of coincidences given by a relation between u_1 and u_2 that defines a curve of geometric genus at most 1. To see that these values of n will lead to all such families, note that every family we find gives us a varying pair of elliptic curves connected by a cyclic n-isogeny, and so comes provided with a nonconstant map to $X_0(n)$. Since no family of genus 0 or 1 can map to a modular curve with genus larger than 1, for our goal of finding all families defined by genus-0 and genus-1 relations between u_1 and u_2, it will suffice for us to consider the values of n specified above.

In the end, we found sixteen families of coincidences in terms of u_1 and u_2. However, if we count two families as being equivalent if they produce the same pairs (Z_1, Z_2) — that is, if one family can be obtained from the other by applying transformations from Lemma 6.1 to u_1 and u_2 — then we have only four equivalence classes of families. We describe these four classes of families in the following section, where we keep close track of fields of definition of isogenies.

Remark 6.6. A family given by a relation between u_1 and u_2 can be made more explicit by replacing each u_i with $(1/2)(t_i - 1/t_i)$, and then looking at an irreducible factor of the resulting expression. For example, the relation between t_1 and t_2 obtained from the relation $u_1^2 + u_2^2 + 1 = 0$ from Example 6.3 has degree 6, but it factors into two factors of degree 1 and two factors of degree 2. One of the factors is $t_2 - \zeta t_1$. See Section 6.3.1.

6.3. **Description of the families.**

6.3.1. *The first family.* Let K be a field of characteristic not 2 that contains a primitive 4th root of unity ζ. For $i = 1, 2$, let c_i and t_i be elements of $K^\times$ with $t_i^4 \neq 1$, let Z_i be given by (6.1), and let E_i be the quotient curve

$$E_i\colon \quad y^2 = c_i(x+1)(x - t_i^2)(x - 1/t_i^2). \tag{6.2}$$

Lemma 6.7. *Suppose $t_2 = \zeta t_1$, and suppose $(t_1^2 + 1)(t_2^2 + 1)$ and $c_1 c_2$ are squares in K. Then over K the following statements hold*:

1. *the elliptic curve in Orbit 1 for Z_1 is isomorphic to the elliptic curve in Orbit 1 for Z_2*;
2. *the elliptic curves in Orbit 2B for Z_1 and the elliptic curves in Orbit 2B for Z_2 are related by a degree-2 isogeny*;
3. *the elliptic curves in Orbit 2C for Z_1 are isomorphic to those in Orbit 2C for Z_2*;
4. *the elliptic curve E_1 (resp. E_2) and the elliptic curves in Orbit 2A for Z_2 (resp. Z_1) are related by a degree-2 isogeny.*

Furthermore, if K is the algebraic closure of the function field $\mathbb{Q}(t)$ and $t_1 = t$, then there are no other isogenies among the orbits associated to Z_1 and Z_2.

Lemma 6.7 could also be rephrased in terms of Prym varieties using Proposition 3.11.

Proof of Lemma 6.7. To avoid a proliferation of subscripts and to aid in visual comprehension of various formulas, in this proof we will write t and c for t_1 and c_1, and we will write T and C for t_2 and c_2. More generally, we will use lower case letters for variables associated with Z_1, and upper case letters for variables associated with Z_2.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Since the isomorphism classes of the curves Z_i and the elliptic curves E_i only depend on the values of c and C up to squares, and since cC is a square by hypothesis, we may assume that $C = c$.

By Table 1, the Orbit 1 curves for Z_1 and Z_2 can be written as

$$y^2 = x(x-1)(x-\lambda) \quad \text{and} \quad Y^2 = X(X-1)(X-\Lambda),$$

respectively, where $\lambda = 4t^2/(t^2+1)^2$ and $\Lambda = 4T^2/(T^2+1)^2 = -4t^2/(t^2-1)^2$. Then an isomorphism between the curves is given by

$$X = (x-\lambda)/(1-\lambda) \quad \text{and} \quad Y = y \cdot (t^2+1)^3/(t^2-1)^3.$$

This proves the first statement.

The Orbit 2B curves for Z_1 and Z_2 can be written as

$$y^2 = c(t^2+1) \cdot x(x-1)(x-\lambda) \quad \text{and} \quad Y^2 = c(T^2+1) \cdot X(X-1)(X-\Lambda),$$

respectively, where

$$\lambda = \frac{2(t^2-1)}{(t+\zeta)^2} \quad \text{and} \quad \Lambda = \frac{2(T^2-1)}{(T+\zeta)^2} = \frac{2(t^2+1)}{(t+1)^2}.$$

Then a degree-2 isogeny from the first curve to the second is given by

$$X = \frac{\zeta}{2(t+1)^2} \cdot \frac{((t+\zeta)x - (1+\zeta)(t+1))^2}{x-1},$$
$$Y = y \cdot \frac{(t+\zeta)(\zeta-1)}{4(t+1)^3} \cdot \frac{(t+\zeta)^2x^2 - 2(t+\zeta)^2x + (2t^2-2)}{(x-1)^2}.$$

This proves the second statement.

The Orbit 2C curves for Z_1 and Z_2 are both twists of $y^2 = x^3 - x$, by $c(t^2+1)$ and by $c(T^2+1)$, respectively. By hypothesis, $(t^2+1)(T^2+1)$ is a square in K, so these two twists are isomorphic to one another. This proves the third statement.

By Lemma 6.2 and Table 1, we can write E_1 and the Orbit 2A curve for Z_2 as

$$y^2 = c(t^2+1) \cdot x(x-1)(x-\lambda) \quad \text{and} \quad Y^2 = c(T^2+1) \cdot X(X-1)(X-\Lambda),$$

respectively, where $\lambda = t^2$ and $\Lambda = 4\zeta T/(T+\zeta)^2 = 4t/(t+1)^2$. Then a degree-2 isogeny from the first curve to the second is given by

$$X = \frac{1}{(t+1)^2} \cdot \frac{(x+t)^2}{x} \quad \text{and} \quad Y = y \cdot \frac{1}{(t+1)^3} \cdot \frac{x^2-t^2}{x^2}.$$

This proves one case of the fourth statement. The proof of the other case is similar.

Finally, we check that no other pairs of elliptic curves associated to Z_1 and Z_2 are isogenous to one another when K is the algebraic closure of $\mathbb{Q}(t)$ and $t_1 = t$. As we noted earlier, two elliptic curves over a field are connected by a cyclic n-isogeny over the algebraic closure if and only if their j-invariants satisfy the n-th classical modular polynomial $\Phi_n \in \mathbb{Z}[x,y]$. If this relation holds in K, then it will also hold when we reduce modulo p and specialize t and c to specific values for which the resulting curves are nonsingular. We take $p = 421$, $\zeta = 29 \in \mathbb{F}_p$, $t = 19 \in \mathbb{F}_p$, and $c = 1 \in \mathbb{F}_p$. Computing traces shows the elliptic curves in question are all ordinary. It follows that any geometric isogeny between them is defined already over $\mathbb{F}_{p^{12}}$; see [6, §5, p. 251]. Thus we simply compute the traces of these elliptic curves over $\mathbb{F}_{p^{12}}$ and observe that there are no further matches. □

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

We noted in Section 5.2 that replacing t_1 with any of eight linear fractional expressions in t_1 will result in a curve isomorphic to Z_1, but possibly with the labels on Orbits 2A and 2B swapped, and similarly for Orbits 4A and 4B. If we take the relation $t_2 = \zeta t_1$ and apply one of these transformations to t_1 and a possibly different one to t_2, we will get another family of curves satisfying the conclusions of Lemma 6.7, possibly with the roles of various orbits swapped. There are 64 ways of applying these eight linear fractional transformations separately to t_1 and t_2, but some of these will produce equivalent relations; for example, replacing t_1 with $-t_1$ and t_2 with $-t_2$ fixes the relation $t_2 = \zeta t_1$. In fact, we obtain only 16 different families in this way. When we multiply the 16 corresponding relations together, we get a relation that can be expressed in terms of I_1 and I_2, namely:

$$I_1^2 I_2 + I_1 I_2^2 - 3 I_1 I_2 + 1 = 0. \tag{6.3}$$

Definition 6.8. We say that two curves Z_1 and Z_2 with D_4-action are *in the first family* if their invariants satisfy (6.3).

Remark 6.9. Equation (6.3) defines a genus-0 curve, which can be parametrized as

$$I_1 = \frac{-(1+z)^2}{2(1-z)}, \quad I_2 = \frac{-(1-z)^2}{2(1+z)}.$$

Under this parametrization, the involution swapping I_1 and I_2 corresponds to $z \leftrightarrow -z$.

Proposition 3.11 shows that each of the elliptic curves that appears in Table 1 as an isogeny factor of $\widetilde{Z}_i$ can also be viewed as a Prym variety Prym^H for a double cover of Z_i specified by an index-2 subgroup H of $\mathrm{Jac}(Z_i)[2]$, and each such subgroup H is determined as the set of elements of $\mathrm{Jac}(Z_i)[2]$ that pair trivially with a nonzero element $U \in \mathrm{Jac}(Z_i)[2]$. Lemma 6.7 could therefore be restated in terms of these Pryms. The labeling of these Pryms via the elements U has the same problem as the labeling of the orbits associated to the Z_i: The labels depend on which of the eight possible values of t_i we used to write down an equation for Z_i. However, using Prym varieties we can state a variant of Lemma 6.7 whose hypotheses and conclusions depend only on the isomorphism classes of the curves Z_i and not on the choices we made to write them down.

Notation 6.10. Let Z be a genus-2 curve with D_4-action over a field K of characteristic not 2. As we see from Table 1, there is a unique nonzero point U of $\mathrm{Jac}(Z)[2](\bar{K})$ that is fixed by the action of D_4. Let H be the order-2 subgroup of $\mathrm{Jac}(Z)[2]$ generated by U. In the notation of Definition 3.2, let $\widehat{Z} = \widetilde{Z}^H$, so that there is a degree-8 cover $\widehat{Z} \to Z$ and $\widehat{Z}$ has genus 9.

Proposition 6.11. *Let Z_1 and Z_2 be curves with D_4-action over a field K of characteristic not 2, and suppose Z_1 and Z_2 lie in the first family. If $\mathrm{Jac}(Z_1)$ and $\mathrm{Jac}(Z_2)$ are geometrically isogenous to one another, then $\mathrm{Jac}(\widehat{Z}_1)$ and $\mathrm{Jac}(\widehat{Z}_2)$ are geometrically isogenous to one another.*

Proof. We may assume that K is algebraically closed. Let ζ be a primitive fourth root of unity in K. Since Z_1 and Z_2 are in the first family and since K is algebraically closed, we can choose values of t_1 and t_2 with $t_2 = \zeta t_1$ such that each Z_i has a model as in (3.1) with $t = t_i$ and with $c = 1$. The hypotheses of Lemma 6.7 are then satisfied.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Since $\mathrm{Jac}(Z_1)$ and $\mathrm{Jac}(Z_2)$ are isogenous to one another and since $\mathrm{Jac}(Z_i) \sim E_i^2$ for each i, the elliptic curves E_1 and E_2 are isogenous to one another. Lemma 6.7 then shows that the Orbit 1 curves for Z_1 and Z_2 are isogenous to one another, as are the Orbit 2A curves, the Orbit 2B curves, and the Orbit 2C curves.

Proposition 3.6 shows that $\mathrm{Jac}(\widehat{Z}_i)$ decomposes up to isogeny as the product of E_i^2 with the product of the $\mathrm{Prym}^{H'}$, where H' ranges over the index-2 subgroups of $\mathrm{Jac}(Z_i)[2]$ that contain the subgroup $H = \langle U \rangle$, where $U = [W_\zeta - W_{-\zeta}]$. Taking duals with respect to the Weil pairing, we see that the H' are the index-2 subgroups such that $(H')^\perp \subseteq H^\perp$. This means that the $(H')^\perp$ are precisely the subgroups $\langle U' \rangle$, where U' is a nontrivial 2-torsion point that pairs trivially with U. We see from Lemma 3.10 and Table 1 that these U' are the labels of Orbits 1, 2A, 2B, and 2C, so each $\mathrm{Jac}(\widehat{Z}_i)$ is isogenous to E_i^2 times the product of the elliptic curves in Orbits 1, 2A, 2B, and 2C. Therefore, the $\mathrm{Jac}(\widehat{Z}_i)$ are isogenous to one another. □

Proposition 6.12. *Let Z_1 and Z_2 be curves with D_4-action given as in* (6.1) *by values of t_i and c_i such that $t_2 = \zeta t_1$ and such that $c_1 c_2$ and $(t_1^2+1)(t_2^2+1)$ are both squares. For $i = 1, 2$, let E_i be the elliptic curve given by* (6.2)*. Suppose that E_1 and E_2 are isogenous to one another, and that either of the following two conditions holds*:

(1) *The curve $y^2 = \zeta x(x-1)(x + 2\zeta t_1/(t_1-\zeta)^2)$ is isogenous to either*

$$y^2 = \zeta x(x-1)(x + 2\zeta t_2/(t_2-\zeta)^2) \quad \text{or}$$
$$y^2 = \zeta c_2(t_2^2+1) \cdot x(x-1)(x + 2\zeta t_2/(t_2-\zeta)^2),$$

and the curve $y^2 = \zeta x(x-1)(x - 2\zeta t_1/(t_1+\zeta)^2)$ is isogenous to either

$$y^2 = \zeta x(x-1)(x - 2\zeta t_2/(t_2+\zeta)^2) \quad \text{or}$$
$$y^2 = \zeta c_2(t_2^2+1) \cdot x(x-1)(x - 2\zeta t_2/(t_2+\zeta)^2).$$

(2) *The curve $y^2 = \zeta x(x-1)(x + 2\zeta t_1/(t_1-\zeta)^2)$ is isogenous to either*

$$y^2 = \zeta x(x-1)(x - 2\zeta t_2/(t_2+\zeta)^2) \quad \text{or}$$
$$y^2 = \zeta c_2(t_2^2+1) \cdot x(x-1)(x - 2\zeta t_2/(t_2+\zeta)^2),$$

and the curve $y^2 = \zeta x(x-1)(x - 2\zeta t_1/(t_1+\zeta)^2)$ is isogenous to either

$$y^2 = \zeta x(x-1)(x + 2\zeta t_2/(t_2-\zeta)^2) \quad \text{or}$$
$$y^2 = \zeta c_2(t_2^2+1) \cdot x(x-1)(x + 2\zeta t_2/(t_2-\zeta)^2).$$

Then Z_1 and Z_2 are doubly isogenous.

Proof. Since $\mathrm{Jac}(Z_i) \sim E_i^2$, the assumption that $E_1 \sim E_2$ implies that $\mathrm{Jac}(Z_1) \sim \mathrm{Jac}(Z_2)$. By Lemma 6.7, the elliptic curves in Orbit 1 for Z_1 are isogenous to those in Orbit 1 for Z_2, and similarly for Orbits 2A and 2B. The Orbit 2C curves for Z_1 and Z_2 are isomorphic, because each curve is the twist of $y^2 = x^3 - x$ determined by $c_i(t_i^2+1)$, and the product of these two factors is a square. Therefore, in order for Z_1 and Z_2 to be doubly isogenous, it suffices that the elliptic curves in Orbits 4A and 4B for Z_1 are, in some order, isogenous to the Orbit 4A and 4B curves for Z_2. This is equivalent to conditions (1) and (2). □

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

6.3.2. *The second family.* In Table 1, the four elliptic curves in Orbit 4A are not necessarily isomorphic to one another over the base field, because there are two possible values for the factor d that determines the twist of the curve. We will refer to the first two curves (with $d = \zeta$) as the "first pair" of Orbit 4A, and the last two curves (with $d = \zeta c(t^2+1)$) as the "second pair." Likewise, we refer to the $d = \zeta$ curves in Orbit 4B as the first pair of that orbit, and the $d = \zeta c(t^2+1)$ curves as the second pair of that orbit.

As in the preceding subsection, for $i = 1$ and $i = 2$ we let Z_i and E_i be the curves given by (6.1) and (6.2). We will consider the following relation between t_1 and t_2:

$$(t_1 - \zeta)^2(t_2 - \zeta)^2 = -8t_1t_2. \tag{6.4}$$

Lemma 6.13. *Suppose* (6.4) *holds. Then*:

(1) *the elliptic curve in Orbit 1 for Z_1 and the elliptic curve in Orbit 1 for Z_2 are related by a degree-2 isogeny over K*;
(2) *if $c_1c_2(t_1^2+1)(t_2^2+1) \in K^{\times 2}$, then the elliptic curves in Orbit 2C for Z_1 are isomorphic over K to the elliptic curves in Orbit 2C for Z_2*;
(3) *if $c_1t_1(t_1^2+1) \in K^{\times 2}$, then the elliptic curves in Orbit 2A for Z_1 are isomorphic over K to the first pair of elliptic curve in Orbit 4A of Z_2, and the elliptic curves in Orbit 2B for Z_1 are isomorphic over K to the first pair of elliptic curves in Orbit 4B of Z_2*;
(4) *if $c_1c_2t_1(t_1^2+1)(t_2^2+1) \in K^{\times 2}$, then the elliptic curves in Orbit 2A for Z_1 are isomorphic over K to the second pair of elliptic curve in Orbit 4A of Z_2, and the elliptic curves in Orbit 2B for Z_1 are isomorphic over K to the second pair of elliptic curves in Orbit 4B of Z_2*;
(5) *the statements obtained from* (3) *and* (4) *by interchanging the roles of Z_1 and Z_2 also hold.*

Furthermore, if K is the algebraic closure of the function field $\mathbb{Q}(t)$ and $t_1 = t$, then there are no other isogenies among the orbits associated to Z_1 and Z_2.

Proof. We leave the proof to the reader, because it is essentially the same as the proof of Lemma 6.7 and is mostly straightforward. The only nonobvious details involved in the proof of the numbered statements are that if $t_1, t_2 \in K$ satisfy (6.4), then $\zeta t_1 t_2$ and $t_1(t_1^2-1)$ and $t_2(t_2^2-1)$ are all squares in K. The first of these is a square because of (6.4) and the fact that $-8\zeta = (2-2\zeta)^2$; the second is a square because (6.4) can be rewritten as

$$t_1(t_1^2-1) = (1+\zeta)^2 t_1^2 (t_2+\zeta)^2/(t_2-\zeta)^2;$$

and the third is a square by symmetry.

The final statement can be proven by taking $p = 421$, $\zeta = 29 \in \mathbb{F}_p$, $t_1 = 19 \in \mathbb{F}_p$, $t_2 = 204 \in \mathbb{F}_p$, and $c_1 = c_2 = 1 \in \mathbb{F}_p$, and comparing traces over $\mathbb{F}_{p^{12}}$ as in the end of the proof of Lemma 6.7. □

Proposition 6.14. *Let Z_1 and Z_2 be curves with D_4-action given as in* (6.1) *by values of t_i that satisfy* (6.4) *and with $c_i = \zeta(t_i^2+1)$, and such that t_2 and ζt_1 are squares in $K^\times$. For $i = 1, 2$, let E_i be the elliptic curve given by* (6.2). *Suppose that*:

(1) *E_1 and E_2 are isogenous to one another*;

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

(2) *the first pair of curves in Orbit 4A of Z_1 are isogenous to the second pair of curves in Orbit 4A for Z_2; and*
(3) *the first pair of curves in Orbit 4B of Z_1 are isogenous to the second pair of curves in Orbit 4A for Z_2.*

Then Z_1 and Z_2 are doubly isogenous.

Remark 6.15. Proposition 6.14 follows from making choices that allow us to apply certain statements from Lemma 6.13; in particular, we make choices that imply that $c_1t_1(t_1^2+1)$ and $c_1c_2t_2(t_1^2+1)(t_2^2+1)$ are squares. Other choices would lead to variations of Proposition 6.14.

Proof of Proposition 6.14. From Lemma 6.13(1), the curves in Orbit 1 for Z_1 and Z_2 are isogenous to one another. From Lemma 6.13(3), the curves in Orbits 2A and 2B for Z_1 are isogenous to the first pairs of Orbits 4A and 4B for Z_2, respectively, and from Lemma 6.13(5) applied to (4), the curves in Orbits 2A and 2B for Z_2 are isogenous to the second pairs of Orbits 4A and 4B for Z_1, respectively.

Since $\zeta c_1(t_1^2+1)$ and $\zeta c_2(t_2^2+1)$ are both squares, $c_1(t_1^2+1)$ and $c_2(t_2^2+1)$ are in the same square class in $K^\times$. Since the first pair and second pair of Orbit 4A for Z_i are twists of one another by $c_i(t_i^2+1)$, the hypothesis (2) of the proposition implies that the second pair of curves in Orbit 4A of Z_1 is isogenous to the first pair of curves in Orbit 4A of Z_2. Thus, by the preceding paragraph, the curves in Orbit 2A for Z_1 are isogenous to the curves in Orbit 2A for Z_2. Similarly, the first pair and second pair of Orbit 4B for Z_i are twists of one another by $c_i(t_i^2+1)$ and the same argument shows that the curves in Orbit 2B for Z_1 are isogenous to the curves in Orbit 2B for Z_2.

Again as $c_1(t_1^2+1)$ and $c_2(t_2^2+1)$ are in the same square class in $K^\times$, Lemma 6.13(2) implies that the curves in Orbit 2C for Z_1 are isomorphic to the curves in Orbit 2C for Z_2. As $E_1 \sim E_2$, we conclude that Z_1 and Z_2 are doubly isogenous. □

As in the preceding subsection, we can apply any of eight linear fractional transformations to t_1 and to t_2 in the relation given by (6.4) to get another family that satisfies a lemma similar to Lemma 6.13. Only four of these families are distinct. Multiplying the polynomials defining these four families together, we find a relation that can be expressed in terms of the invariants I_1 and I_2 of Z_2 and Z_2:

$$I_1I_2 = 16. \tag{6.5}$$

Definition 6.16. We say that two curves Z_1 and Z_2 with D_4-action are *in the second family* if their invariants satisfy (6.5).

Remark 6.17. Equation (6.5) defines a genus-0 curve, which can be parametrized as

$$I_1 = \frac{4(1-z)}{1+z}, \quad I_2 = \frac{4(1+z)}{1-z}.$$

Under this parametrization, the involution swapping I_1 and I_2 corresponds to $z \leftrightarrow -z$.

Remark 6.18. Proposition 6.11 gives an interpretation of the first family that can be stated in terms of the isomorphism classes of the curves, without reference to the choices of t_1 and t_2 that we make to write down the curves; this is possible because the orbits involved in Lemma 6.7 are exactly the orbits contained in the Prym variety of a cover that can be defined independently of the choices of t_i. There is no straightforward analog of Proposition 6.11 for the second family.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

6.3.3. *The third and fourth families.* We found two further families of pairs of curves where there are more isogenies between the associated elliptic curves than expected. They produce fewer doubly isogenous curves than the preceding two families, so here we just summarize the results. We also simplify the exposition by assuming in this section that the base field K is algebraically closed, so that we do not have to worry about twists.

Let Z_1 and Z_2 be genus-2 curves with D_4-action and with invariants I_1 and I_2. We say that Z_1 and Z_2 are *in the third family* if we have

$$I_1^2 I_2^2 - 3 \cdot 2^8 I_1 I_2 + 2^{12} I_1 + 2^{12} I_2 = 0. \tag{6.6}$$

If Z_1 and Z_2 are in the third family, then

- the curves in Orbit 1 for Z_1 and Z_2 are 4-isogenous to one another;
- the curves in either Orbit 4A or Orbit 4B for Z_1 are 2-isogenous to the curves in either Orbit 4A or Orbit 4B for Z_2.

Note that (6.6) defines a curve of genus 0, which can be parametrized by

$$I_1 = -32z(z+1)/(z-1)^2, \quad I_2 = -32z(z-1)/(z+1)^2.$$

Under this parametrization, the involution swapping I_1 and I_2 corresponds to $z \leftrightarrow -z$.

We say that Z_1 and Z_2 are *in the fourth family* if their invariants satisfy

$$(I_2^2 + 2^4 I_1^2 I_2 - 3 \cdot 2^4 I_1 I_2 + 2^8 I_1)(I_1^2 + 2^4 I_1 I_2^2 - 3 \cdot 2^4 I_1 I_2 + 2^8 I_2) = 0. \tag{6.7}$$

Suppose I_1 and I_2 satisfy the first factor in this expression. Then

- the curves in Orbit 1 for Z_1 and Z_2 are 2-isogenous to one another;
- one of the following holds:
  - the curve E_1 is isomorphic to the Orbit 4A curves for Z_2 and the Orbit 2A curves for Z_1 are 2-isogenous to the Orbit 4B curves for Z_2;
  - the curve E_1 is isomorphic to the Orbit 4B curves for Z_2 and the Orbit 2A curves for Z_1 are 2-isogenous to the Orbit 4A curves for Z_2;
  - the curve E_1 is 2-isogenous to the Orbit 4A curves for Z_2 and the Orbit 2B curves for Z_1 are 2-isogenous to the Orbit 4B curves for Z_2;
  - the curve E_1 is 2-isogenous to the Orbit 4B curves for Z_2 and the Orbit 2B curves for Z_1 are 2-isogenous to the Orbit 4A curves for Z_2.

If I_1 and I_2 satisfy the second factor in (6.7), then the roles of Z_1 and Z_2 in the above list are reversed. Each factor in (6.7) defines a curve of genus 0.

6.4. **Intersections of families.** Under mild restrictions on the field K, we will produce genus-2 curves Z_1 and Z_2 with D_4-action that are very close to being doubly isogenous. The invariants I_1 and I_2 of these curves are the two roots of $x^2 - (47/16)x + 16$. Since $I_1 I_2 = 16$, this pair of curves lies in the second family; since

$$I_1^2 I_2 + I_1 I_2^2 - 3 I_1 I_2 + 1 = 16(I_1 + I_2) - 47 = 0,$$

the pair also lies in the first family; and since

$$I_1^2 I_2^2 - 3 \cdot 2^8 I_1 I_2 + 2^{12} I_1 + 2^{12} I_2 = 16^2 - 3 \cdot 2^8 \cdot 16 + 2^{12}(47/16) = 0,$$

the pair lies in the third family as well.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Proposition 6.19. *Let K be a field in which -1, 2, and -7 are nonzero squares, and let $\zeta \in K$ satisfy $\zeta^2 = -1$. In K, let*

$$t_1 = \frac{(1+\zeta)(3+\zeta\sqrt{-7})}{2} \quad \text{and} \quad t_2 = \frac{(-1+\zeta)(3+\zeta\sqrt{-7})}{2}.$$

For $i = 1, 2$, let $c_i = 1$, and let Z_i and E_i be defined by (6.1) and (6.2). Then the invariants of Z_1 and Z_2 are the two roots of $x^2 - (47/16)x + 16$, and if E_1 is isogenous to E_2, the curves Z_1 and Z_2 are doubly isogenous.

Proof. An easy computation verifies the statement about the invariants of Z_1 and Z_2.

We check that $t_2 = \zeta t_1$ and that $(t_1^2 + 1)(t_2^2 + 1)$ is equal to the square of $\sqrt{2}^3(3 + \zeta\sqrt{-7})$. Since $c_1 c_2 = 1$ is also a square, the hypotheses of Lemma 6.7 are satisfied.

We also check that (6.5) holds, and that

$$c_1 t_1 (t_1^2 + 1) = \sqrt{2}^{-2}(2 + 5\zeta - 2\sqrt{-7} + \zeta\sqrt{-7})^2 \quad \text{and}$$
$$c_2 t_2 (t_2^2 + 1) = \sqrt{2}^{-2}(5 + 2\zeta - \sqrt{-7} + 2\zeta\sqrt{-7})^2.$$

As we already noted, $(t_1^2 + 1)(t_2^2 + 1)$ is a square, so the hypotheses of statements (1), (2), and (3) of Lemma 6.13 hold, as does the hypothesis of the variation of the lemma's statement (3) obtained by interchanging the roles of Z_1 and Z_2.

Finally, we note that the first pair and the second pair of Orbit 4A for Z_1 are twists of one another by $c_1(t_1^2 + 1)$, while the first pair and the second pair of Orbit 4A for Z_2 are twists of one another by $c_2(t_2^2 + 1)$; these two twisting factors lie in the same square class in $K^\times$. The analogous statement holds for the first and second pairs of Orbit 4B for Z_1 and for Z_2.

Combining the conclusions of Lemma 6.7 and Lemma 6.13 with this last observation, it is straightforward to verify that Z_1 and Z_2 are doubly isogenous. □

Remark 6.20. It is easy to check that the only pair (I_1, I_2) of nonzero elements of K that satisfies (6.3) and (6.5) is the pair from Proposition 6.19. This pair is also the only pair to satisfy both (6.5) and (6.6). There are other pairs that satisfy the defining equations of more than one of the four families, but in characteristic 0 the curves with those invariants do not have as many isogeny factors in common as the curves in Proposition 6.19.

Remark 6.21. As we noted in Remark 4.11, if two curves over a finite field are Galois conjugates of one another, they are necessarily doubly isogenous. We check that the values of s_i (see Equation (3.2)) for the two curves in Proposition 6.19 are $s_1 = 6\sqrt{-7}$ and $s_2 = -6\sqrt{-7}$. Thus, if K is finite and -7 is not a square in its prime field, the curves in the proposition are automatically doubly isogenous for an unsurprising reason.

Example 6.22. In $K = \mathbb{F}_{113}$, take $\zeta = 15$ and $\sqrt{-7} = 28$, and apply Proposition 6.19. We find that $t_1 = 107$ and $t_2 = 23$, that $s_1 = 55$ and $s_2 = 58$, and that the elliptic curves E_1 and E_2 both have trace 6, so that $E_1 \sim E_2$. This gives an example where the curves in Proposition 6.19 are not Galois conjugates of one another, but are doubly isogenous.

Remark 6.23. Let E_1 be the elliptic curve $y^2 = (x+1)(x^2 + 6\sqrt{-7}x + 1)$ over the field $K = \mathbb{Q}(\sqrt{-7})$ and let E_2 be its conjugate over $\mathbb{Q}$. If $\mathfrak{p}$ is a prime of K such

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

that the reductions of E_1 and E_2 modulo $\mathfrak{p}$ are isogenous, then over an extension of the residue field of $\mathfrak{p}$, the two curves $y^2 = (x^2+1)(x^4 \pm 6\sqrt{-7}x^2+1)$ will be doubly isogenous. By [3, Theorem 1.1], there are infinitely many such primes. However, the two curves we obtain from such a prime will be conjugate to one another — and hence, will give an uninteresting example — exactly when $\mathfrak{p}$ is a prime of degree 2.

This leads to the following question: Are there infinitely many degree-1 primes $\mathfrak{p}$ of $\mathbb{Q}(\sqrt{-7})$ such that the reductions of E_1 and E_2 modulo $\mathfrak{p}$ are isogenous? We suspect that the answer is yes, because if $\mathfrak{p}$ lies over p then heuristically there is roughly one chance out of $\sqrt{p}$ that they will be isogenous by chance, and the sum of $1/\sqrt{p}$ diverges. Unfortunately, we do not know how to prove that there are infinitely many such primes.

7. Heuristics for the families of coincidences

In the preceding section, we identified four families of pairs (Z_1, Z_2) of genus-2 curves with D_4-action where there are unexpected isogenies among a number of the elliptic curves that appear in the decomposition (up to isogeny) of the Jacobians $\mathrm{Jac}(\widetilde{Z}_1)$ and $\mathrm{Jac}(\widetilde{Z}_2)$. In this section, we formulate heuristics for the expected number of doubly isogenous pairs over a finite field that occur in these families.

7.1. **Counting doubly isogenous pairs in families.**

First, we introduce notation to keep track of the number of doubly isogenous pairs in each family; see also Definition 5.2.

Definition 7.1. We consider unordered pairs $\{Z_1, Z_2\}$ of doubly isogenous curves over $\mathbb{F}_q$, where Z_1 and Z_2 are genus-2 curves with D_4-action and all Weierstrass points rational, and where Z_1 and Z_2 are not Galois conjugates of one another. For $n = 1, 2, 3, 4$, let $\delta_n(q)$ be the number of these pairs $\{Z_1, Z_2\}$ that lie in the nth family. Let $\delta_0(q)$ be the number of these pairs $\{Z_1, Z_2\}$ that do *not* lie in any of these four families. Let $\delta_{1,2,3}(q)$ be the number of these pairs $\{Z_1, Z_2\}$ that are simultaneously in families 1, 2, and 3 — that is, the pairs whose invariants are the two roots of $x^2 - (47/16)x + 16$.

Remark 7.2. For $n > 0$, each $\delta_n(q)$ counts doubly isogenous pairs whose invariants satisfy one of the four equations (6.3), (6.5), (6.6), or (6.7). We do not demand that the doubly isogenous curves come from values of t that are related to one another as in, for example, Lemma 6.7 or Lemma 6.13.

We saw in Section 5 that Naïve Heuristic 5.3 did not seem to reflect the data that we had collected. Here we present another heuristic which better reflects the data. In each family, let m be the number of pairs of elliptic curves required to be isogenous to ensure double isogeny of two curves in that family; for example, Proposition 6.12 shows that $m = 3$ for family 1. Then we model the double isogeny class of a curve in that family as an m-tuple of independent elliptic curves. Given this, as in Section 5.1, one can compute the expected number of doubly isogenous pairs in the given families under this heuristic. By abuse of notation, we will denote this by $\mathbb{E}(\delta_i(q))$, even though for fixed q, the integer $\delta_i(q)$ is a fixed value and not a random variable.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Heuristic 7.3. *The following are reasonable estimates for the "expected value" of* $\delta_n(q)$ *for prime powers* $q \equiv 1 \bmod 4$:

$$\mathbb{E}(\delta_0(q)) \asymp 1/q, \qquad \mathbb{E}(\delta_1(q)) \asymp 1/\sqrt{q}, \qquad \mathbb{E}(\delta_2(q)) \asymp 1/\sqrt{q},$$
$$\mathbb{E}(\delta_3(q)) \asymp 1/\sqrt{q}, \qquad \mathbb{E}(\delta_4(q)) \asymp 1/q^{3/2}, \quad \textit{and} \quad \mathbb{E}(\delta_{1,2,3}(q)) \asymp 1/\sqrt{q}.$$

Combining these values, we expect that $\mathbb{E}(\delta(q)) \asymp 1/\sqrt{q}$.

Justification. First we consider $\delta_0(q)$. If we assume that there are no families of unexpected coincidences other than the four presented in Section 6.3, then the justification of Naïve Heuristic 5.3 applies to the pairs $\{Z_1, Z_2\}$ that are not in these four families; this suggests that the expected value of $\delta_0(q)$ is $\Theta(1/q)$.

Next we consider $\delta_1(q)$, and in particular we look at the pairs of curves (Z_1, Z_2) which can be written with $t_2 = \zeta t_1$ and $c_2 = c_1$. There are roughly q such ordered pairs. By Proposition 6.12, in order for such a pair to be doubly isogenous, it is sufficient for three coincidences to hold: E_1 and E_2 should be isogenous, and one of the two pairs of isogenies in items (1) and (2) of Proposition 6.12 should hold. We model each of these coincidences as asking that two random elliptic curves lie in the same isogeny class, which happens with probability $\Theta(1/\sqrt{q})$. Thus, we expect to find on the order of $q/(\sqrt{q})^3 = 1/\sqrt{q}$ doubly isogenous pairs with $t_2 = \zeta t_1$ and $c_2 = c_1$.

There are other relations between t_1 and t_2 that lead to Equation (6.3) holding, and again we expect $\Theta(1/\sqrt{q})$ doubly isogenous pairs that satisfy the relation. Thus, in total, we expect $\Theta(1/\sqrt{q})$ pairs of doubly isogenous pairs in the first family.

For $\delta_2(q)$ the argument is similar. By Proposition 6.14, if each of three pairs of elliptic curves is isogenous to one another, the curves Z_1 and Z_2 in the proposition are doubly isogenous. Again modeling these isogeny class collisions as occurring with probability $\Theta(1/\sqrt{q})$, we find that we expect $\Theta(1/\sqrt{q})$ pairs of curves (Z_1, Z_2) coming from pairs of values (t_1, t_2) satisfying (6.4).

As for the first family, there are other relations between t_1 and t_2 that lead to Equation (6.5) holding. For each such relation we again expect $\Theta(1/\sqrt{q})$ doubly isogenous pairs that satisfy the relation. Again, in total, we expect $\Theta(1/\sqrt{q})$ pairs of doubly isogenous pairs in the second family.

We skip over the third family for the moment, for reasons that will become apparent.

For pairs $\{Z_1, Z_2\}$ in the fourth family, we need five coincidental isogenies in order for the curves to be doubly isogenous. This suggests that the expected number of such curves is $\Theta(q/q^{5/2}) = \Theta(1/q^{3/2})$.

Proposition 6.19 suggests that when -7 is a square in $\mathbb{F}_q$ there is one chance out of $\sqrt{q}$ that the two values of t in the proposition give rise to a doubly isogenous pair over $\mathbb{F}_q$ that lies in the first, second, and third families. When -7 is a square in the prime field the curves in this pair are not Galois conjugates of one another and so contribute to the value of $\delta_{1,2,3}(q)$. For other pairs of curves whose invariants are the roots of $x^2 - (47/16)x + 1$ and that are not Galois conjugates of one another, the likelihood of being doubly isogenous is less than this, so in total the expected value of $\delta_{1,2,3}(q)$ is $\Theta(1/\sqrt{q})$.

For pairs $\{Z_1, Z_2\}$ in the third family, if we argue as above we see that we need four coincidental isogenies in order for the curves to be doubly isogenous. This suggests that the expected number of such curves is $\Theta(q/q^{4/2}) = \Theta(1/q)$. But once

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

again our naïve analysis needs revision, because clearly $\delta_3(q) \geq \delta_{1,2,3}(q)$. Thus, we take the expected value of $\delta_3(q)$ to be $\Theta(1/\sqrt{q})$. □

7.2. **Comparison with data.** For $n = 15, \ldots, 23$, we considered the 1024 primes q with $q \equiv 1 \bmod 4$ closest to 2^n. For each such q, we found all unordered pairs $\{Z_1, Z_2\}$ of nonconjugate curves over $\mathbb{F}_q$ with D_4-action and with all Weierstrass points rational for which Z_1 and Z_2 are doubly isogenous. A given pair may appear in more than one family. Table 5 shows which of these pairs are explained by one (or more) of the families.

TABLE 5. Data for doubly isogenous curves. For each n, column 2 contains the total number of (unordered) pairs of doubly isogenous curves over $\mathbb{F}_q$ for the 1024 primes $q \equiv 1 \bmod 4$ closest to 2^n. The 3rd (resp. 4th) column contains the number of these in (resp. not in) at least one family. The remaining columns contain the number for each family.

n	Total	In a Family	Not in a Family	F1	F2	F3	F4	(F1 ∩ F2 ∩ F3)
15	820	586	234	366	222	62	20	38
16	580	494	86	286	198	34	0	12
17	407	318	89	192	138	24	0	18
18	282	238	44	148	96	14	0	10
19	218	196	22	116	90	10	2	10
20	138	132	6	78	58	4	0	4
21	100	90	10	54	40	4	0	4
22	58	58	0	40	16	2	0	0
23	42	40	2	20	20	0	0	0

As predicted by Heuristic 7.3, increasing n by *two* appears to roughly halve the total number of pairs, as well as the pairs in family 1 or family 2 (and possibly in family 3 and in the intersection of the first three families, although it is harder to tell because the numbers are smaller). In contrast, increasing n by *one* appears to roughly halve the number of pairs coming from no family. This is as expected as $\Theta(q^{-1/2}) = \Theta(2^{-n/2})$ and $\Theta(q^{-1}) = \Theta(2^{-n})$ for primes q near 2^n. The numbers for the fourth family drop off too rapidly to easily determine the rate of decline, but our heuristics do at least predict that the fourth family will decrease the fastest.

ACKNOWLEDGMENTS

We thank Bjorn Poonen and Felipe Voloch for helpful conversations.

REFERENCES

[1] J. D. Achter and E. W. Howe, *Split abelian surfaces over finite fields and reductions of genus-2 curves*, Algebra Number Theory **11** (2017), no. 1, 39–76, DOI 10.2140/ant.2017.11.39. MR3602766

[2] G. Cardona and J. Quer, *Curves of genus 2 with group of automorphisms isomorphic to D_8 or D_{12}*, Trans. Amer. Math. Soc. **359** (2007), no. 6, 2831–2849, DOI 10.1090/S0002-9947-07-04111-6. MR2286059

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

[3] F. Charles, *Exceptional isogenies between reductions of pairs of elliptic curves*, Duke Math. J. **167** (2018), no. 11, 2039–2072, DOI 10.1215/00127094-2018-0011. MR3843371
[4] E. W. Howe, *The Weil pairing and the Hilbert symbol*, Math. Ann. **305** (1996), no. 2, 387–392. MR1391223
[5] E. W. Howe, F. Leprévost, and B. Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364, DOI 10.1515/form.2000.008. MR1748483
[6] E. W. Howe, E. Nart, and C. Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields* (English, with English and French summaries), Ann. Inst. Fourier (Grenoble) **59** (2009), no. 1, 239–289. MR2514865
[7] J.-i. Igusa, *Kroneckerian model of fields of elliptic modular functions*, Amer. J. Math. **81** (1959), 561–577, DOI 10.2307/2372914. MR108498
[8] J.-i. Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649, DOI 10.2307/1970233. MR114819
[9] J.-i. Igusa, *On the algebraic theory of elliptic modular functions*, J. Math. Soc. Japan **20** (1968), 96–106, DOI 10.2969/jmsj/02010096. MR240103
[10] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), no. 2, 307–327. MR1000113
[11] E. Kani, *The number of curves of genus two with elliptic differentials*, J. Reine Angew. Math. **485** (1997), 93–121. MR1442190
[12] J.-F. Mestre, *Couples de Jacobiennes isogenes de courbes hyperelliptiques de genre arbitraire*, Preprint, `arXiv:0902.3470 [math.AG]`, 2009.
[13] J.-F. Mestre, *Une généralisation d'une construction de Richelot* (French, with English summary), J. Algebraic Geom. **22** (2013), no. 3, 575–580, DOI 10.1090/S1056-3911-2012-00589-X. MR3048546
[14] J. S. Milne, *Abelian varieties*, Arithmetic Geometry (Storrs, Conn., 1984), 1986, pp. 103–150. MR861974
[15] J. S. Milne, *Jacobian varieties*, Arithmetic Geometry (Storrs, Conn., 1984), 1986, pp. 167–212. MR861976
[16] B. Moonen, *Special subvarieties arising from families of cyclic covers of the projective line*, Doc. Math. **15** (2010), 793–819. MR2735989
[17] B. Poonen, *Using zeta functions to factor polynomials over finite fields*, Arithmetic Geometry: Computation and Applications, Contemp. Math., vol. 722, Amer. Math. Soc., [Providence], RI, [2019] ©2019, pp. 141–147, DOI 10.1090/conm/722/14528. MR3896853
[18] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), no. 2, 183–211, DOI 10.1016/0097-3165(87)90003-3. MR914657
[19] B. Smith, *Families of explicitly isogenous Jacobians of variable-separated curves*, LMS J. Comput. Math. **14** (2011), 179–199, DOI 10.1112/S1461157010000410. MR2831229
[20] A. V. Sutherland and J. F. Voloch, *Maps between curves and arithmetic obstructions*, Arithmetic Geometry: Computation and Applications, Contemp. Math., vol. 722, Amer. Math. Soc., [Providence], RI, [2019] ©2019, pp. 167–175, DOI 10.1090/conm/722/14532. MR3896855

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.

Unaffiliated mathematician, Sunnyvale, California 94086
Email address: varul.math@gmail.com

School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand
Email address: jeremybooher@ufl.edu

Department of Mathematics, Lehigh University, 17 Memorial Drive E, Bethlehem, Pennsylvania 18018
Email address: stg323@lehigh.edu

Unaffiliated mathematician, San Diego, California 92104
Email address: however@alumni.caltech.edu

Department of Mathematics, Washington University in St. Louis, One Brookings Drive, St. Louis, MO 63130
Email address: wanlin@wustl.edu

Institute of Mathematics of the Romanian Academy, P.O. Box 1-764, Bucharest RO-70700, Romania
Email address: vmatei@imar.ro

Department of Mathematics, Colorado State University, Fort Collins, Colorado 80523
Email address: pries@colostate.edu

Department of Mathematics, University College London, Gower Street, London WC1H 0AY; and The Heilbronn Institute for Mathematical Research, Bristol, UK
Email address: c.springer@ucl.ac.uk

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.