PRIME-LEVEL ENTANGLEMENTS UNDER RATIONAL ISOGENY

MICHAEL CERCHIA

Abstract. We classify how the prime-level entanglement fields $\mathbb{Q}(E[p]) \cap \mathbb{Q}(E[q])$ vary in a rational isogeny class of non-CM elliptic curves over $\mathbb{Q}$. If p and q are odd, this field is constant throughout the class. For cyclic isogenies of odd degree, the field can change only when the isogeny has degree 3 and $\{p, q\} = \{2, 3\}$. If such a change occurs, the isogeny class consists of two curves, and the two entanglement fields are L and $\mathbb{Q}(\sqrt{-3})$, where L is their common 2-division field and $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$.

For classes containing a rational 2-isogeny, we classify all possible $(2, q)$-intersection patterns in the isogeny graph. Some of the patterns occur precisely when certain elliptic curves have positive rank. As a consequence, a rational cyclic 16-isogeny with a nontrivial $(2, q)$-intersection exists if and only if q is a congruent number.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. The action of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the torsion points of E yields the adelic representation $\rho_E : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}})$. When E is non-CM, Serre's open image theorem says that $\rho_E(G_{\mathbb{Q}})$ has finite index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ [17]. It is then natural to ask which images can occur.

For elliptic curves over $\mathbb{Q}$ admitting a rational cyclic isogeny, recent work of Finnerty, Genao, Mayle, and Rakvi determines the possible adelic indices $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})]$ [9]. However, the index alone does not determine the adelic image. Even the individual ℓ-adic images do not determine the adelic image, since division fields at distinct primes can intersect. Understanding these division field "entanglements" and how they vary under isogeny is therefore a necessary step towards classifying the possible adelic images of elliptic curves admitting a rational isogeny.

To formulate the current problem precisely, we introduce some notation. For $n \geq 1$ and distinct primes p, q, set

$$K_n(E) := \mathbb{Q}(E[n]) \quad \text{and} \quad F_{p,q}(E) := K_p(E) \cap K_q(E).$$

All division fields are viewed inside a fixed algebraic closure $\overline{\mathbb{Q}}$. For notational convenience, we write $F = F_{p,q}(E)$ when this is unambiguous. If $F \neq \mathbb{Q}$, we call F an *entanglement field*, and say that E has a (p, q)-*entanglement*. We say that the entanglement is *abelian* if $F/\mathbb{Q}$ is abelian and *nonabelian* if $F/\mathbb{Q}$ is nonabelian. Since $K_{pq}(E) = K_p(E)K_q(E)$, it follows from Galois theory that $\rho_{E,pq}(G_{\mathbb{Q}}) \simeq \rho_{E,p}(G_{\mathbb{Q}}) \times_{\mathrm{Gal}(F/\mathbb{Q})} \rho_{E,q}(G_{\mathbb{Q}})$. Consequently,

$$[\rho_{E,p}(G_{\mathbb{Q}}) \times \rho_{E,q}(G_{\mathbb{Q}}) : \rho_{E,pq}(G_{\mathbb{Q}})] = [F : \mathbb{Q}].$$

Thus, the entanglement field F measures the failure of the mod pq image to be the direct product of the mod p and mod q images.

Date: October 30, 2026.

2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F80, 14G35.

Key words and phrases. Elliptic curves, division fields, entanglements, isogenies, Galois representations.

Entanglements of division fields have been studied in [7, 6, 5, 11]. To study entanglement variation under rational isogeny, we organize a rational isogeny class $\mathcal{C}$ by its *isogeny graph* $\mathcal{G}(\mathcal{C})$. The vertices of this graph are the $\mathbb{Q}$-isomorphism classes of elliptic curves in the class, and there is an edge between two vertices whenever there is a rational isogeny of prime degree between them. Our main theorem determines how the fields $F_{p,q}(E)$ can vary in this graph.

For an odd prime q, let $q^* = (-1)^{(q-1)/2}q$ and let $W_q = \mathbb{Q}(\sqrt{q^*})$, which is the unique quadratic subfield of $\mathbb{Q}(\zeta_q)$.

Theorem 1.1. *Let $\mathcal{C}$ be a rational isogeny class of non-CM elliptic curves, and let $p \neq q$ be primes. Then the following hold.*

1. *If p and q are both odd, then $F_{p,q}(E)$ is the same for every $E \in \mathcal{C}$.*
2. *Suppose that $\mathcal{C}$ has no rational 2-isogeny. If $F_{p,q}(E)$ is not constant on $\mathcal{C}$, then $\{p,q\} = \{2,3\}$ and $\mathcal{C}$ consists of two curves, E and E', connected by a rational 3-isogeny. Their common 2-division field $L = K_2(E) = K_2(E')$ satisfies $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$, and*
$$\{F_{2,3}(E), F_{2,3}(E')\} = \{L, \mathbb{Q}(\sqrt{-3})\}.$$
This variation occurs for infinitely many distinct rational isogeny classes.
3. *Suppose that $\mathcal{C}$ has a rational 2-isogeny. For every odd prime q, the field $K_q(E) \cap \mathbb{Q}^{\mathrm{ab}}$ is the same for all $E \in \mathcal{C}$. Writing $A_q(\mathcal{C})$ for this common field, we have*
$$F_{2,q}(E) = K_2(E) \cap A_q(\mathcal{C})$$
for every $E \in \mathcal{C}$. These intersections have degree at most two over $\mathbb{Q}$, are constant along edges of odd degree, and equal $\mathbb{Q}$ at vertices with full rational 2-torsion.
4. *Under the hypothesis of (3), if $q \geq 7$, then $F_{2,q}(E) \in \{\mathbb{Q}, W_q\}$ for every $E \in \mathcal{C}$. For every odd prime q, the complete graph-level classification is given in tables 4 and 5. Every such pattern occurs in infinitely many distinct rational isogeny classes.*

We note that the cases $q = 3, 5$ require separate treatment because their division fields may contain quadratic subfields other than W_q.

The existence of certain $(2,q)$-entanglement patterns at a fixed q is governed by the ranks of the following elliptic curves, with $w = q^*$:

$$\mathscr{E}_{10,q}: \quad Y^2 = X^3 - 2wX^2 + 5w^2X, \tag{1.1}$$

$$\mathscr{E}_{12,q}: \quad Y^2 = X^3 + 2wX^2 - 3w^2X, \tag{1.2}$$

$$\mathscr{E}_{16,q}: \quad Y^2 = X^3 - q^2X, \tag{1.3}$$

$$\mathscr{E}_{18,q}: \quad Y^2 = X^3 + w^3. \tag{1.4}$$

Write $r_N(q) = \operatorname{rank} \mathscr{E}_{N,q}(\mathbb{Q})$.

Theorem 1.2. *Let q be an odd prime and $N \in \{10, 12, 16, 18\}$. There is a rational cyclic N-isogeny $E \to E'$ between non-CM elliptic curves for which one of $F_{2,q}(E)$ and $F_{2,q}(E')$ is W_q if and only if $r_N(q) > 0$. Whenever this happens, the other intersection is $\mathbb{Q}$. If $r_N(q) > 0$, both ordered pairs $(W_q, \mathbb{Q})$ and $(\mathbb{Q}, W_q)$ occur for infinitely many distinct source j-invariants.*

A positive integer is a *congruent number* if it is the area of a right triangle with rational side lengths. The standard correspondence between congruent numbers and nontorsion rational points on $Y^2 = X^3 - q^2X$ (see, for example, [8]) leads to the following consequence.

Corollary 1.3. *Let q be an odd prime. There exists a rational cyclic 16-isogeny $E \to E'$ between non-CM elliptic curves such that one of $F_{2,q}(E)$ and $F_{2,q}(E')$ is nontrivial if and only if q is a congruent number.*

We also determine the possible pairs of intersection fields across rational cyclic isogenies of composite degree. The complete list is given in corollary 9.2. Arbitrary (possibly noncyclic) isogenies are handled by proposition 9.3.

1.1. **Proof strategy.** It is a standard fact that a rational isogeny of degree d preserves the n-division field whenever $\gcd(n, d) = 1$. Consequently, a prime-level intersection can change across an isogeny only if one of its level primes divides d.

For isogenies of odd prime degree, we show that the maximal abelian subfield of every prime-level intersection is preserved, and that a change involving a nonabelian intersection can occur only for the pair $\{2, 3\}$ across a rational 3-isogeny. We use a level 18 modular curve of Jones–McMurdy [11] and the modular curve $X'(6)$ of Brau–Jones [2] to determine the two intersection fields in theorem 1.1(2).

For classes containing a rational 2-isogeny, each 2-division field $K_2(E)$ has degree at most two over $\mathbb{Q}$ and is therefore abelian. We show that $K_q(E) \cap \mathbb{Q}^{\mathrm{ab}}$ is constant throughout the isogeny class for every odd prime q. Thus, $F_{2,q}(E)$ is nontrivial precisely when $K_2(E)$ is a quadratic subfield of this fixed abelian field.

To apply this criterion, we use the classification of rational isogeny-torsion graphs of Chiloyan–Lozano-Robledo [4] to determine the 2-division fields at the vertices. For $q \geq 7$, the mod q image is surjective, so $F_{2,q}(E)$ is nontrivial precisely when $K_2(E) = W_q$. For $q = 3, 5$, the division fields $K_q(E)$ may contain quadratic subfields other than W_q. We determine these from the quadratic characters of the mod q Galois images. Specifically, for $q = 3$ we use Rakvi's classification of the 3-adic images [16]. For $q = 5$, we use the mod 5 image restrictions of [9] and the quadratic field calculations of [6].

1.2. **Outline.** In Section 2, we present preliminary results on division fields and rational isogeny graphs. In Section 3, we consider odd-degree isogenies and determine the exceptional $(2, 3)$ transition. In Section 4, we compute the 2-division fields across a rational 2-isogeny and classify the intersections when $K_q(E)$ has a unique quadratic subfield. In Section 5, we classify $(2, 3)$-intersections for curves admitting rational 2 and 3-isogenies and determine the $(2, q)$-intersection patterns on the mixed graphs $R_4(6)$, S, and $R_6(18)$. In Section 6, we handle the remaining $(2, 3)$-intersection cases. In Section 7, we study $(2, q)$-intersections in classes admitting rational 5-isogenies. In Section 8, we analyze isogeny graphs with multiple 2-isogenies and no odd-degree edges, and establish the congruent-number criterion. In Section 9, we assemble the complete graph-level classification, prove theorems 1.1 and 1.2, and determine the possible intersection fields across composite-degree and arbitrary isogenies. The appendix collects the rational point calculations used in the proofs.

Acknowledgments. We thank Rakvi for a helpful conversation that led to the extension of the main theorem from fixed isogenies to full isogeny classes.

2. Preliminaries on division fields and rational isogeny graphs

For a positive integer n, let $A_n(E) := K_n(E) \cap \mathbb{Q}^{\mathrm{ab}}$ be the maximal abelian subfield of $K_n(E)$. For distinct primes p and q, we have that $F_{p,q}(E) \cap \mathbb{Q}^{\mathrm{ab}} = A_p(E) \cap A_q(E)$. When

this field is nontrivial, its Galois group over $\mathbb{Q}$ is the prime-level abelian entanglement type in the terminology of Daniels–Lozano-Robledo–Morrow [6, Definition 3.2].

The following Lemma is well known, but we include it here for completeness.

Lemma 2.1. *Let $\phi : E \to E'$ be a $\mathbb{Q}$-rational isogeny of degree d, and let n be a positive integer with $\gcd(n, d) = 1$. Then $K_n(E) = K_n(E')$.*

Proof. Since $\gcd(n, \deg \phi) = 1$, we have that $E[n] \cap \ker \phi = \{0\}$. Thus, the restriction $\phi : E[n] \longrightarrow E'[n]$ is injective, and hence an isomorphism since both groups have order n^2. Since ϕ is defined over $\mathbb{Q}$, this isomorphism is $G_{\mathbb{Q}}$-equivariant. Therefore, $\sigma \in G_{\mathbb{Q}}$ fixes $E[n]$ pointwise if and only if it fixes $E'[n]$ pointwise, and so $K_n(E) = K_n(E')$. □

In particular, across an isogeny of prime degree λ, a prime-level intersection $F_{p,q}$ can change only if $\lambda \in \{p, q\}$.

2.1. **Invariance under odd-prime isogenies.** To prove the invariance of maximal abelian subfields under odd-prime isogenies, we use the following description of the abelianization of a Borel subgroup.

Lemma 2.2. *Let λ be an odd prime and let $H \subseteq \mathsf{B}(\lambda)$ have surjective determinant. Let U be the subgroup of upper triangular matrices with 1's on the diagonal and let $\delta : H \to (\mathbb{F}_\lambda^\times)^2$ be the diagonal map. Then $[H, H] = H \cap U = \ker \delta$. Consequently, $H^{\mathrm{ab}} \simeq \delta(H)$, and the commutator subgroup of every quotient of H has order 1 or λ.*

Proof. Since the determinant is surjective and λ is odd, H contains an element with unequal diagonal entries. By [14, Lemma 2.2], we have $[H, H] = H \cap U = \ker \delta$. The remaining assertions follow since $U \simeq C_\lambda$. □

In particular, if the mod λ representation of $E/\mathbb{Q}$ has diagonal characters α and β, then $A_\lambda(E) = \overline{\mathbb{Q}}^{\ker(\alpha,\beta)}$, where $\ker(\alpha, \beta) = \ker \alpha \cap \ker \beta$.

Theorem 2.3. *Let $\phi : E \to E'$ be a rational cyclic isogeny of odd prime degree λ. Then $A_\ell(E) = A_\ell(E')$ for every prime ℓ. Consequently, for distinct primes p and q,*

$$F_{p,q}(E) \cap \mathbb{Q}^{\mathrm{ab}} = F_{p,q}(E') \cap \mathbb{Q}^{\mathrm{ab}}.$$

Proof. For $\ell \neq \lambda$, it follows immediately from lemma 2.1 that $A_\ell(E) = A_\ell(E')$.

It remains to consider $\ell = \lambda$. Let ψ and ψ' be the characters describing the Galois actions on $\ker \phi$ and $\ker \widehat{\phi}$, respectively, where $\widehat{\phi}$ is the dual isogeny. Choose a basis $\{P, Q\}$ of $E[\lambda]$ with P generating $\ker \phi$. Then $\phi(Q)$ is a nonzero element of $\ker \widehat{\phi}$ and therefore generates it. Since ϕ is $G_{\mathbb{Q}}$-equivariant, the diagonal characters on $E[\lambda]$ are (ψ,ψ'). Similarly, using the dual isogeny, the diagonal characters on $E'[\lambda]$ are (ψ', ψ). By the remark following lemma 2.2, $A_\lambda(E) = \overline{\mathbb{Q}}^{\ker(\psi,\psi')} = \overline{\mathbb{Q}}^{\ker(\psi',\psi)} = A_\lambda(E')$. The final assertion follows from $F_{p,q}(E) \cap \mathbb{Q}^{\mathrm{ab}} = A_p(E) \cap A_q(E)$ and the same identity for E'. □

We record the following standard result on the factorization of rational isogenies.

Lemma 2.4. *Let $\phi : E \to E'$ be a rational isogeny. There exist a positive integer a and a rational cyclic isogeny $\psi : E \to E'$ such that $\phi = \psi \circ [a]$. Moreover, ψ factors over $\mathbb{Q}$ into isogenies of prime degree.*

Proof. Over $\overline{\mathbb{Q}}$, we write $\ker\phi \simeq C_a \times C_b$, where $a \mid b$. The subgroup $(\ker\phi)[a]$ has order a^2. Since $(\ker\phi)[a] \subseteq E[a]$ and $|E[a]| = a^2$, we have $(\ker\phi)[a] = E[a]$. Thus, $\phi = \psi \circ [a]$ for an isogeny $\psi : E \to E'$, and $\ker\psi = [a](\ker\phi)$ is cyclic of order b/a. The factorization through the surjective map $[a]$ is unique, and so ψ is defined over $\mathbb{Q}$.

The cyclic group $\ker\psi$ has a unique subgroup of each order dividing its order. Since $\ker\psi$ is $G_{\mathbb{Q}}$-stable, each of these subgroups is also $G_{\mathbb{Q}}$-stable. Successive quotients therefore produce a factorization of ψ over $\mathbb{Q}$ into isogenies of prime degree. □

Applying theorem 2.3 along this factorization shows that every rational cyclic isogeny of odd degree preserves $A_\ell(E)$ for every prime ℓ, and hence preserves $F_{p,q}(E) \cap \mathbb{Q}^{\mathrm{ab}}$.

Proposition 2.5. *Let $\mathcal{C}$ be a rational isogeny class. For every odd prime q, the field $A_q(E)$ is the same for all $E \in \mathcal{C}$.*

Proof. By lemma 2.4, any two vertices can be connected by rational prime-degree isogenies. An isogeny of prime degree $\ell \neq q$ preserves $K_q(E)$ by lemma 2.1, while an isogeny of degree q preserves $A_q(E)$ by theorem 2.3. Applying these statements successively proves the claim. □

We write $A_q(\mathcal{C})$ for this common field. The restriction to odd q is important: $A_2(E)$ need not be constant on $\mathcal{C}$.

2.2. **Rational isogeny graphs.** We organize an isogeny class $\mathcal{C}$ by its corresponding *isogeny graph* $\mathcal{G}(\mathcal{C})$. The vertices of $\mathcal{G}(\mathcal{C})$ are the $\mathbb{Q}$-isomorphism classes in $\mathcal{C}$. An edge of label ℓ joins two vertices when they are connected by a rational isogeny of prime degree ℓ. We use the graph notation of Chiloyan–Lozano-Robledo [4], and we call a vertex corresponding to a curve with full rational 2-torsion a *core vertex*. We call an isogeny graph *mixed* if it contains both 2-edges and odd-degree edges.

For non-CM curves, the graphs containing a 2-edge are

$$L_2(2), \quad T_4, \quad T_6, \quad T_8, \quad R_4(6), \quad R_4(10), \quad S, \quad R_6(18).$$

The graph $L_2(2)$ is a single edge; the other shapes appear in figure 1. This is the list from [4, Theorem 1.2] needed here. The curves at all vertices of these graphs have rational 2-torsion. Across an odd-degree edge, rational 2-torsion is preserved because an odd-degree isogeny induces a $G_{\mathbb{Q}}$-equivariant isomorphism on 2-torsion, as in the proof of lemma 2.1. Across a 2-edge, both curves have rational 2-torsion, since the isogeny and its dual each have a rational kernel of order 2.

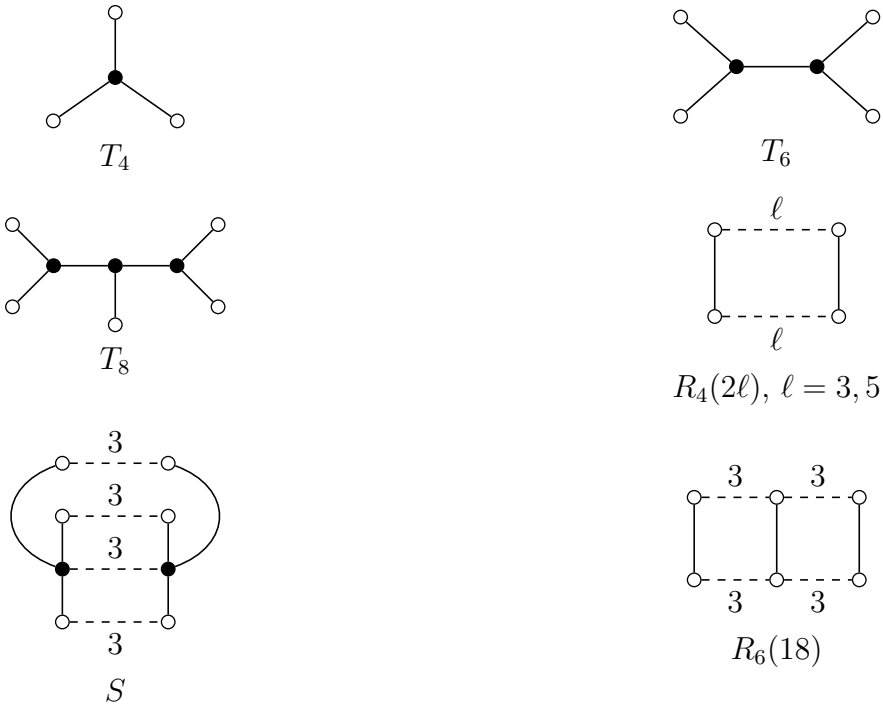

FIGURE 1. The non-CM rational isogeny graphs containing a 2-edge other than $L_2(2)$. Solid edges have degree 2; dashed edges have the indicated odd degree. Filled vertices have full rational 2-torsion.

For the analysis of $(2,3)$-entanglements, we also need the possible mod 3 Galois images on these graphs. We write $\mathsf{B}(q)$ for the upper-triangular subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$, and $C_{\mathrm{s}}(q)$, $C_{\mathrm{ns}}(q)$, $N_{\mathrm{s}}(q)$, and $N_{\mathrm{ns}}(q)$ for the split and nonsplit Cartans and their normalizers. Rakvi's classification shows that every vertex of T_4, T_6, T_8, and $R_4(10)$ has full mod 3 image. On $L_2(2)$, the possible mod 3 images are $\mathrm{GL}_2(\mathbb{F}_3)$, $N_{\mathrm{s}}(3)$, and $N_{\mathrm{ns}}(3)$ [16, Theorem 1.1, Tables 1 and 3]. The graphs $R_4(6)$, S, and $R_6(18)$ have rational 3-isogenies at every vertex.

2.3. **An infinitude criterion.** We use the following consequence of Hilbert irreducibility to show that the intersection patterns constructed below occur for infinitely many distinct j-invariants.

Lemma 2.6. *Let U be a smooth rational variety of positive dimension over $\mathbb{Q}$, and let $\mathcal{E} \to U$ be a family of elliptic curves. Fix a positive integer n and a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing the generic mod n image. Suppose some good rational specialization has exact mod n image G.*

Let $f_1, \dots, f_r \in \mathbb{Q}(U)^\times$ be nonsquares. Then there are infinitely many $u \in U(\mathbb{Q})$ for which the specialization has exact mod n image G and every $f_i(u)$ is defined and nonsquare. These points can be chosen outside any prescribed proper closed subset of U. If the j-map is nonconstant, they can also be chosen with pairwise distinct j-invariants.

Proof. The image at a good specialization is, up to conjugacy, contained in the generic image. Thus the generic image is G, and Hilbert irreducibility shows that the specializations with smaller image lie in a thin set [18, Chapter 3].

Since each f_i is a nonsquare in $\mathbb{Q}(U)$, the equation $y^2 = f_i$ defines an irreducible double cover of U over a suitable open subset. Hence the rational points where $f_i(u)$ is a square

also form a thin set. A finite union of thin sets and proper closed subsets cannot exhaust the rational points of a positive-dimensional rational variety.

Finally, if the j-map is nonconstant, each fiber is a proper closed subset of U. We can therefore avoid the j-invariants of previously chosen points, obtaining infinitely many distinct ones. □

To apply the lemma, it suffices to exhibit a specialization with exact mod n image G and verify that the functions defining the unwanted squareclass conditions are nonsquares in $\mathbb{Q}(U)$. For the latter, it suffices to find for each function a specialization where its value is nonsquare.

3. Odd-degree isogenies and the nonabelian exception

By lemma 2.1 and theorem 2.3, if a prime-level intersection changes across a rational isogeny of odd prime degree λ, then λ is one of the two level primes, and at least one of the two intersection fields is nonabelian.

The goal of this section is to determine the pairs (λ, q) for which such a nonabelian intersection can occur.

3.1. Twists and Galois images.

We adapt the argument of [23, Lemma 3.1] to apply for every odd prime.

Lemma 3.1. *Let q be an odd prime. If $\rho_{E,q}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_q)$, then the mod q representation of every quadratic twist of E is also surjective.*

Proof. Let $E^{(d)}$ be a quadratic twist of E, and let $\chi_d : G_{\mathbb{Q}} \to \{\pm 1\}$ be the character that factors through $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \hookrightarrow \{\pm 1\}$. After choosing compatible bases, $\rho_{E^{(d)},q}(\sigma) = \chi_d(\sigma)\rho_{E,q}(\sigma)$. Hence $\pm\rho_{E^{(d)},q}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_q)$. Since $-I$ lies in the center of $\mathrm{GL}_2(\mathbb{F}_q)$, taking commutator subgroups shows that $\rho_{E^{(d)},q}(G_{\mathbb{Q}})$ contains $\mathrm{SL}_2(\mathbb{F}_q)$. The determinant of $\rho_{E^{(d)},q}$ is the mod q cyclotomic character, and so it is surjective onto $\mathbb{F}_q^{\times}$. Thus, $\rho_{E^{(d)},q}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_q)$. □

To apply the q-adic image results below, we need a way to ensure that the image contains $-I$. The following lemma shows that this can be achieved by quadratic twisting and that doing so does not change which rational isogenies the curve admits.

Lemma 3.2. *Let $E/\mathbb{Q}$ be an elliptic curve, let q be an odd prime, and let $H = \rho_{E,q}(G_{\mathbb{Q}})$. There is a quadratic twist $E^{\chi}/\mathbb{Q}$ whose mod q image is $\langle H, -I\rangle$ and whose q-adic image contains $-I$. Moreover, for every prime r, the curve E admits a rational r-isogeny if and only if E^{χ} does.*

Proof. Choose a quadratic character χ whose corresponding quadratic field is linearly disjoint from $K_q(E)$. Such a field exists because $K_q(E)$ has only finitely many quadratic subfields. The image of $(\rho_{E,q}, \chi)$ is $H \times \{\pm 1\}$, and so

$$\rho_{E^{\chi},q}(G_{\mathbb{Q}}) = \{\varepsilon h : h \in H,\ \varepsilon \in \{\pm 1\}\} = \langle H, -I\rangle.$$

This mod q claim also follows from [19, Corollary 5.25].

The q-adic image of E^{χ} is closed and contains an element $g \equiv -I \pmod{q}$. Writing $g = -I(I + qA)$, we have $g^{q^n} \to -I$ as $n \to \infty$, since q is odd. Thus, the q-adic image of E^{χ} contains $-I$.

Under the identification $E[r] \simeq E^{\chi}[r]$ over $\overline{\mathbb{Q}}$, the two Galois actions differ by the scalar $\chi(\sigma)$. They therefore preserve the same one-dimensional subspaces, which correspond to kernels of rational r-isogenies. For $r = 2$, the two representations are identical, since $-1 = 1$ in $\mathbb{F}_2$. □

For the mod 5 argument below, we need to recover the original image from the group obtained by adjoining $-I$. We let $\mathcal{E}S_4(5)$ denote the exceptional subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$ with projective image isomorphic to S_4, which is unique up to conjugacy.

Lemma 3.3. *Let $H \subseteq \mathrm{GL}_2(\mathbb{F}_5)$ have surjective determinant, and let $H^{\pm} := \langle H, -I \rangle$. If $H^{\pm}$ is either $\mathrm{GL}_2(\mathbb{F}_5)$ or $\mathcal{E}S_4(5)$, then $H = H^{\pm}$.*

Proof. For either group $G \in \{\mathrm{GL}_2(\mathbb{F}_5), \mathcal{E}S_4(5)\}$, the determinant induces $G^{\mathrm{ab}} \simeq \mathbb{F}_5^{\times}$. For $\mathrm{GL}_2(\mathbb{F}_5)$ this follows from $[\mathrm{GL}_2(\mathbb{F}_5), \mathrm{GL}_2(\mathbb{F}_5)] = \mathrm{SL}_2(\mathbb{F}_5)$; for $\mathcal{E}S_4(5)$ it follows from the calculation in the proof of [5, Proposition 5.10]. Since $\mathbb{F}_5^{\times} \simeq C_4$, the unique index two subgroup of G is $\ker(\det^2)$, whose determinants are squares. If $-I \notin H$, then H has index two in $H^{\pm}$ and must be this subgroup, contradicting the surjectivity of $\det(H)$. □

Lemma 3.4. *Let $E/\mathbb{Q}$ be non-CM and admit a rational 11-isogeny. Then $\rho_{E,23}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_{23})$.*

Proof. There are two non-CM rational j-invariants on $X_0(11)$ (see [9, Section 6]). Representatives are

$$E_1 : y^2 + xy + y = x^3 + x^2 - 305x + 7888,$$
$$E_2 : y^2 + xy = x^3 + x^2 - 3632x + 82757.$$

Both curves have good reduction at 2 and 3. A point count gives

	$\#E(\mathbb{F}_2)$	a_2	$\#E(\mathbb{F}_3)$	a_3
E_1	4	-1	2	2
E_2	2	1	2	2,

where $a_\ell = \ell + 1 - \#E(\mathbb{F}_\ell)$.

For either curve, let $G := \rho_{E,23}(G_{\mathbb{Q}})$ and let $\overline{G}$ be its image in $\mathrm{PGL}_2(\mathbb{F}_{23})$. At a prime $\ell \neq 23$ of good reduction, Frobenius has characteristic polynomial $x^2 - a_\ell x + \ell \bmod 23$.

At $\ell = 2$, the discriminant is $a_2^2 - 8 = -7 \equiv 16 \pmod{23}$, a nonzero square. The eigenvalues are $13, 9$ for E_1 and $14, 10$ for E_2. Their ratios in $\mathbb{F}_{23}^{\times}$ are $13/9 = 4$ and $14/10 = 6$, both of order 11. The order of the eigenvalue ratio is the projective order. Thus, $\overline{G}$ contains an element of order 11, represented by a matrix with distinct eigenvalues in $\mathbb{F}_{23}$ and nonzero trace.

At $\ell = 3$, the characteristic polynomial is $x^2 - 2x + 3$, with discriminant $-8 \equiv 15 \pmod{23}$, a nonsquare. Thus, the corresponding Frobenius element has irreducible characteristic polynomial over $\mathbb{F}_{23}$ and nonzero trace.

By Dickson's classification [19, Proposition 3.1], if G does not contain $\mathrm{SL}_2(\mathbb{F}_{23})$, then it is contained in a Borel or a Cartan normalizer, or its projective image is isomorphic to A_4, S_4, or A_5. The Frobenius at 3 excludes a Borel, since an upper-triangular matrix has its eigenvalues in $\mathbb{F}_{23}$. It also excludes a split Cartan normalizer, since elements of the Cartan have split characteristic polynomial, while elements outside the Cartan have trace zero. The Frobenius at 2 excludes a nonsplit Cartan normalizer, since non-scalar elements of the

Cartan have irreducible characteristic polynomial, while elements outside the Cartan have trace zero. Finally, none of A_4, S_4, or A_5 has an element of order 11. Hence, $\mathrm{SL}_2(\mathbb{F}_{23}) \subseteq G$.

The determinant is the surjective mod 23 cyclotomic character, and so $G = \mathrm{GL}_2(\mathbb{F}_{23})$.

Every curve over $\mathbb{Q}$ with either of these j-invariants is a quadratic twist of the corresponding representative. The result follows from lemma 3.1. □

3.2. **Restricting the prime pairs.**

Proposition 3.5. *Suppose $E/\mathbb{Q}$ is non-CM and admits a rational isogeny of odd prime degree λ. Let $q \neq \lambda$ be prime. Suppose that the mod q image has a nonabelian solvable quotient whose commutator subgroup is cyclic of order λ. Then*

$$(\lambda, q) = (3, 2) \quad \text{or} \quad (\lambda, q) = (3, 5).$$

In the second case, the mod 5 image is conjugate to $\mathcal{E}S_4(5)$.

Proof. Let $H_q := \rho_{E,q}(G_{\mathbb{Q}})$. If $q = 2$, a subgroup of $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$ can have no nonabelian quotient other than S_3, which means $\lambda = 3$. If $q = 3$, then λ would divide $|\mathrm{GL}_2(\mathbb{F}_3)| = 48$, which is impossible for an odd prime $\lambda \neq 3$.

Suppose that $q \geq 5$. If $H_q = \mathrm{GL}_2(\mathbb{F}_q)$, let $\pi : H_q \twoheadrightarrow T$ be a solvable quotient. The group $\mathrm{SL}_2(\mathbb{F}_q)$ is perfect, and so its image in T is both perfect and solvable, hence trivial. Thus $\mathrm{SL}_2(\mathbb{F}_q) \subseteq \ker \pi$, and π factors through $\mathrm{GL}_2(\mathbb{F}_q)/\mathrm{SL}_2(\mathbb{F}_q) \simeq \mathbb{F}_q^\times$. In particular, T is abelian. If H_q is contained in a Borel, its determinant is surjective, so lemma 2.2 shows that the commutator subgroup of any quotient is trivial or cyclic of order q. Since $q \neq \lambda$, neither a full image nor a subgroup of a Borel has the required quotient.

By Mazur's theorem [15], the possible odd prime isogeny degrees for non-CM curves over $\mathbb{Q}$ are $\lambda \in \{3, 5, 7, 11, 13, 17, 37\}$. Furthermore, Lemos proved that the mod q Galois representation is surjective for every $q > 37$ [13], so we need only consider $q \leq 37$.

The proposition numbers below refer to arXiv:2512.00652v2 of [9]. Whenever one of these propositions states that the q-adic image is $\mathrm{GL}_2(\mathbb{Z}_q)$, reduction mod q shows that the mod q image is $\mathrm{GL}_2(\mathbb{F}_q)$. The exceptional 5-adic group 5.5.0.a.1 in that paper reduces to $\mathcal{E}S_4(5)$.

Suppose first that $\lambda = 3$ and E has no rational isogeny of larger prime degree. Proposition 19(4) of [9] gives surjectivity for every $q \geq 7$. To apply Proposition 19(3) at $q = 5$, use lemma 3.2 to choose a twist whose 5-adic image contains $-I$. The twist has the same possible prime isogeny degrees, and its mod 5 image is $\langle H_5, -I \rangle$. Reducing the possibilities in Proposition 19(3) mod 5, we find that $\langle H_5, -I \rangle$ is either $\mathrm{GL}_2(\mathbb{F}_5)$ or conjugate to $\mathcal{E}S_4(5)$. By lemma 3.3, the same holds for H_5.

If E also has a rational isogeny of prime degree $r > 3$, the two kernels generate a Galois-stable cyclic subgroup of order $3r$. Kenku's list [12] implies $r \in \{5, 7\}$. At $q = r$, the image is contained in a Borel. For every prime $q \geq 5$ with $q \neq r$, it is surjective by [9, Propositions 20(4) and 21(4)]. Thus, for $\lambda = 3$, only $q = 2$ or $q = 5$ with mod 5 image conjugate to $\mathcal{E}S_4(5)$ remains.

For $\lambda = 5$, [9, Proposition 20(4)] gives surjectivity for every $q \geq 7$, while the groups at $q = 2, 3$ have order prime to 5. For $\lambda = 7$, [9, Proposition 21(4)] gives surjectivity for $q \geq 5$, $q \neq 7$, and the groups at $q = 2, 3$ have order prime to 7. For $\lambda = 13$, [9, Proposition 22(3)] gives surjectivity for every $q \geq 3$, $q \neq 13$, while $|\mathrm{GL}_2(\mathbb{F}_2)|$ is prime to 13.

For $\lambda \in \{17, 37\}$, no prime $q \leq 37$ with $q \neq \lambda$ satisfies $\lambda \mid q(q-1)^2(q+1) = |\mathrm{GL}_2(\mathbb{F}_q)|$. For $\lambda = 11$, the only such prime is $q = 23$, which is excluded by lemma 3.4.

Thus, the only remaining pairs are $(\lambda, q) = (3, 2)$ and $(3, 5)$. □

The remaining mod 5 possibility cannot produce a nonabelian $(3,5)$-intersection over $\mathbb{Q}$.

Lemma 3.6. *Let $E/\mathbb{Q}$ have mod 3 image $H_3 \subseteq \mathsf{B}(3)$ and mod 5 image conjugate to $\mathcal{E}S_4(5)$. Then $K_3(E) \cap K_5(E)$ is abelian over $\mathbb{Q}$.*

Proof. Suppose that $F := K_3(E) \cap K_5(E)$ is nonabelian, and let $T := \mathrm{Gal}(F/\mathbb{Q})$. Restriction makes T a quotient of both H_3 and $\mathcal{E}S_4(5)$. By lemma 2.2, $[T,T] \simeq C_3$ and $H_3^{\mathrm{ab}} \simeq \delta(H_3) \subseteq C_2 \times C_2$. On the other hand, $\mathcal{E}S_4(5)^{\mathrm{ab}} \simeq C_4$ via the determinant, as recalled in the proof of lemma 3.3. Thus T^{ab}, which is a quotient of both abelianizations, is either trivial or C_2. It cannot be trivial, since this would mean $T = [T,T] \simeq C_3$. Hence $|T| = 6$ and $T \simeq S_3$.

On the mod 3 side, write $U_3 = \{\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) : x \in \mathbb{F}_3\}$. Since $[T,T]$ is the image of $[H_3,H_3] = H_3 \cap U_3$ and has order 3, we have $U_3 \subseteq H_3$, and the quotient map identifies U_3 with A_3. Conjugation by $h = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ on U_3 is equivalent to multiplication by $a/d = ad = \det h$. Conjugation on A_3 is trivial for even permutations and inversion for odd permutations. Hence, the sign character of the S_3 quotient is the mod 3 cyclotomic character, and so the unique quadratic subfield of F is $\mathbb{Q}(\sqrt{-3})$.

On the mod 5 side, the unique nontrivial quadratic character of $\mathcal{E}S_4(5)$ is $\det^2$. Composing with $\rho_{E,5}$ yields the character corresponding to $\mathbb{Q}(\sqrt{5})$. The two quadratic fields are distinct, which is a contradiction. □

Corollary 3.7. *Let $\phi : E \to E'$ be a rational isogeny of odd prime degree λ between non-CM elliptic curves over $\mathbb{Q}$, and suppose that $\lambda \in \{p,q\}$. If either $K_p(E) \cap K_q(E)$ or $K_p(E') \cap K_q(E')$ is nonabelian, then*

$$\lambda = 3 \quad \textit{and} \quad \{p,q\} = \{2,3\},$$

and the nonabelian Galois group is S_3.

Proof. Assume, after replacing ϕ by its dual if necessary, that $K_p(E) \cap K_q(E)$ is nonabelian, and relabel the primes so that $p = \lambda$. The Galois group T of the intersection is a quotient of the mod λ Borel image. It is therefore solvable, with $[T,T] \simeq C_\lambda$ by lemma 2.2. It is also a quotient of the mod q image. Apply proposition 3.5 and exclude $(3,5)$ by lemma 3.6. At $q = 2$, the only possible nonabelian quotient is S_3. □

3.3. **Excluding simultaneous nonabelian $(2,3)$-entanglements.** To determine the exceptional $(2,3)$ transition, we first show that both endpoints of a rational 3-isogeny cannot have nonabelian $(2,3)$-entanglement.

Lemma 3.8. *Let $H \subseteq \mathsf{B}(3)$ admit a surjection $\pi : H \twoheadrightarrow S_3$. The projective map $H \longrightarrow \mathsf{B}(3)/\{\pm I\} \simeq S_3$ is surjective, and $\ker \pi = H \cap \{\pm I\}$. Thus, π differs from the projective map only by an automorphism of S_3.*

Proof. Since $|\mathsf{B}(3)| = 12$, the order of H is 6 or 12. If $|H| = 6$, then $H \simeq S_3$ has trivial center, so $-I \notin H$. The projective map is then injective and has image of order 6. If $|H| = 12$, then $H = \mathsf{B}(3)$. The normal subgroup $\ker \pi$ has order two and therefore lies in the center. Since the center of $\mathsf{B}(3)$ is $\{\pm I\}$, this is its kernel. In either case, the two surjections have the same kernel and differ by an automorphism of their common target. □

Jones and McMurdy construct a genus zero modular curve X_{18} of level 18 whose associated family satisfies $K_2(E) \subseteq K_9(E)$ [11, Section 3.5].

Proposition 3.9. *Let $\phi : E \to E'$ be a rational 3-isogeny, and choose a basis of $T_3(E)$ whose first vector reduces to a generator of $\ker\phi$. Let $B_9 \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ be the inverse image of $\mathsf{B}(3)$ under reduction mod 3. Then the projective mod 3 representation of E' is obtained from the mod 9 representation of E via*

$$\Theta : B_9 \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3), \qquad \begin{pmatrix} a & b \\ 3c & d \end{pmatrix} \longmapsto \left[\begin{pmatrix} \bar{a} & 0 \\ \bar{c} & \bar{d} \end{pmatrix} \right].$$

In particular, if ϕ is the rational 3-isogeny parametrized by a noncuspidal rational point on X_{18} with non-CM j-invariant, then $K_2(E) \subseteq K_3(E')$.

Proof. Write $T_3(E) = \mathbb{Z}_3 e_1 \oplus \mathbb{Z}_3 e_2$, where the reduction of e_1 generates $\ker\phi$. The isogeny identifies $T_3(E) \otimes \mathbb{Q}_3$ with $T_3(E') \otimes \mathbb{Q}_3$, under which $T_3(E') = \mathbb{Z}_3(e_1/3) \oplus \mathbb{Z}_3 e_2$.

For $\sigma \in G_{\mathbb{Q}}$, suppose its action on $T_3(E)$ is represented by $g = \left(\begin{smallmatrix} a & b \\ 3c & d \end{smallmatrix}\right)$. In the corresponding basis of $T_3(E')$, the action of σ is represented by $g' = \left(\begin{smallmatrix} a & 3b \\ c & d \end{smallmatrix}\right)$. Reducing g' mod 3 and projectivizing yields the map Θ. This map is well-defined mod 9, since the lower-left entry of g determines c mod 3.

The kernel of Θ is $N_9 = \left\{ \left(\begin{smallmatrix} a & b \\ \gamma & d \end{smallmatrix}\right) \in B_9 : \gamma \equiv 0 \pmod 9, \quad a \equiv d \pmod 3 \right\}$. Its image is the full projective lower-triangular subgroup of $\mathrm{PGL}_2(\mathbb{F}_3)$, which has order 6 and is isomorphic to S_3.

By [11, Section 3.5], the group defining X_{18} is, up to conjugacy, the fiber product $G_{18} := \mathrm{GL}_2(\mathbb{F}_2) \times_{B_9/N_9} B_9$, where the first map is an isomorphism $\mathrm{GL}_2(\mathbb{F}_2) \simeq B_9/N_9$.

Since $-I \in N_9$, the scalar $-I$ belongs to G_{18} under the isomorphism $\mathrm{GL}_2(\mathbb{Z}/18\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{F}_2) \times \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. Thus, containment in G_{18} is preserved by quadratic twisting and depends only on the corresponding j-invariant.

For a rational point of X_{18}, choose compatible bases so that the mod 18 image of E is contained in G_{18}. The fiber product relation shows that the mod 2 representation of E and the projective mod 3 representation of E' have the same kernel. Thus, $\ker\rho_{E',3} \subseteq \ker\rho_{E,2}$, and hence $K_2(E) \subseteq K_3(E')$, as claimed. □

Proposition 3.10. *Let $E \to E'$ be a rational 3-isogeny between non-CM elliptic curves over $\mathbb{Q}$, and suppose that $(K_2(E') \cap K_3(E'))/\mathbb{Q}$ is nonabelian. Then $j(E)$ lies in the image of $X_{18}(\mathbb{Q})$.*

Proof. By lemma 2.1, $K_2(E) = K_2(E')$. Since $\mathrm{Gal}(K_2(E')/\mathbb{Q})$ is a subgroup of S_3, its only possible nonabelian quotient is S_3. The hypothesis therefore yields

$$L := K_2(E) = K_2(E') = K_2(E') \cap K_3(E')$$

with $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$.

By lemma 3.8, the restriction map from the mod 3 image of E' onto $\mathrm{Gal}(L/\mathbb{Q})$ is its projective quotient, up to an automorphism of S_3. By proposition 3.9, this projective representation is obtained from the mod 9 image of E by applying Θ. Hence, the mod 18 image of E is contained in the fiber product identifying these two S_3 quotients.

Every automorphism of S_3 is inner, so the choice of identification changes the fiber product only by conjugacy. Thus, the mod 18 image of E is contained in a conjugate of G_{18}. By the modular interpretation, this corresponds to a rational point on X_{18} with j-invariant $j(E)$. □

On $X_0(3)$, choose the parameter t for which $j_0(t) = (t+27)(t+243)^3/t^3$. Jones–McMurdy's parameter u on X_{18} satisfies $t = -27/(u^3-1)^2$ (see [11, Theorem 3.13]). For the rational

3-isogeny $E \to E'$ parametrized by u, denote the j-invariants of E and E' by $j_{18}(u)$ and $j_{18}^{\vee}(u)$, respectively. Then

$$j_{18}(u) = -27\frac{u^3(u^3-2)(3u^3-4)^3(3u^3-2)^3}{(u^3-1)^2}, \tag{3.1}$$

while $j_{18}^{\vee}(u) = (t+27)(t+3)^3/t$.

For any such rational point with $\mathrm{Gal}(K_2(E)/\mathbb{Q}) \simeq S_3$, proposition 3.9 gives $K_2(E') \cap K_3(E') = K_2(E') = K_2(E)$. We next show that the intersection at E cannot also be this field.

The Brau–Jones curve $X'(6)$ parametrizes elliptic curves with $K_2(E) \subseteq K_3(E)$. Its j-map is $j_6(v) = 2^{10}3^3v^3(1-4v^3)$. To compare this map with (3.1), we use Fermat's Last Theorem for exponent 3: $X^3 + Y^3 = Z^3$ has no solution in nonzero integers [10, Chapter 17].

Lemma 3.11. (1) *The equation $x^3 - y^3 = 1$ has exactly two rational solutions, $(1,0)$ and $(0,-1)$.*
(2) *The affine curve $(x^3-1)(y^3-1) = -1$ has no rational points.*

Proof. Clearing denominators in $x^3 - y^3 = 1$ and applying Fermat's Last Theorem shows that x or y must be zero, giving the two stated solutions.

For the second assertion, write $x = a/b$ in lowest terms, with $b > 0$. The equation forces $x^3 \neq 1$ and $y^3 = \frac{a^3-2b^3}{a^3-b^3}$. The numerator and denominator are coprime: a common divisor divides b^3 and a^3, hence is 1. Writing $y = c/d$ in lowest terms with $d > 0$, we obtain $a^3 - 2b^3 = \varepsilon c^3$ and $a^3 - b^3 = \varepsilon d^3$ for $\varepsilon \in \{\pm 1\}$. If $a = 0$, the original equation gives $y^3 = 2$, which is impossible in $\mathbb{Q}$. Thus a, b, d are all nonzero. When $\varepsilon = 1$, the second identity gives $a^3 = b^3 + d^3$; when $\varepsilon = -1$, it gives $b^3 = a^3 + d^3$. Both contradict Fermat's Last Theorem. □

Theorem 3.12. *Two non-CM elliptic curves over $\mathbb{Q}$ connected by a rational 3-isogeny cannot both have nonabelian $(2,3)$-entanglement.*

Proof. Suppose that $E \to E'$ is such an isogeny and both intersections are nonabelian. By proposition 3.10, $j(E) = j_{18}(u)$ for some $u \in \mathbf{P}^1(\mathbb{Q})$. The containment $K_2(E) \subseteq K_3(E)$ also means $j(E) = j_6(v)$ for some $v \in \mathbb{Q}$. Since $u = 1$ and $u = \infty$ are poles of j_{18}, neither can occur.

Factoring the numerator of $j_6(v) - j_{18}(u)$ gives two possibilities: $v^3 = \frac{u^3(3u^3-4)^3}{64(u^3-1)}$ or $v^3 = -\frac{(u^3-2)(3u^3-2)^3}{64(u^3-1)}$. In the first case, $v = 0$ would force $u = 0$, since $4/3$ is not a rational cube. This means $j(E) = 0$, contrary to the non-CM hypothesis. We may therefore set $w = u(3u^3-4)/(4v)$, which implies $w^3 = u^3 - 1$. By lemma 3.11, the only possibilities are $(u,w) = (1,0)$ or $(0,-1)$, which are both already excluded.

In the second case, $3u^3 - 2 \neq 0$ for rational u, so set $w = -4v/(3u^3-2)$. Then $w^3 = (u^3-2)/(u^3-1)$, and hence $(u^3-1)(w^3-1) = -1$, which contradicts lemma 3.11. □

3.4. **The exceptional $(2,3)$ transition.**

Lemma 3.13. *Let $\phi : E \to E'$ be a rational 3-isogeny between non-CM elliptic curves over $\mathbb{Q}$, and suppose that $K_2(E) \cap K_3(E)$ is nonabelian over $\mathbb{Q}$. Then*

$$K_2(E) \cap K_3(E) = K_2(E), \quad \textit{and} \quad \mathrm{Gal}(K_2(E)/\mathbb{Q}) \simeq S_3,$$

and the unique quadratic subfield of $K_2(E)$ is $W := \mathbb{Q}(\sqrt{-3})$. Moreover, $W \subseteq K_2(E') \cap K_3(E')$.

Proof. The group $\mathrm{Gal}(K_2(E)/\mathbb{Q})$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$. The only such subgroup with a nonabelian quotient is S_3 itself, and its only nonabelian quotient is S_3. Since $K_2(E) \cap K_3(E)$ is Galois over $\mathbb{Q}$, it follows that $K_2(E) \cap K_3(E) = K_2(E)$ and $\mathrm{Gal}(K_2(E)/\mathbb{Q}) \simeq S_3$.

Choose a basis of $E[3]$ whose first vector spans $\ker \phi$, and let $H_3 \subseteq \mathsf{B}(3)$ be the mod 3 image. Restriction gives $\pi : H_3 \twoheadrightarrow \mathrm{Gal}(K_2(E)/\mathbb{Q}) \simeq S_3$. The sign character calculation in the proof of lemma 3.6 applies to any such quotient and yields $\mathrm{sgn} \circ \pi = \det$. Composing with $\rho_{E,3}$ identifies the unique quadratic subfield of $K_2(E)$ with $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$.

Finally, $K_2(E') = K_2(E)$ by lemma 2.1, and the Weil pairing implies $W = \mathbb{Q}(\zeta_3) \subseteq K_3(E')$. Therefore, $W \subseteq K_2(E') \cap K_3(E')$. □

Theorem 3.14. *Let $E \to E'$ be a rational 3-isogeny between non-CM elliptic curves over $\mathbb{Q}$, and suppose that either E or E' has nonabelian $(2,3)$-entanglement. Then*

$$K_2(E) = K_2(E') =: L, \quad \textit{with} \quad \mathrm{Gal}(L/\mathbb{Q}) \simeq S_3,$$

and

$$\{K_2(E) \cap K_3(E), K_2(E') \cap K_3(E')\} = \{L, \mathbb{Q}(\sqrt{-3})\}.$$

Both orderings occur for infinitely many rational 3-isogenies with pairwise distinct source j-invariants.

Proof. Use the dual isogeny if necessary so that $K_2(E) \cap K_3(E)$ is nonabelian. By lemmas 2.1 and 3.13, $L := K_2(E) = K_2(E')$ is an S_3-extension, $K_2(E) \cap K_3(E) = L$, and $W := \mathbb{Q}(\sqrt{-3}) \subseteq K_2(E') \cap K_3(E')$. The only Galois subfields of $L/\mathbb{Q}$ are $\mathbb{Q}$, W, and L. The containment excludes $\mathbb{Q}$, while theorem 3.12 excludes L. Therefore, $K_2(E') \cap K_3(E') = W$.

For the infinite claim, take a model $\mathcal{E}/\mathbb{Q}(u)$ of the Jones–McMurdy level 18 family. The 2-division field has Galois group S_3 over $\mathbb{Q}(u)$ [11, Theorem 3.13]. Hilbert irreducibility applied to $\mathbb{Q}(u)(\mathcal{E}[2])/\mathbb{Q}(u)$ yields infinitely many rational specializations with the same 2-division Galois group, after excluding the finitely many bad parameters. For each specialization, proposition 3.9 gives the S_3-intersection at E', while lemma 3.13 and theorem 3.12 show that the intersection at E is W.

Since j_{18} is nonconstant and has finite fibers, these specializations yield infinitely many distinct source j-invariants. We may discard the finitely many CM j-invariants over $\mathbb{Q}$. The map $j_{18}^\vee$ is also nonconstant, so taking dual isogenies gives infinitely many distinct source j-invariants in the other orientation. □

Example 3.15. At $u = -1$, the level 18 family gives a rational 3-isogeny from 486d1 to 486d2 [20]. For $E = 486d1$, the 2-division polynomial $f(x) = 4x^3 - 3x^2 - 78x - 115$ is irreducible mod 7 and has discriminant $-3 \cdot 72^2$. Hence, $\mathrm{Gal}(K_2(E)/\mathbb{Q}) \simeq S_3$. By proposition 3.9 and theorem 3.14, the $(2,3)$-intersection fields at 486d1 and 486d2 are $\mathbb{Q}(\sqrt{-3})$ and $K_2(E)$, respectively.

3.5. **Isogenies of odd composite degree.** For $a \in \mathbb{Q}^\times$, write $[a]$ for its class in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.

Lemma 3.16. *A non-CM elliptic curve over $\mathbb{Q}$ admitting two distinct rational 3-isogenies does not have discriminant squareclass $[-3]$.*

Proof. Such a curve has mod 3 image contained in a split Cartan. The standard parameter [22, Theorem 1.2] gives $J_s(t) = 27\frac{(t+1)^3(t+3)^3(t^2+3)^3}{t^3(t^2+3t+3)^3}$. Direct factorization then yields $J_s(t) - 1728 = 27\frac{(t^2-3)^2(t^4+6t^3+18t^2+18t+9)^2}{t^3(t^2+3t+3)^3}$.

The identity $j - 1728 = c_6^2/\Delta$ shows that the discriminant squareclass is $[3t(t^2+3t+3)]$. Equality with $[-3]$ requires $y^2 = -t(t^2+3t+3)$. Setting $x = -t-1$ gives $y^2 = x^3+1$. Its rational points are $O, (-1,0), (0,\pm 1), (2,\pm 3)$, as recorded in section A. The resulting values $t = 0, -1, -3, \infty$ are cuspidal or give $j = 0$. □

Proposition 3.17. *Every rational cyclic isogeny of odd composite degree between non-CM elliptic curves preserves $F_{p,q}$ for every distinct prime pair. Moreover, a nonconstant $(2,3)$ pattern across a 3-edge can occur only on the exact graph $L_2(3)$.*

Proof. The only possible non-CM odd composite cyclic degrees are $9, 15, 21, 25$ [4, Theorem 4.6 and Remark 5.19]. A change across an odd-prime edge requires degree 3 and the pair $\{2,3\}$, by theorems 2.3 and 3.14 and corollary 3.7. This already proves the assertion for degree 25.

For 9, factor the isogeny as $E_0 \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} E_2$, with both maps of degree 3. Since the composite is cyclic, $\ker \phi_2 \neq \ker \widehat{\phi_1}$. Thus, E_1 admits two distinct rational 3-isogenies, and so its mod 3 image is contained in a split Cartan and $K_3(E_1)$ is abelian.

All three curves have the same 2-division field. If either outer curve had a nonabelian $(2,3)$-intersection, lemma 3.13 would force the common discriminant squareclass to be $[-3]$, contradicting lemma 3.16. The middle curve cannot have a nonabelian intersection since $K_3(E_1)$ is abelian. All intersections at $(2,3)$ are therefore abelian, and odd-prime abelian invariance identifies them. Every other pair is unchanged by theorem 2.3, corollary 3.7, and lemma 2.1.

For 15 and 21, [1, Table 6] provides models, up to quadratic twist, for all curves admitting rational cyclic 15 or 21-isogenies. Substitution of its eight models $y^2 = x^3 + Ax + B$ gives the discriminant squareclass $[-16(4A^3 + 27B^2)] = [-2]$. The squareclass does not change under quadratic twisting. Since every vertex has a rational 3-isogeny, a nonabelian $(2,3)$-intersection would again require $[-3]$. Thus, all such intersections are abelian and are preserved along the graph. Other pairs are already invariant.

Finally, an S_3 2-division field excludes every graph with rational 2-torsion. A graph containing a 3-edge but no 2-edge is $L_2(3)$, $L_3(9)$, $R_4(15)$ or $R_4(21)$ in the non-CM case [4, Theorem 1.2]. The exclusions above leave only $L_2(3)$. □

4. Quadratic intersections in isogeny classes

Now that we have determined the possible changes in prime-level entanglements under odd-degree isogenies, we consider classes containing a rational 2-isogeny. In this case, the 2-division fields have degree at most two.

Proposition 4.1. *Let $\mathcal{C}$ be a rational isogeny class with a rational 2-isogeny, and let q be an odd prime. For every $E \in \mathcal{C}$,*

$$F_{2,q}(E) = K_2(E) \cap A_q(\mathcal{C}) = \mathbb{Q}(\sqrt{\Delta_E}) \cap A_q(\mathcal{C}),$$

where Δ_E is the discriminant of a Weierstrass equation for E. In particular, $F_{2,q}$ is unchanged along every odd-prime edge of $\mathcal{G}(\mathcal{C})$, and it is $\mathbb{Q}$ at every core vertex.

Proof. Since every curve $E \in \mathcal{C}$ has rational 2-torsion, $K_2(E)$ has degree at most two over $\mathbb{Q}$ and is generated by $\sqrt{\Delta_E}$. Hence, intersecting $K_2(E)$ with $K_q(E)$ is the same as intersecting it with $A_q(E) = A_q(\mathcal{C})$.

By lemma 2.1, K_2 is preserved along odd-prime edges, so $F_{2,q}$ is also preserved. At a core vertex, all 2-torsion is rational, so $K_2(E) = \mathbb{Q}$, and consequently $F_{2,q}(E) = \mathbb{Q}$. □

We first study the possible intersection fields across a single rational 2-isogeny $E \to E'$. Write $F = F_{2,q}(E)$ and $F' = F_{2,q}(E')$. Table 1 summarizes the possibilities established in this section and Sections 5–7. We later use these results to classify the patterns on entire isogeny graphs.

The table uses the following notation. Recall that $W_q = \mathbb{Q}(\sqrt{q^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_q)$.

For $q = 3$: When the mod 3 Galois image is conjugate to $\mathsf{B}(3)$ or $C_{\mathrm{s}}(3)$, the fields M and M' denote the two quadratic subfields of $K_3(E)$ other than W_3. When the image is conjugate to $N_{\mathrm{s}}(3)$ or $N_{\mathrm{ns}}(3)$, we use $M_{\mathrm{s}}, M'_{\mathrm{s}}$ or $M_{\mathrm{ns}}, M'_{\mathrm{ns}}$, respectively, for the two non-Weil quadratic subfields. In the nonsplit case, M_{ns} is the field defined by the character $N_{\mathrm{ns}}(3)/C_{\mathrm{ns}}(3)$, so the two non-Weil labels are not interchangeable.

For $q = 5$: When the mod 5 image is contained in a Borel, $K_5(E)$ has either one or three quadratic subfields. When there are three, T_5 and T'_5 denote the two other than W_5.

In the second column of table 1, subgroup names refer to the exact mod q image up to conjugacy, unless containment is explicitly stated.

q	mod q case	Possible nontrivial values of F and F'	Restrictions on (F, F')
$q \geq 7$	$\mathrm{GL}_2(\mathbb{F}_q)$	W_q	(W_q, W_q) is excluded when $q \equiv 3 \pmod 4$.
3	$K_3(E)$ has one quadratic subfield	W_3	At most one of F and F' is nontrivial.
3	$\mathsf{B}(3)$ or $C_{\mathrm{s}}(3)$	W_3, M, M'	If F and F' are both nontrivial, they are distinct and exactly one is W_3.
3	$N_{\mathrm{s}}(3)$	$M_{\mathrm{s}}, M'_{\mathrm{s}}$	At most one of F and F' is nontrivial.
3	$N_{\mathrm{ns}}(3)$	$M_{\mathrm{ns}}, M'_{\mathrm{ns}}$	$(M_{\mathrm{ns}}, M_{\mathrm{ns}})$ is excluded.
5	$\mathrm{GL}_2(\mathbb{F}_5)$	W_5	No further restriction.
5	Contained in $\mathsf{B}(5)$	T_5, T'_5 when present	At most one of F and F' is nontrivial.

TABLE 1. The possible $(2, q)$-intersection fields for a rational 2-isogeny. The value $\mathbb{Q}$ is also allowed for either entry.

4.1. The 2-division fields.

Proposition 4.2. *Let $E : y^2 = x^3 + Ax^2 + Bx$ be nonsingular, and let $D := A^2 - 4B$. The quotient by $(0, 0)$ has the model*

$$E' : y^2 = x^3 - 2Ax^2 + Dx. \tag{4.1}$$

Moreover,

$$K_2(E) = \mathbb{Q}(\sqrt{D}) \quad \text{and} \quad K_2(E') = \mathbb{Q}(\sqrt{B}). \tag{4.2}$$

Proof. The model of the quotient is the standard degree 2 case of Vélu's formulas [21]. The remaining nonzero 2-torsion of E is cut out by $x^2 + Ax + B$, whose discriminant is D. For E', it is cut out by $x^2 - 2Ax + D$, whose discriminant is $16B$. Finally, $\Delta_E = 16B^2D$ and $\Delta_{E'} = 256BD^2$, so the discriminant squareclasses are $[D]$ and $[B]$. □

Proposition 4.3. *Every non-CM elliptic curve over $\mathbb{Q}$ with a chosen rational 2-isogeny is $\mathbb{Q}$-isomorphic to a curve*

$$E_{s,u} : y^2 = x^3 + u(s+4)x^2 + u^2(s+4)x \tag{4.3}$$

for some $u \in \mathbb{Q}^\times$ and $s \in \mathbb{Q} \setminus \{0, -4\}$. The j-invariant of $E_{s,u}$ and the 2-division fields of $E_{s,u}$ and its 2-isogenous quotient are

$$j(E_{s,u}) = 256\frac{(s+1)^3}{s}, \tag{4.4}$$

and

$$K_2(E_{s,u}) = \mathbb{Q}\left(\sqrt{s(s+4)}\right) \quad \text{and} \quad K_2(E'_{s,u}) = \mathbb{Q}\left(\sqrt{s+4}\right). \tag{4.5}$$

Proof. Start with a model $E : y^2 = x^3 + Ax^2 + Bx$ as in proposition 4.2. Since E is non-CM, $A \neq 0$. The case $A = 0$ has $j = 1728$. Set $s := (A^2 - 4B)/B$ and $u := B/A$. Then $s+4 = A^2/B$, so $u(s+4) = A$ and $u^2(s+4) = B$, giving (4.3). Nonsingularity implies $s \neq 0$, while $s = -4$ would force $A = 0$. The formulas (4.4) and (4.5) follow from the standard invariants and proposition 4.2. □

For brevity, write $F_q(E) = F_{2,q}(E)$. Since $K_2(E)$ has degree at most two, $F_q(E)$ is nontrivial precisely when $K_2(E)$ is a quadratic subfield of $K_q(E)$, in which case $F_q(E) = K_2(E)$. In particular, $F_q(E) = W_q$ precisely when $K_2(E) = W_q$.

4.2. **The one quadratic-field case.** If the mod q image contains $\mathrm{SL}_2(\mathbb{F}_q)$, the surjectivity of the determinant implies it is $\mathrm{GL}_2(\mathbb{F}_q)$, and $A_q(E) = \mathbb{Q}(\zeta_q)$ by [5, Corollary 5.3]. Thus W_q is then the only possible nontrivial quadratic intersection.

Proposition 4.4. *Let $E/\mathbb{Q}$ be non-CM and suppose it admits a rational 2-isogeny. Then $\rho_{E,q}$ is surjective for every prime $q \geq 7$. At $q = 5$, its image is either $\mathrm{GL}_2(\mathbb{F}_5)$ or contained in a Borel.*

Proof. Let p be the largest prime degree of a rational isogeny from E. If $p > 2$, the chosen 2-isogeny and a p-isogeny yield a rational cyclic subgroup of order $2p$. The classification of rational cyclic isogenies implies $p \in \{3, 5\}$ [12]. Thus, $p \in \{2, 3, 5\}$. The three cases are covered by [9, Propositions 18, 19, and 20], respectively, and each gives surjectivity for every $q \geq 7$.

At $q = 5$, Dickson's classification puts a proper image in a Borel, a Cartan normalizer, or an exceptional subgroup. The non-Borel possibilities on the rational 2-isogeny locus are excluded by the rational point calculations on $X_0(2) \times X_{S_4}(5)$ and $X_0(2) \times X_{\mathrm{ns}}^+(5)$ in the proof of [9, Proposition 18]. The split-normalizer case is contained in the S_4 case. □

Proposition 4.5. *Let q be an odd prime, and let $E \to E'$ be a rational 2-isogeny between non-CM elliptic curves over $\mathbb{Q}$. Suppose that W_q is the unique quadratic subfield of $K_q(E)$. Then*

$$(F_q(E), F_q(E')) \in \{\mathbb{Q}, W_q\}^2,$$

with (W_q, W_q) excluded when $q \equiv 3 \pmod 4$. For every odd prime q, each allowed pair occurs for infinitely many distinct source j-invariants with exact mod q image $\mathrm{GL}_2(\mathbb{F}_q)$.

Proof. We use the family $E_{s,u}$ of proposition 4.3, and write $w = q^*$. By (4.5), the source and target intersections equal W_q precisely when $s(s+4) \in w\mathbb{Q}^{\times 2}$ and $s+4 \in w\mathbb{Q}^{\times 2}$, respectively. If $q \equiv 3 \pmod 4$, then $w < 0$. If both conditions held, $s(s+4)$ and $s+4$ would be negative, so $s > 0$, contradicting $s + 4 < 0$. Thus (W_q, W_q) is impossible.

The conditions at the source and target are parametrized by $s = 4/(wr^2 - 1)$ and $s = wr^2 - 4$, respectively. In the first family, $s(s + 4) = w(4r/(wr^2 - 1))^2$, and the target intersection is also W_q precisely when $wr^2 - 1$ is a square. In the second family, the source intersection is also W_q precisely when $wr^2 - 4$ is a square. These additional conditions define nontrivial double covers of the r-line. The pair $(\mathbb{Q}, \mathbb{Q})$ occurs on the s-line after excluding the square conditions $s(s+4)/w \in \mathbb{Q}^{\times 2}$ and $(s+4)/w \in \mathbb{Q}^{\times 2}$, which likewise define nontrivial double covers.

If $q \equiv 1 \pmod 4$, the simultaneous conditions are $s = v^2$ and $v^2 + 4 = qr^2$. Write $q = a^2 + b^2$ with b even. Then $(v, r) = (2a/b, 2/b)$ is a rational point on this conic, so the conic is rational. The j-map is nonconstant on each of these parameter families.

For $q \geq 7$, proposition 4.4 shows that every non-CM curve in these families has mod q image $\mathrm{GL}_2(\mathbb{F}_q)$. By lemma 2.6, each family contains infinitely many curves with distinct j-invariants satisfying the required squareclass conditions, after excluding singular and CM curves.

For $q = 3, 5$, take $u = 1$ and the values of s in table 2. We verify that the mod q images are full, so that W_q is the only quadratic subfield of $K_q(E)$.

q	$(F_q(E), F_q(E'))$	s
3	$(\mathbb{Q}, \mathbb{Q})$	1
3	$(W_3, \mathbb{Q})$	$-4/13$
3	$(\mathbb{Q}, W_3)$	-7
5	$(\mathbb{Q}, \mathbb{Q})$	$1/3$
5	$(W_5, \mathbb{Q})$	5
5	$(\mathbb{Q}, W_5)$	$-4/5$
5	(W_5, W_5)	$16/121$

TABLE 2. Examples with full mod q image at $q = 3, 5$.

For the three $q = 3$ curves, the 3-division quartics have a 4-cycle mod $11, 5, 5$ and a 3-cycle mod $7, 19, 19$, respectively. Thus, their Galois groups are S_4. The central extension $1 \to \{\pm I\} \to \mathrm{GL}_2(\mathbb{F}_3) \to S_4 \to 1$ does not split: a splitting would yield an A_4 subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$, but $\mathrm{SL}_2(\mathbb{F}_3)$ has only one involution. Hence, each mod 3 image is $\mathrm{GL}_2(\mathbb{F}_3)$.

For the four $q = 5$ curves, the 5-division polynomial is irreducible, which excludes a rational 5-isogeny. Their j-invariants are nonintegral, and so the curves are non-CM, and from proposition 4.4 $\mathrm{GL}_2(\mathbb{F}_5)$ is the mod 5 image. The accompanying code verifies these factorizations.

The intersection fields in the table now follow from (4.5). Each example lies in the corresponding rational parameter family and satisfies the nonsquare conditions needed to exclude the other intersection fields. Applying lemma 2.6 to these families yields infinitely many distinct j-invariants with each listed pair, after excluding singular and CM curves. □

5. Rational 3-isogenies and the mixed graphs

For $q = 3$, the cases where $K_3(E)$ has only one quadratic subfield are covered by proposition 4.5. When $K_3(E)$ has three quadratic subfields, either E admits a rational 3-isogeny or its mod 3 image is a split or nonsplit Cartan normalizer. We treat the former here and the latter in section 6.

We first classify the possible $(2, 3)$-intersection fields across a rational 2-isogeny using a family over $X_0(6)$. By section 2.2, the only non-CM rational isogeny graphs containing both 2 and 3-edges are $R_4(6)$, S, and $R_6(18)$. We then determine the $(2, q)$-intersection patterns on these graphs for every odd prime q.

5.1. **Curves with rational 2 and 3-isogenies.** A choice of rational 2 and 3-isogenies on an elliptic curve determines a rational cyclic subgroup of order 6. These choices are therefore parametrized by $X_0(6)$. We use an explicit family to compute the 2 division fields on either side of the 2-isogeny and compare them with the common 3-division field.

Proposition 5.1. *Every elliptic curve over $\mathbb{Q}$ with chosen rational 2 and 3-isogenies is $\mathbb{Q}$-isomorphic to a curve*

$$E_{t,u} : y^2 = x^3 + u(t^2 - 6t - 3)x^2 + 16u^2tx \tag{5.1}$$

for some $u \in \mathbb{Q}^\times$ and $t \in \mathbb{Q} \setminus \{0, 1, 9\}$. Conversely, every nonsingular curve in (5.1) admits rational 2 and 3-isogenies.

Proof. Set the kernel point of the rational 2-isogeny at $(0, 0)$ and complete the square to obtain a model $E : y^2 = x^3 + Ax^2 + Bx$ with $B(A^2 - 4B) \neq 0$. The 3-division polynomial of this model is $\psi_3(x) = 3x^4 + 4Ax^3 + 6Bx^2 - B^2$. Let $C_3 \subseteq E[3]$ be the chosen rational cyclic subgroup. Its two nonzero points are negatives of one another, so their common x-coordinate is rational. Write this coordinate as $4u$, with $u \in \mathbb{Q}^\times$, and set $t := B/(16u^2)$. Substituting $x = 4u$ into $\psi_3(x) = 0$ yields $3 + A/u + 6t - t^2 = 0$. Thus, $A = u(t^2 - 6t - 3)$ and $B = 16u^2t$, and so we get (5.1).

Conversely, on (5.1) we have $\psi_3(4u) = 0$, and the right-hand side at $x = 4u$ is $16u^3(t-1)^2$. Thus, the points

$$P_\pm = \left(4u,\ \pm 4u(t-1)\sqrt{u}\right) \tag{5.2}$$

are nonzero points of order 3, and the subgroup $\{O, P_+, P_-\}$ is Galois-stable. The point $(0, 0)$ yields the rational 2-isogeny.

The discriminant of this model is

$$\Delta(E_{t,u}) = 2^{12}u^6t^2(t-1)^3(t-9), \tag{5.3}$$

and so the curve is nonsingular precisely when $u \neq 0$ and $t \notin \{0, 1, 9\}$. Finally,

$$j(E_{t,u}) = \frac{(t-3)^3(t^3 - 9t^2 + 3t - 3)^3}{t^2(t-1)^3(t-9)}, \tag{5.4}$$

which is independent of u. The model with parameter u is the quadratic twist by u of the model with $u = 1$. □

Set $d = (t - 1)(t - 9)$, and let $E'_{t,u}$ be the quotient of $E_{t,u}$ by $(0, 0)$.

Lemma 5.2. *For the family (5.1),*

$$K_2(E_{t,u}) = \mathbb{Q}(\sqrt{d}), \quad K_2(E'_{t,u}) = \mathbb{Q}(\sqrt{t}), \quad \text{and} \quad A_3(E_{t,u}) = \mathbb{Q}(\sqrt{-3}, \sqrt{u}).$$

Consequently, with $V_u = \langle [-3], [u] \rangle$, the source and target intersections are nontrivial precisely when $[d]$ and $[t]$, respectively, belong to $V_u \setminus \{[1]\}$. If $[u] \notin \{[1], [-3]\}$, the three quadratic subfields are $W = \mathbb{Q}(\sqrt{-3})$, $M = \mathbb{Q}(\sqrt{u})$, and $M' = \mathbb{Q}(\sqrt{-3u})$.

Proof. The coefficients in (5.1) satisfy $A^2 - 4B = u^2(t-1)^3(t-9)$ and $B = 16u^2t$, so proposition 4.2 yields the two 2-division fields. A generator P of the chosen 3-isogeny kernel in (5.2) has $\mathbb{Q}(P) = \mathbb{Q}(\sqrt{u})$. By lemma 2.2, $A_3(E_{t,u})$ is the field cut out by the diagonal characters of the mod 3 representation. One of these characters cuts out $\mathbb{Q}(P)$, and their product is the mod 3 cyclotomic character. Hence, $A_3(E_{t,u}) = \mathbb{Q}(P, \zeta_3)$. The conditions for the two intersections to be nontrivial follow by comparing squareclasses. □

We use the 3-division polynomial of $E_{t,u}$ to give a sufficient condition for its mod 3 image to be the full Borel subgroup.

Lemma 5.3. *For $f_t(z) = 3z^3 + (t^2 - 6t)z^2 + t^2z + t^2$, we have*

$$\psi_3(4uz) = 256u^4(z-1)f_t(z), \tag{5.5}$$

$$\operatorname{disc}(f_t) = -3t^4(t-1)^2(t-9)^2. \tag{5.6}$$

If f_t is irreducible over $\mathbb{Q}$ and $[u] \notin \{[1], [-3]\}$, then $\rho_{E_{t,u},3}(G_{\mathbb{Q}}) = \mathsf{B}(3)$.

Proof. The identities follow by expansion. The root $z = 1$ corresponds to the chosen rational 3-isogeny, while the roots of f_t correspond to the other three cyclic subgroups of order 3 in $E[3]$. If f_t is irreducible, its nonsquare discriminant yields the full projective Borel $\mathsf{B}(3)/\{\pm I\} \simeq S_3$. The mod 3 image therefore has order 6 or 12. The independent diagonal characters defining $\mathbb{Q}(\sqrt{u})$ and $\mathbb{Q}(\sqrt{-3u})$ give a quotient of order four, and so the mod 3 image has order 12 and is the full Borel. □

5.2. **The $(2,3)$-intersection patterns on $X_0(6)$.** Write $d = (t-1)(t-9)$. By lemma 5.2, the two intersection fields are determined by the squareclasses $[d]$ and $[t]$. If both intersections are nontrivial, equality requires $[dt] = [1]$. If they are distinct and neither is W_3, they must be the two non-Weil quadratic subfields, so $[dt] = [-3]$. The following rational point calculation rules out both possibilities.

Proposition 5.4. *Let $C_0 : Y^2 = T(T-1)(T-9)$ and $C_{-3} : Y^2 = -3T(T-1)(T-9)$. Then*

$$C_0(\mathbb{Q}) = C_{-3}(\mathbb{Q}) = \{O, (0,0), (1,0), (9,0)\}.$$

Proof. The change of variables $x = -3T$ and $y = 3Y$ transforms C_{-3} into $y^2 = x(x+3)(x+27)$. By lemma A.2, the only rational points on either curve are the point at infinity and the three points of order 2. Translating back to T gives the stated points. □

Corollary 5.5. *If $t \in \mathbb{Q} \setminus \{0, 1, 9\}$ and $d = (t-1)(t-9)$, then*

$$[d] \neq [t]\,, \tag{5.7}$$

$$[dt] \neq [-3]\,. \tag{5.8}$$

Proof. The equality $[d] = [t]$ is equivalent to td being a square, and hence to the existence of a rational point on C_0 with T-coordinate t. By proposition 5.4, this means $t \in \{0, 1, 9\}$.

Similarly, $[dt] = [-3]$ is equivalent to $-3td$ being a square, and hence to a rational point on C_{-3} with T-coordinate t. By proposition 5.4, this requires $t \in \{0, 1, 9\}$, contrary to our hypothesis.

□

Theorem 5.6. *Let $E/\mathbb{Q}$ admit chosen rational 2 and 3-isogenies, and let E' be the quotient by the chosen rational 2-isogeny. If*

$$K_2(E) \cap K_3(E) \neq \mathbb{Q} \qquad \text{and} \qquad K_2(E') \cap K_3(E') \neq \mathbb{Q},$$

then the two intersection fields are distinct, and exactly one is the Weil field $\mathbb{Q}(\sqrt{-3})$.

Proof. Write $E = E_{t,u}$ as in proposition 5.1, and set $d = (t-1)(t-9)$. By lemma 5.2, $[d]$ and $[t]$ are nonidentity elements of $V_u = \langle [-3], [u] \rangle$. They are distinct by (5.7), and so V_u has order four, with nonidentity elements $[-3]$, $[u]$, and $[-3u]$. If neither class were $[-3]$, their product would be $[-3]$, contradicting (5.8). Thus, exactly one intersection field is $\mathbb{Q}(\sqrt{-3})$. □

For exact mod 3 image $\mathsf{B}(3)$, we have $[u] \notin \{[1], [-3]\}$, and so the fields W, M, M' in lemma 5.2 are distinct.

Theorem 5.7. *The possible ordered pairs $(K_2(E) \cap K_3(E), K_2(E') \cap K_3(E'))$ for a rational 2-isogeny edge with exact mod 3 image $\mathsf{B}(3)$ are exactly*

$$(\mathbb{Q}, \mathbb{Q}), \quad (W, \mathbb{Q}), \ (\mathbb{Q}, W), \quad (M, \mathbb{Q}), \ (M', \mathbb{Q}), \ (\mathbb{Q}, M), \ (\mathbb{Q}, M'),$$
$$(W, M), \ (W, M'), \ (M, W), \ (M', W).$$

Every pair in this list occurs for infinitely many distinct j-invariants of non-CM elliptic curves over $\mathbb{Q}$ with exact mod 3 image $\mathsf{B}(3)$.

Proof. Theorem 5.6 excludes the three equal nontrivial pairs and the two pairs of distinct non-Weil fields, leaving exactly the displayed list.

Let $d = (t-1)(t-9)$. From table 3 we get a rational family and an explicit choice of (t, u) for each pattern, with u taken up to multiplication by a nonzero rational square. The field claims follow from lemma 5.2. For $t = 2, 7, -12$, the polynomial f_t is irreducible mod $13, 13, 19$, respectively, and every listed u has $[u] \notin \{[1], [-3]\}$. Thus, lemma 5.3 gives the full Borel image. The three j-invariants are nonintegral.

For the pair $(\mathbb{Q}, \mathbb{Q})$, choose t and u so that neither $[d]$ nor $[t]$ belongs to $V_u \setminus \{[1]\}$. These restrictions exclude only finitely many squareclass conditions. For the families with $d = -3r^2$, the conic $(t-1)(t-9) = -3r^2$ has the rational point $(t, r) = (7, 2)$ and is therefore rational; the relation $t = -3r^2$ is already rationally parametrized. In each family, the specialization in table 3 satisfies none of the unwanted field equalities. Their defining functions are therefore nonsquares. Since the j-map (5.4) is nonconstant, lemma 2.6 gives infinitely many distinct j-invariants with the stated pattern and exact image, after excluding the singular and CM parameters. □

We now determine the $(2, q)$-intersection patterns on the mixed isogeny graphs $R_4(6)$, S, and $R_6(18)$. Since the intersection fields are preserved under 3-isogenies, we need only determine how they can differ across 2-isogenies.

Pattern	Family	(t,u)
$(\mathbb{Q},\mathbb{Q})$	t,u free	$(2,3)$
$(M,\mathbb{Q})$	$u=d$	$(2,-7)$
$(M',\mathbb{Q})$	$u=-d/3$	$(2,21)$
$(\mathbb{Q},M)$	$u=t$	$(2,2)$
$(\mathbb{Q},M')$	$u=-t/3$	$(2,-6)$
$(W,\mathbb{Q})$	$d=-3r^2$	$(7,2)$
$(\mathbb{Q},W)$	$t=-3r^2$	$(-12,2)$
(W,M)	$d=-3r^2,\ u=t$	$(7,7)$
(W,M')	$d=-3r^2,\ u=-t/3$	$(7,-21)$
(M,W)	$t=-3r^2,\ u=d$	$(-12,273)$
(M',W)	$t=-3r^2,\ u=-d/3$	$(-12,-819)$

TABLE 3. Full-Borel families and specializations at $q=3$. Unwanted field matches are excluded in each family.

5.3. **The rectangle $R_4(6)$.** By proposition 4.1, the two endpoints of each 3-edge in $R_4(6)$ have the same intersection field. By lemma 5.2, the 2-division fields on the two 3-edges of $R_4(6)$ have squareclasses $[(t-1)(t-9)]$ and $[t]$, respectively.

At $q=3$, lemma 5.2 and theorem 5.6 give exactly the Borel possibilities in table 1. If $A_3(\mathcal{C})$ is biquadratic, the eleven pairs are those of theorem 5.7; if $A_3(\mathcal{C})=W_3$, at most one of the two fields is W_3.

For $q\geq 5$, the mod q image is full. For $q\geq 7$ this follows from proposition 4.4; a proper image at 5 would yield a rational 5-isogeny and hence a forbidden cyclic 30-isogeny. Thus, the only possible nontrivial field is W_q. The obstruction (5.7) rules out (W_q,W_q). Each one-sided condition is a rational curve: the target condition is $t=wr^2$, and the source condition is $(t-1)(t-9)=wr^2$, a conic with rational point $(t,r)=(1,0)$. After excluding the cusps and the unwanted match, these yield infinitely many distinct j-invariants. Section 9.1 excludes additional isogenies to obtain exactly $R_4(6)$.

5.4. **The graph S and cyclic degree 12.** To parametrize the curves in (5.1) with full rational 2-torsion, we require $(t-1)(t-9)$ to be a square. This means

$$t=\frac{r^2-9}{r^2-1},\qquad r\notin\{0,\pm1,\pm3\}. \tag{5.9}$$

The point at infinity on the r-line corresponds to $t=1$, which is a cusp.

The two core vertices of S are connected by a 3-isogeny, and the six remaining vertices form three pairs connected by 3-isogenies. Since K_2 is preserved under 3-isogenies, the two vertices in each pair have the same 2-division field. The corresponding squareclasses are

$$\begin{aligned} d_1(r)&=(r^2-9)(r^2-1),\\ d_2(r)&=r(r+3)(r-1),\\ d_3(r)&=-r(r-3)(r+1). \end{aligned} \tag{5.10}$$

Indeed, with $u = 1$, the nonzero roots of the cubic defining the chosen core curve are $a = \frac{4(r-1)(r+3)}{(r+1)^2}$ and $b = \frac{4(r-3)(r+1)}{(r-1)^2}$. Their sum is $-(t^2 - 6t - 3)$ and their product is $16t$. Applying equation (8.1) yields equation (5.10).

Lemma 5.8. *For noncuspidal rational r in equation (5.9), the three classes $[d_i(r)]$ are distinct, none is $[1]$ or $[-3]$, and no product of two of them is $[-3]$.*

Proof. Their product is minus a square. The transformations $r \mapsto -r$ and $r \mapsto (r+3)/(r-1)$ permute the three classes. More explicitly, for $h = (r+3)/(r-1)$, $d_1(h) = \frac{64d_3(r)}{(r-1)^4}$, $d_2(h) = \frac{16d_2(r)}{(r-1)^4}$, and $d_3(h) = \frac{4d_1(r)}{(r-1)^4}$. It suffices to show that, for every noncuspidal $r \in \mathbb{Q}$, the squareclass $[d_2(r)]$ is not in $\{[1], [-1], [3], [-3]\}$. The condition $[d_2(r)] = [e]$ is the curve $y^2 = e\,r(r+3)(r-1)$, where $e \in \{1, -1, 3, -3\}$.

Setting $X = er$, $Y = ey$ yields $Y^2 = X^3 + 2eX^2 - 3e^2X$. All four curves have rank zero. For $e = 1$ the rational points map to $r \in \{-3, -1, 0, 1, 3, \infty\}$. For the other three values only $r \in \{-3, 0, 1, \infty\}$ occur. These are all cusps, as verified in section A. Thus, the four squareclasses are excluded.

If two of the d_i had the same class, the remaining class would be $[-1]$. If the product of two were $[-3]$, the remaining class would be $[3]$. Both are impossible. □

At $q = 3$, lemma 5.8 shows that $[d_i(r)] \neq [-3]$ for $i = 1, 2, 3$, so no non-core vertex has intersection field W_3. Recall that the two non-Weil quadratic fields, when present, are $M = \mathbb{Q}(\sqrt{u})$ and $M' = \mathbb{Q}(\sqrt{-3u})$. If two distinct squareclasses $[d_i(r)]$ and $[d_j(r)]$ gave nontrivial intersection fields, those fields would be M and M', whose squareclasses have product $[-3]$. This is also excluded by lemma 5.8. Choosing $u = d_i(r)$ or $u = -3d_i(r)$ gives intersection field M or M', respectively, at the two vertices of the corresponding 3-edge.

For $q \geq 5$, the mod q image is full. At $q = 5$, a rational 5-isogeny would yield a forbidden cyclic 30-isogeny, while for $q \geq 7$ surjectivity follows from proposition 4.4. Since the three squareclasses are distinct, at most one pair can have intersection field W_q. The symmetries in the proof of lemma 5.8 permute these classes, and so such an intersection occurs precisely when there is a noncuspidal rational point on $y^2 = w\,r(r+3)(r-1)$.

The substitution $X = wr$, $Y = wy$ identifies this curve with $\mathscr{E}_{12,q}$. By lemma A.1, its rational torsion subgroup is $C_2 \times C_2$, and all torsion points correspond to cusps. Hence, a nontrivial intersection occurs precisely when $r_{12}(q) > 0$. In particular, since $r_{12}(5) = 0$, all $(2, 5)$-intersections on S are trivial.

5.5. **The graph $R_6(18)$.** Each middle-column vertex of $R_6(18)$ has two distinct rational 3-isogenies. In the family (5.1), one is already chosen. A second exists precisely when the residual cubic $f_t(z)$ in lemma 5.3 has a rational root. Viewed as a quadratic in t, this polynomial has discriminant $-12z^3(z-1)^2$. Thus, a rational root has the form $z = -3v^2$. Solving for t yields

$$t = \frac{9v^3}{3v^2 - 3v + 1}, \qquad v \notin \{0, 1, 1/3\}. \tag{5.11}$$

The other choice is obtained by replacing v by $-v$. The point at infinity on the v-line also corresponds to a cusp.

The two horizontal 3-isogeny chains have 2-division fields with squareclasses

$$a(v) = (v-1)(3v-1)(3v^2+1) \quad \text{and} \quad b(v) = v(3v^2 - 3v + 1). \tag{5.12}$$

These follow by substituting (5.11) into $(t-1)(t-9)$ and t, respectively. The nonzero points in the two rational 3-isogeny kernels are defined over $\mathbb{Q}(\sqrt{u})$ and $\mathbb{Q}(\sqrt{-3u})$, respectively. Hence the quadratic subfields of $K_3(E)$ are determined by $\langle[-3],[u]\rangle$.

The middle-column vertices have mod 3 images contained in a split Cartan. By lemma 3.16, neither of their 2-division fields can be W_3. Thus, no vertex has intersection field W_3. The squareclass restrictions in corollary 5.5 exclude equal nontrivial fields on both rows, as well as the pair (M, M') in either order. Hence, at $q = 3$ at most one row has a nontrivial intersection, equal to M or M'. Neither row has trivial 2-division field, since $R_6(18)$ has no core vertices. Taking $u = a(v)$ or $u = -3a(v)$, and similarly with $b(v)$, yields the corresponding one-row patterns.

For $q \geq 7$, the mod q image is full by proposition 4.4. At $q = 5$, a proper image would produce a rational 5-isogeny and hence a forbidden cyclic 90-isogeny, so the image is also full. Thus, the only possible nontrivial intersection field is W_q. At most one row can have this field, since $[a(v)] \neq [b(v)]$ by corollary 5.5. For a fixed noncuspidal v, the row with squareclass $[b(v)]$ has intersection field W_q precisely when $y^2 = w\,v(3v^2 - 3v + 1)$ has a rational solution y. The substitutions $X = w(3v-1)$ and $Y = 3wy$ identify this curve with $\mathscr{E}_{18,q}$. The involution $v \longmapsto (v-1)/(3v-1)$ exchanges the two row conditions, so the same criterion applies to either row. By lemma A.1, the rational torsion on $\mathscr{E}_{18,q}$ consists of O and $(-w, 0)$, both corresponding to cusps. Consequently, a nontrivial intersection occurs precisely when $r_{18}(q) > 0$. Since $r_{18}(5) = 0$, all $(2,5)$-intersections on this graph are trivial.

6. Cartan-normalizer images at $q = 3$

The cases where $K_3(E)$ has only one quadratic subfield were covered in proposition 4.5. Among the cases with three quadratic subfields, those admitting a rational 3-isogeny were treated in the previous section. We now consider the remaining cases, where the mod 3 image is a split or nonsplit Cartan normalizer. By section 2.2, these occur only on the graph $L_2(2)$.

Throughout this section, let $E \to E'$ be a rational 2-isogeny between non-CM curves with mod 3 image $N_\star(3)$, where $\star \in \{\mathrm{s}, \mathrm{ns}\}$. Write $W = W_3 = \mathbb{Q}(\sqrt{-3})$. The quotient character $\varepsilon_\star : N_\star(3) \to N_\star(3)/C_\star(3) \simeq \{\pm 1\}$ defines a quadratic field $M_\star$, and $\det \cdot \varepsilon_\star$ defines $M'_\star$. These are the two quadratic subfields of $K_3(E) = K_3(E')$ other than W.

6.1. The split Cartan normalizer.

The degree-two cover $X_{\mathrm{s}}(3) \to X_{\mathrm{s}}^+(3)$ determines M_{s}. We use it to compute the quadratic subfields of $K_3(E)$ and compare them with the 2-division fields across the 2-isogeny. Zywina's j-maps for the split Cartan and its normalizer are [22, Theorem 1.2]

$$J_{\mathrm{s}}^+(\tau) = 27\frac{(\tau+1)^3(\tau-3)^3}{\tau^3}, \tag{6.1}$$

$$J_{\mathrm{s}}(v) = 27\frac{(v+1)^3(v+3)^3(v^2+3)^3}{v^3(v^2+3v+3)^3}. \tag{6.2}$$

Proposition 6.1. *The normalization of $X_0(2) \times_{X(1)} X_{\mathrm{s}}^+(3)$ is rational, with a parameter z whose cusps are $z = \pm 1, -1/2, \infty$. Set $h_{\mathrm{s}}(z) = z^2 - 2z - 2$. Then*

$$M_{\mathrm{s}} = \mathbb{Q}\big(\sqrt{-3h_{\mathrm{s}}(z)}\big), \qquad M'_{\mathrm{s}} = \mathbb{Q}\big(\sqrt{h_{\mathrm{s}}(z)}\big), \tag{6.3}$$

$$K_2(E) = \mathbb{Q}\big(\sqrt{-(2z+1)h_{\mathrm{s}}(z)}\big), \qquad K_2(E') = \mathbb{Q}\big(\sqrt{(z^2-1)h_{\mathrm{s}}(z)}\big). \tag{6.4}$$

Proof. We may take

$$s = -4\frac{(2z+1)^3}{(z-1)^3(z+1)^3} \quad \text{and} \quad \tau = 9\frac{(z+1)^2}{(z-1)^2(2z+1)}. \tag{6.5}$$

Substitution verifies $256(s+1)^3/s = J_{\mathrm{s}}^+(\tau)$. The coprime level conditions yield a geometrically connected modular curve of degree 18 over the j-line. The modular curve and the displayed parametrization both have degree 18 over the j-line, so the parametrization is birational. Its poles are the cusps.

The relation $\tau = v + 3 + 3/v$ implies $J_{\mathrm{s}}(v) = J_{\mathrm{s}}^+(\tau)$. Thus, the degree-two cover $X_{\mathrm{s}}(3) \to X_{\mathrm{s}}^+(3)$ is described by $v^2 + (3-\tau)v + 3 = 0$. Its discriminant $\tau^2 - 6\tau - 3$ has squareclass $[-3h_{\mathrm{s}}(z)]$, giving M_{s}. Multiplication by the determinant character gives M_{s}'. Finally, substituting (6.5) into (4.5) gives the two 2-division fields. s □

Comparing (6.3) and (6.4) gives the following conditions. An intersection at E or E' equals the field in the first column precisely when the corresponding entry is a nonzero rational square.

(6.6)

field	E	E'
M_{s}'	$-(2z+1)$	z^2-1
M_{s}	$(2z+1)/3$	$(1-z^2)/3$
W	$(2z+1)h_{\mathrm{s}}(z)/3$	$(1-z^2)h_{\mathrm{s}}(z)/3$

Lemma 6.2. *For noncuspidal $z \in \mathbb{Q}$, neither $F_3(E)$ nor $F_3(E')$ equals W.*

Proof. The source condition is $y^2 = 3(2z+1)(z^2-2z-2)$. Under $X = 6z-3$, $Y = 6y$, it becomes $Y^2 = X^3 - 135X - 594$. By lemma A.2, its only rational points are O and $(-6, 0)$, and so $z = \infty, -1/2$. For the target condition $y^2 = 3(1-z^2)(z^2-2z-2)$, set $X = 18/(z-1)+3$ and $Y = 18y/(z-1)^2$. This yields the same elliptic curve, whose points pull back to $z = \pm 1$. All these values are cusps. □

Lemma 6.3. *For noncuspidal $z \in \mathbb{Q}$, the intersections $F_3(E)$ and $F_3(E')$ cannot both be nontrivial.*

Proof. By lemma 6.2, the only possible nontrivial intersection fields are M_{s} and M_{s}'. The source conditions in (6.6) give $z = -(r^2+1)/2$ or $z = (3r^2-1)/2$. The four possibilities for nontrivial intersections at both endpoints lead to

$(F_3(E), F_3(E'))$	quartic model
$(M_{\mathrm{s}}', M_{\mathrm{s}}')$	$y^2 = (r^2-1)(r^2+3)$
$(M_{\mathrm{s}}', M_{\mathrm{s}})$	$y^2 = -3(r^2-1)(r^2+3)$
$(M_{\mathrm{s}}, M_{\mathrm{s}}')$	$y^2 = 3(r^2-1)(3r^2+1)$
$(M_{\mathrm{s}}, M_{\mathrm{s}})$	$y^2 = -(r^2-1)(3r^2+1)$.

The first and fourth are isomorphic to $\mathcal{E}_1 : Y^2 = X^3 - X^2 + X$, using $X = (r+1)/(r-1)$ and $X = -(r+1)/(r-1)$, respectively, with $Y = y/(r-1)^2$. The second and third are isomorphic to $\mathcal{E}_2 : Y^2 = X^3 + 3X^2 + 9X$, using $X = -3(r+1)/(r-1)$ and $X = 3(r+1)/(r-1)$, with $Y = 3y/(r-1)^2$. Their rational points are

$$\mathcal{E}_1(\mathbb{Q}) = \{O, (0,0), (1, \pm 1)\}, \qquad \mathcal{E}_2(\mathbb{Q}) = \{O, (0,0), (3, \pm 9)\}$$

by lemma A.2. The corresponding values $r \in \{0, \pm 1, \infty\}$ are cusps. □

Theorem 6.4. *For a rational 2-isogeny between non-CM curves with exact mod 3 image $N_{\mathrm{s}}(3)$, the possible pairs are*

$$(\mathbb{Q},\mathbb{Q}),\quad (M_{\mathrm{s}},\mathbb{Q}),\quad (M'_{\mathrm{s}},\mathbb{Q}),\quad (\mathbb{Q},M_{\mathrm{s}}),\quad (\mathbb{Q},M'_{\mathrm{s}}). \tag{6.7}$$

Every pair occurs for infinitely many distinct j-invariants with this exact image.

Proof. By lemma 6.2, neither intersection can equal W_3, and by lemma 6.3, they cannot both be nontrivial. This leaves exactly the five pairs in (6.7).

The five pairs in (6.7) are realized, in that order, by $z = 2, -1/3, -5, 1/2, -5/3$, as follows from (6.6). For each parameter, $[-3h_{\mathrm{s}}(z)]$ is neither $[1]$ nor $[-3]$, so the two quadratic characters are independent and the projective mod 3 image is $C_2 \times C_2$. Every index two subgroup of $N_{\mathrm{s}}(3)$ contains its commutator $\{\pm I\}$, so no proper subgroup surjects onto the projective quotient. Thus, the exact image is $N_{\mathrm{s}}(3)$. These j-invariants are nonintegral, so the curves are non-CM.

Each one-sided condition defines a rational conic containing the corresponding specialization above, where the unwanted conditions fail. For $(\mathbb{Q},\mathbb{Q})$, the value $z = 2$ shows that all four unwanted conditions define nontrivial covers of the z-line. The j-map is nonconstant, so lemma 2.6 applies to each family. □

6.2. **The nonsplit Cartan normalizer.** Zywina's j-map for the nonsplit Cartan normalizer is $J^+_{\mathrm{ns}}(\tau) = \tau^3$ [22, Theorem 1.2].

Proposition 6.5. *The normalization of $X_0(2) \times_{X(1)} X^+_{\mathrm{ns}}(3)$ is rational, with parameter z. The cusps are $z = 0, \infty$, and $z = -1$ gives $j = 1728$. Set $h_{\mathrm{ns}}(z) = z^2 - z + 1$. Then*

$$M_{\mathrm{ns}} = \mathbb{Q}\big(\sqrt{-3h_{\mathrm{ns}}(z)}\big), \qquad M'_{\mathrm{ns}} = \mathbb{Q}\big(\sqrt{h_{\mathrm{ns}}(z)}\big), \tag{6.8}$$

$$K_2(E) = \mathbb{Q}\big(\sqrt{(z+1)h_{\mathrm{ns}}(z)}\big), \qquad K_2(E') = \mathbb{Q}\big(\sqrt{z(z+1)h_{\mathrm{ns}}(z)}\big). \tag{6.9}$$

Proof. We may take

$$s = \frac{4}{z^3}, \qquad \tau = 4\frac{z^3+4}{z^2}, \qquad j(z) = 64\frac{(z^3+4)^3}{z^6}. \tag{6.10}$$

These formulas follow from $256(s+1)^3/s = \tau^3$ by setting $z = \tau/(4(s+1))$. The substitution is rationally invertible, so the parametrization is birational.

For $j = \tau^3$, the quadratic fields computed in [7, Example 6.1] are W, $\mathbb{Q}(\sqrt{d(\tau)})$, and $\mathbb{Q}(\sqrt{-3d(\tau)})$, where $d(\tau) = \tau^2 + 12\tau + 144$. Their characters factor through the projective image, so these fields are unchanged by quadratic twisting [7, Remark 6.2]. Complex conjugation has determinant -1 and cannot lie in $C_{\mathrm{ns}}(3) \simeq C_8$, whose only involution is $-I$. Thus, M_{ns} is imaginary and, since $d(\tau) > 0$, equals $\mathbb{Q}(\sqrt{-3d(\tau)})$.

By substitution we get $d(\tau) = 16h_{\mathrm{ns}}(z)(z^2+2z+4)^2/z^4$, proving the two character-field formulas. The 2-division formulas follow from (4.5) and $z^3 + 1 = (z+1)h_{\mathrm{ns}}(z)$. □

The following table gives the corresponding squareclass conditions: an intersection at E or E' equals the field in the first column precisely when the entry is a nonzero rational square.

field	E	E'
M'_{ns}	$z+1$	$z(z+1)$
M_{ns}	$-(z+1)/3$	$-z(z+1)/3$
W	$-(z^3+1)/3$	$-z(z^3+1)/3$.

(6.11)

Lemma 6.6. *At a noncuspidal non-CM point, neither $F_3(E)$ nor $F_3(E')$ equals W.*

Proof. The source condition $y^2 = -3(z^3+1)$ becomes $V^2 = U^3 - 27$ under $U = -3z$, $V = 3y$. For the target condition $y^2 = -3z(z^3+1)$, use $U = -3/z$, $V = 3y/z^2$. This elliptic curve has rational points $O, (3, 0)$ by lemma A.2. Their preimages give only $z = 0, \infty, -1$, which are cusps or the excluded CM value. □

Lemma 6.7. *For a non-CM point with exact image $N_{\mathrm{ns}}(3)$, the pair $(M_{\mathrm{ns}}, M_{\mathrm{ns}})$ cannot occur.*

Proof. In (6.11), the source condition requires $z < -1$, whereas the target condition requires $-1 < z < 0$. □

Theorem 6.8. *For a rational 2-isogeny between non-CM curves with exact mod 3 image $N_{\mathrm{ns}}(3)$, the possible pairs are*

$$\begin{gathered}(\mathbb{Q},\mathbb{Q}),\quad (M_{\mathrm{ns}},\mathbb{Q}),\quad (M'_{\mathrm{ns}},\mathbb{Q}),\quad (\mathbb{Q},M_{\mathrm{ns}}),\quad (\mathbb{Q},M'_{\mathrm{ns}}),\\ (M'_{\mathrm{ns}},M'_{\mathrm{ns}}),\quad (M'_{\mathrm{ns}},M_{\mathrm{ns}}),\quad (M_{\mathrm{ns}},M'_{\mathrm{ns}}).\end{gathered} \tag{6.12}$$

Every pair occurs for infinitely many distinct source j-invariants with this exact image.

Proof. By lemma 6.6, neither intersection can equal W_3, and by lemma 6.7, the pair $(M_{\mathrm{ns}}, M_{\mathrm{ns}})$ is impossible. This leaves exactly the eight pairs in (6.12).

The eight pairs in (6.12) are realized by

z	-3	$-7/3$	3	$-3/7$	$1/3$	$16/9$	$-3/4$	$-4/3$
ℓ	11	11	5	11	11	11	5	17

(6.13)

respectively. For the model $y^2 = x^3 - 3j(j-1728)x - 2j(j-1728)^2$, with j from (6.10), the 3-division quartic is irreducible mod the corresponding prime ℓ. Thus, the projective image contains a 4-cycle. Complex conjugation lies outside the nonsplit Cartan, so the projective image is the full dihedral group of order eight. An index-two subgroup of $N_{\mathrm{ns}}(3)$ contains its commutator $\langle c^2 \rangle$, where c generates $C_{\mathrm{ns}}(3)$, and hence contains $-I = c^4$. It cannot map isomorphically onto the projective quotient. The exact image is therefore $N_{\mathrm{ns}}(3)$. These specializations have nonintegral j-invariants.

The allowed simultaneous conditions produce rational conics; for example,

$$(M'_{\mathrm{ns}}, M'_{\mathrm{ns}}) : z = \frac{(1-v^2)^2}{4v^2}, \qquad (M'_{\mathrm{ns}}, M_{\mathrm{ns}}) : z = -\frac{12v^2}{(1+3v^2)^2}.$$

The pair $(M_{\mathrm{ns}}, M'_{\mathrm{ns}})$ is obtained from $z+1 = -3r^2$ and $-3z = s^2$.

The one-sided conditions also define rational conics. Each of these, as well as the conics for the simultaneous cases, contains a rational point corresponding to the appropriate value of z in (6.13). At these points, the mod 3 image is $N_{\mathrm{ns}}(3)$, and the intersection fields are as claimed. For $(\mathbb{Q}, \mathbb{Q})$, take $z = -3$ on the unrestricted z-line. Since the j-map is nonconstant, lemma 2.6 gives infinitely many distinct source j-invariants realizing each pair with this exact image.

□

7. Rational 5-isogenies and the degree-10 criterion

Having classified the $(2, 3)$-intersections, we now consider $q = 5$. By proposition 4.4, a non-CM curve admitting a rational 2-isogeny has either full mod 5 image or an image contained in a Borel. The former case was treated in proposition 4.5. In the latter case, the curve also

admits a rational 5-isogeny, so we use $X_0(10)$ to classify the possible $(2,5)$-intersections. We then determine the $(2,q)$-intersection patterns on $R_4(10)$ and establish the degree 10 rank criterion.

Let $E \to E'$ be a rational 2-isogeny between non-CM elliptic curves over $\mathbb{Q}$, and set $L_5 = K_5(E) = K_5(E')$ and $W_5 = \mathbb{Q}(\sqrt{5})$.

7.1. **A parameter on $X_0(10)$.** Let t be the standard parameter on $X_0(5)$, normalized so that

$$j = \frac{(t^2+10t+5)^3}{t}. \tag{7.1}$$

Equating this j-map with $j = 256(s+1)^3/s$ from (4.4) produces a curve whose normalization is $X_0(10)$. The following proposition gives a rational parametrization.

Proposition 7.1. *The curve $X_0(10)$ has a rational parameter z with*

$$s = 4\frac{2z+3}{(z-1)(z+1)^5}, \qquad t = \frac{(z-1)^2(2z+3)}{(z+1)^2}. \tag{7.2}$$

Its cusps are $z = 1, -1, -3/2, \infty$, and its j-map is

$$j(z) = 256\frac{(s(z)+1)^3}{s(z)}. \tag{7.3}$$

Proof. Substitution verifies that (7.1) and (4.4) agree. The normalization of their fiber product is $X_0(10)$, since $\Gamma_0(10) = \Gamma_0(2) \cap \Gamma_0(5)$. Both its j-degree and that of the displayed parametrization are 18, so the map is birational. Its poles are the stated cusps. □

Let $h(z) = z^2 + 2z + 2$. The following proposition gives the quadratic fields needed to determine the $(2,5)$-intersections.

Proposition 7.2. *Let $z \in \mathbb{Q} \setminus \{1, -1, -3/2\}$, let $E = E_{s(z),u}$ be the curve (4.3), and let E' be its 2-isogenous quotient. Let $\psi : G_{\mathbb{Q}} \longrightarrow \mathbb{F}_5^\times$ be the character on the chosen rational 5-isogeny kernel, and let $M_5 := \overline{\mathbb{Q}}^{\ker(\psi^2)}$. Then*

$$M_5 = \mathbb{Q}\left(\sqrt{h(z)}\right), \tag{7.4}$$

$$K_2(E) = \mathbb{Q}\left(\sqrt{(2z+3)h(z)}\right), \tag{7.5}$$

$$K_2(E') = \mathbb{Q}\left(\sqrt{(z^2-1)h(z)}\right). \tag{7.6}$$

If M_5 is nontrivial and distinct from W_5, then the three quadratic subfields of L_5 are

$$W_5, \qquad M_5, \qquad M_5' := \mathbb{Q}\left(\sqrt{5h(z)}\right). \tag{7.7}$$

In particular, this holds when the exact mod 5 image is the full Borel $\mathsf{B}(5)$.

Proof. For a generator P of the rational 5-isogeny kernel, $M_5 = \mathbb{Q}(x(P))$. Using the parameter r on $X_0(5)$ from [6, Section 5.9], we have $\mathbb{Q}(x(P)) = \mathbb{Q}(\sqrt{5r^2 + (22/5)r + 1})$. Their j-map is $25(r^2+10r+5)^3/r^5$. The substitution $r = 5/t$ gives our normalization, and hence $M_5 = \mathbb{Q}(\sqrt{t^2+22t+125})$. Under (7.2), this radicand has squareclass $[h(z)]$. The same substitution into (4.5) gives $[s(s+4)] = [(2z+3)h(z)]$ and $[s+4] = [(z^2-1)h(z)]$.

Finally, every quadratic character of the image factors through the diagonal image $D \subseteq \mathbb{F}_5^\times \times \mathbb{F}_5^\times$. When $M_5 \notin \{\mathbb{Q}, W_5\}$, the characters ψ^2 and χ_5^2 are independent. Thus, D maps onto the quotient $(C_4 \times C_4)/2(C_4 \times C_4)$. A proper subgroup of $C_4 \times C_4$ lies in an index-2 subgroup, so cannot have this property. Hence $D = C_4 \times C_4$, and its three nontrivial quadratic characters are ψ^2, χ_5^2, and their product. They correspond to the fields in (7.7). □

When the fields in (7.7) are distinct, the following table determines the intersections: the indicated field occurs at an endpoint precisely when the corresponding entry is a nonzero rational square. The W_5 row also applies when there is only one quadratic subfield.

(7.8)

field	E	E'
M_5	$2z+3$	z^2-1
M_5'	$(2z+3)/5$	$(z^2-1)/5$
W_5	$(2z+3)h(z)/5$	$(z^2-1)h(z)/5$

Lemma 7.3. *Suppose that $H = \rho_{E,5}(G_\mathbb{Q})$ is contained in a Borel subgroup and has full determinant. Then $K_5(E)$ has either one or three quadratic subfields. In the first case the unique quadratic subfield is W_5. In the second case the three fields may be written W_5, T_5, and T_5', where $T_5 = \mathbb{Q}(\sqrt{d})$ is either non-Weil field and $T_5' = \mathbb{Q}(\sqrt{5d})$ is the other.*

Proof. By [5, Corollary 5.7], $\mathrm{Gal}(A_5(E)/\mathbb{Q}) \simeq C_4 \times C$, where C is cyclic of order dividing four. Hence $A_5(E)$, and therefore $K_5(E)$, has either one or three quadratic subfields. One of them is always W_5, cut out by χ_5^2. If there are three, multiplying either non-Weil quadratic character by χ_5^2 gives the other one, as claimed. □

7.2. **Excluding Weil and simultaneous intersections.**

Proposition 7.4. *For noncuspidal $z \in \mathbb{Q}$, neither $F_5(E)$ nor $F_5(E')$ equals W_5.*

Proof. The source condition is

$$y^2 = 5(2z+3)(z^2+2z+2). \tag{7.9}$$

Under $X = 5(2z+3)$, $Y = 10y$, this becomes $Y^2 = X^3 - 10X^2 + 125X$. Its only rational points are $O, (0,0)$ by lemma A.2, which means the cusps are $z = \infty, -3/2$. The involution

$$w_2(z) = -\frac{z+2}{z+1} \tag{7.10}$$

satisfies $s(w_2(z)) = 16/s(z)$ and exchanges the two 2-division squareclasses. The same argument rules out W_5 at the target.

□

To rule out nontrivial intersections at both endpoints, we consider all the quadratic subfields of $K_5(E)$, not only the field defined by ψ^2.

Proposition 7.5. *For noncuspidal $z \in \mathbb{Q}$, the two endpoint intersections cannot both be nontrivial.*

Proof. Their 2-division squareclasses are $[(2z+3)h(z)]$ and $[(z^2-1)h(z)]$. By proposition 7.4, neither intersection is W_5. If the two nontrivial fields are equal, the product of their squareclasses is $[1]$; if distinct, they are the two non-Weil fields of lemma 7.3, whose product class is

[5]. Thus, simultaneous nontrivial intersections would produce a noncuspidal rational point on one of the curves

$$C_0 : \quad y^2 = (2z+3)(z^2-1), \tag{7.11}$$

$$C_5 : \quad y^2 = 5(2z+3)(z^2-1). \tag{7.12}$$

In $y^2 = e(2z+3)(z^2-1)$, put $X = e(2z+1)$, $Y = 2ey$. For $e = 1, 5$ this gives, respectively,

$$Y^2 = X^3 - 7X - 6, \qquad Y^2 = X^3 - 175X - 750.$$

By lemma A.2, each has only its rational 2-torsion and O. Their preimages have $z \in \{\infty, -3/2, -1, 1\}$, so all are cusps. □

7.3. **The $(2,5)$-intersection patterns.**

Theorem 7.6. *Let $E \to E'$ be a rational 2-isogeny between non-CM elliptic curves over $\mathbb{Q}$, and suppose that the mod 5 image is contained in a Borel. Then neither $F_5(E)$ nor $F_5(E')$ equals W_5, and at most one is nontrivial.*

If W_5 is the only quadratic subfield of $K_5(E)$, then $(F_5(E), F_5(E')) = (\mathbb{Q}, \mathbb{Q})$. Otherwise, write the three quadratic subfields as W_5, T_5, and T_5', where T_5 is either of the two fields other than W_5. Then

$$(F_5(E), F_5(E')) \in \big\{(\mathbb{Q},\mathbb{Q}),\ (T_5,\mathbb{Q}),\ (T_5',\mathbb{Q}),\ (\mathbb{Q},T_5),\ (\mathbb{Q},T_5')\big\}. \tag{7.13}$$

Every pair in this list occurs for infinitely many distinct source j-invariants with exact mod 5 image $\mathsf{B}(5)$. In these cases, we may take $T_5 = M_5 := \overline{\mathbb{Q}}^{\ker(\psi^2)}$, where ψ is the character on the rational 5-isogeny kernel.

Proof. By proposition 7.4, neither intersection can equal W_5, and by proposition 7.5, they cannot both be nontrivial. If W_5 is the only quadratic subfield of $K_5(E)$, both intersections are therefore trivial. Otherwise, lemma 7.3 gives the two remaining possibilities T_5 and T_5', yielding (7.13).

To show that all five pairs occur, take $T_5 = M_5$, $T_5' = M_5'$, and $u = 1$ in (4.3). The values $z = 0, 1/2, -3/5, 5/4, 3/2$ give the five pairs in (7.13), respectively, by proposition 7.2. For each value, $[h(z)] \notin \{[1],[5]\}$, so the diagonal image is $\mathbb{F}_5^\times \times \mathbb{F}_5^\times$.

For these five curves, the 5-division polynomial has irreducible factors of degrees 2 and 10, as verified by the accompanying code. The factor of degree 10 shows that the mod 5 image has order divisible by 5. Since its diagonal image has order 16, it must be the full Borel $\mathsf{B}(5)$. The five j-invariants are nonintegral, so the curves are non-CM.

It remains to prove that each pair occurs infinitely often. The four conditions for a non-Weil intersection at one endpoint are

$$2z+3 = r^2, \qquad 2z+3 = 5r^2, \qquad z^2-1 = r^2, \qquad z^2-1 = 5r^2.$$

Each defines a rational conic containing the corresponding example above. At that point, the other endpoint has trivial intersection, so the squareclass conditions that would make it nontrivial define nontrivial double covers. For $(\mathbb{Q},\mathbb{Q})$, the example $z = 0$ likewise shows that the unwanted squareclass conditions define nontrivial covers of the z-line.

Since the j-map (7.3) is nonconstant, lemma 2.6 gives infinitely many distinct source j-invariants realizing each pair with exact mod 5 image $\mathsf{B}(5)$. □

7.4. **The rectangle $R_4(10)$.** A class with rational 2 and 5-isogenies has graph $R_4(10)$. By proposition 4.1, the two endpoints of each 5-edge have the same intersection field. The 2-division fields on the two 5-edges have squareclasses $[(2z+3)h(z)]$ and $[(z^2-1)h(z)]$, respectively, by equations (7.5) and (7.6). At $q=5$, theorem 7.6 gives the complete list.

For $q \neq 5$, the mod q image is full, by proposition 4.4 for $q \geq 7$ and [16, Theorem 1.1, Table 1] for $q=3$. At a noncuspidal parameter z, the intersection on the first 5-edge is W_q precisely when $w(2z+3)(z^2+2z+2)$ is a rational square, equivalently when $y^2 = w(2z+3)(z^2+2z+2)$ has a rational solution y. The substitutions

$$X = w(2z+3), \qquad Y = 2wy \tag{7.14}$$

identify this curve with $\mathscr{E}_{10,q}$. The involution (7.10) exchanges the two 2-division squareclasses, so an intersection equal to W_q can occur on either 5-edge precisely when $r_{10}(q) > 0$. The two edges cannot both have field W_q: this would give a noncuspidal rational point on (7.11), whose rational points were determined in the proof of proposition 7.5.

By lemma A.1, the rational torsion of $\mathscr{E}_{10,q}$ is $\{O,(0,0)\}$. These points correspond to $z=\infty,-3/2$, both cusps. Consequently, a nontrivial field occurs at $q \neq 5$ precisely when $r_{10}(q) > 0$. The positive rank gives infinitely many admissible points and hence infinitely many distinct j-invariants. Since $r_{10}(3)=0$ by section A, all $(2,3)$-intersections on $R_4(10)$ are trivial. At $q=5$, theorem 7.6 shows that the only possible nontrivial intersection fields are T_5 and T_5'.

8. 2-isogeny trees and congruent numbers

We now consider the remaining isogeny graphs whose edges all have degree 2: T_4, T_6, and T_8. We determine their possible $(2,q)$-intersections, and the case T_8 leads to a criterion involving congruent numbers. A curve with full rational 2-torsion can be written, up to quadratic twist, as

$$C_t: \quad y^2 = x(x-1)(x-t), \qquad t \neq 0,1.$$

Quadratic twisting does not change its 2-division fields or its rational isogeny graph. For a model with roots e_1,e_2,e_3, the quotient by $(e_i,0)$ has 2-division field

$$\mathbb{Q}\left(\sqrt{(e_i-e_j)(e_i-e_k)}\right), \qquad \{i,j,k\}=\{1,2,3\}. \tag{8.1}$$

This follows from proposition 4.2 after translating the kernel point to $(0,0)$.

For the exact graphs T_4, T_6, T_8, all odd mod q images are full. For $q=3$ this is [16, Table 1]; for $q=5$ a proper image would imply a 5-edge, which these graphs do not have; and for $q \geq 7$ use proposition 4.4. Thus, a vertex is labelled W_q precisely when its 2-division field is W_q, and otherwise it is labelled $\mathbb{Q}$. We call a vertex of an isogeny graph a *leaf* if it is joined to exactly one other vertex. We call a leaf *marked* when its intersection is W_q.

8.1. **The four-vertex star.** The three vertices adjacent to C_t in T_4 are its leaves. Their 2-division fields have squareclasses

$$t, \qquad 1-t, \qquad -t(1-t). \tag{8.2}$$

Exactly one of these classes is negative, and their product is $[-1]$. Thus, if $q \equiv 3 \pmod 4$, the imaginary field W_q can occur on at most one leaf. The three leaves also cannot have the same nontrivial 2-division field: if all three had squareclass $[w]$, their product would force $[w]=[-1]$, contradicting the fact that exactly one is negative.

Two leaves can therefore have field W_q only if $q \equiv 1 \pmod 4$. Conversely, in this case q is a sum of two squares, so the conic $q(a^2+b^2)=1$ has a rational point and is rational. Setting $t = qa^2$ gives $[t] = [1-t] = [q]$, while $[-t(1-t)] = [-1]$. All three classes are nontrivial, so no additional vertex with full rational 2-torsion arises. The graph cannot be S, since lemma 5.8 shows that the three corresponding 2-division fields on S are distinct. Hence, the graph is T_4.

To obtain a pattern with exactly one leaf carrying W_q, take $t = wr^2$ and avoid the squareclass conditions that would mark another leaf or enlarge the graph. The pattern in which all intersection fields are $\mathbb{Q}$ is obtained from the full t-family. By lemma 2.6, these constructions yield infinitely many distinct source j-invariants. We verify in section 9.1 that these constructions correspond to curves with isogeny graph exactly T_4.

8.2. **The six-vertex tree.** Choose two adjacent core vertices as

$$C: \quad y^2 = x(x-1)(x-t^2), \qquad D: \quad y^2 = x\big(x+(t-1)^2\big)\big(x+(t+1)^2\big),$$

with $t \neq 0, \pm 1$. The four outer leaf fields have squareclasses

$$\underbrace{\pm(t^2-1)}_{\text{at } C}, \qquad \underbrace{\pm t}_{\text{at } D}. \tag{8.3}$$

This follows directly from equation (8.1).

At most one leaf at either core can have a given field W_q, since $[a] \neq [-a]$ over $\mathbb{Q}$. If there were a marked leaf at both cores, then $[t(t^2-1)]$ would be $[1]$ or $[-1]$. After replacing t by $-t$ if necessary, this results in a noncuspidal rational point on $Y^2 = X^3 - X$. Its only rational points are $O, (0,0), (1,0), (-1,0)$, as certified in section A. Thus, no such two-leaf pattern exists.

For a single marked leaf take $t = wr^2$. There are infinitely many choices of t for which none of the other leaf squareclasses is trivial. The resulting curves have isogeny graph exactly T_6. By symmetry, any of the four leaves can have intersection field W_q.

8.3. **The eight-vertex tree and congruent numbers.** The three core vertices of T_8 form a path, with the middle core joined to the other two by 2-isogenies. After choosing and orienting this chain, we may take the parameter from (8.3) to be $t = u^2$, where $u \neq 0, \pm 1$. The five leaf classes are

$$\underbrace{\pm(u^4-1)}_{\text{left end}}, \qquad \underbrace{-1}_{\text{middle}}, \qquad \underbrace{\pm 2u(u^2+1)}_{\text{right end}}. \tag{8.4}$$

The three core models have roots

$$\{0, 1, u^4\}, \quad \{0, -(u^2-1)^2, -(u^2+1)^2\}, \quad \{0, -(u-1)^4, -(u+1)^4\}.$$

Each end core is joined to two leaves, and the middle core to one. Applying equation (8.1) to the 2-torsion points defining these five isogenies gives equation (8.4). Conversely, suppose the isogeny graph is T_8. Choose an end core C and the middle core D. The parametrization (8.3) applies to these two cores. Since D is also joined to a third core, one of the two squareclasses $[t]$ and $[-t]$ at D must be trivial. Replacing t by $-t$ interchanges the two nonzero roots of D without changing C. We may therefore assume that t is a square and write $t = u^2$.

The leaf attached to the middle core has 2-division field $\mathbb{Q}(i)$, which is not W_q for any odd prime q. If a leaf at each end of the path were marked, then we would have $[(u^4-1)\, 2u(u^2+$

$1)] = [\pm 1]$, so $[2u(u^2-1)] = [\pm 1]$. Replacing u by $-u$ if necessary and setting $X = 2u$, we obtain a rational point on $Y^2 = X^3 - 4X$ with $X \neq 0, \pm 2$. But its rational points are only $O, (0,0), (2,0), (-2,0)$, so this is impossible. Thus, at most one outer leaf is marked.

The substitution $u \mapsto (u+1)/(u-1)$ is an involution, and $\left(\frac{u+1}{u-1}\right)^4 - 1 = \frac{8u(u^2+1)}{(u-1)^4}$. Thus, it interchanges the pairs of leaf squareclasses at the two ends of the path. Similarly, replacing u by $1/u$ interchanges the two squareclasses $[u^4-1]$ and $[-(u^4-1)]$, since $(1/u)^4 - 1 = -\frac{u^4-1}{u^4}$. Consequently, a marked outer leaf exists exactly when the quartic

$$V^2 = q(U^4 - 1) \tag{8.5}$$

has a rational point with $U \neq 0, \pm 1$.

This has a rational point $(1,0)$ and a nonconstant degree-two map to $\mathscr{E}_{16,q}$:

$$(U, V) \longmapsto (X, Y) = (qU^2, qUV). \tag{8.6}$$

After translating the image of $(1,0)$ to the origin, this is an isogeny of elliptic curves, so the two curves have equal ranks. By lemma A.1, the rational torsion of $\mathscr{E}_{16,q}$ is $C_2 \times C_2$. For a rational point on the quartic whose image under (8.6) is torsion, we must have $U = \pm 1$: $X = 0$ would require $V^2 = -q$, $X = -q$ would require $U^2 = -1$, and rational points at infinity would require q to be a square. Hence, a rational point on (8.5) with $U \neq 0, \pm 1$ exists precisely when $r_{16}(q) > 0$.

Finally, q is a congruent number if and only if $Y^2 = X^3 - q^2X$ has positive rank [8]. Indeed, a nontorsion rational point (X, Y) corresponds to a right triangle with side lengths $\left|\frac{X^2-q^2}{Y}\right|, \left|\frac{2qX}{Y}\right|, \left|\frac{X^2+q^2}{Y}\right|$, whose area is q. This proves corollary 1.3.

Example 8.1. The curves

$$E: \ y^2 = x^3 - 322x^2 + x, \quad E': \ y^2 = x^3 + 992x^2 + 256x$$

are connected by a cyclic 16-isogeny. They lie at opposite ends of T_8, whose three core curves have roots $\{0, 1, 81\}$, $\{0, -64, -100\}$, and $\{0, -16, -256\}$. Their 2-division fields are $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{15})$. Their mod 5 images are full, so

$$F_{2,5}(E) = \mathbb{Q}(\sqrt{5}), \qquad F_{2,5}(E') = \mathbb{Q}.$$

This is the specialization $u = 3$ of equation (8.4). The left curve has nonintegral j-invariant, hence is non-CM; the other curves are isogenous to it.

9. Graph-level classification and cyclic isogenies of arbitrary degree

9.1. **Isogeny graph patterns and their realization.** We summarize the intersection patterns in two tables. Table 4 covers graphs with only 2-isogenies and table 5 covers graphs containing both 2-isogenies and odd-degree isogenies.

Each vertex representing E is labelled by $F_{2,q}(E)$. By proposition 4.1, this field is constant along odd-degree edges. In each pattern, any vertex not assigned a nontrivial intersection field has field $\mathbb{Q}$. When $q = 3$ and a rational 3-isogeny is present, M and M' denote the two quadratic subfields of $A_3(\mathbb{C})$ other than W_3, when they exist.

Graph	Possible $(2,q)$-intersection patterns, for q odd
$L_2(2)$	The pairs in table 1 for which the mod q Galois image is $\mathrm{GL}_2(\mathbb{F}_q)$ when $q \geq 5$, or one of $\mathrm{GL}_2(\mathbb{F}_3)$, $N_{\mathrm{s}}(3)$, and $N_{\mathrm{ns}}(3)$ when $q = 3$.
T_4	The core has field $\mathbb{Q}$. Any one leaf can have field W_q. Two leaves can have field W_q if and only if $q \equiv 1 \pmod 4$; all three cannot.
T_6	Both cores have field $\mathbb{Q}$. At most one of the four leaves can have field W_q, and any one of them can do so for every odd q.
T_8	The three cores and the leaf attached to the middle core have field $\mathbb{Q}$. At most one of the four remaining leaves can have field W_q. This occurs if and only if $r_{16}(q) > 0$, equivalently if q is a congruent number.

TABLE 4. Intersection patterns on the 2-isogeny trees.

Graph	$q = 3$	$q \geq 5$
$R_4(6)$	The fields on the two 3-edges form one of the pairs listed for Borel mod 3 image in table 1.	At most one 3-edge has field W_q, and either edge can do so.
$R_4(10)$	All fields are $\mathbb{Q}$.	At $q = 5$, the only possible nontrivial fields are T_5 and T_5', on at most one 5-edge. For $q \geq 7$, at most one 5-edge has field W_q, occurring if and only if $r_{10}(q) > 0$.
S	Both cores have field $\mathbb{Q}$. At most one non-core 3-edge has field M or M'; none has field W_3.	At most one non-core 3-edge has field W_q, occurring if and only if $r_{12}(q) > 0$.
$R_6(18)$	Each row has one field. At most one row has field M or M', and neither has field W_3.	At most one row has field W_q, occurring if and only if $r_{18}(q) > 0$.

TABLE 5. Intersection patterns on the mixed graphs. At $q = 5$, all fields on S and $R_6(18)$ are $\mathbb{Q}$, since $r_{12}(5) = r_{18}(5) = 0$.

Proposition 9.1. *For every odd prime q, each intersection pattern listed in tables 4 and 5, subject to the stated restrictions, occurs for infinitely many distinct j-invariants of non-CM elliptic curves whose isogeny graph is exactly the indicated graph.*

Proof. By section 2.2, none of S, $R_6(18)$, $R_4(10)$, or T_8 can be enlarged to a larger non-CM isogeny graph. For $N \in \{10, 12, 16, 18\}$ with $r_N(q) > 0$, the elliptic curve $\mathscr{E}_{N,q}$ has infinitely many rational points. The corresponding maps to the j-line are nonconstant and have finite fibers. Excluding the finitely many points giving cusps, singular curves, or CM j-invariants therefore leaves infinitely many distinct j-invariants.

For $q = 3$ on S and $R_6(18)$, set $u = 1$ in (5.1). Then $A_3(\mathcal{C}) = W_3$. Since W_3 cannot occur as an intersection field on either graph, all $(2,3)$-intersections are trivial. To obtain a nontrivial intersection, let d represent the 2-division squareclass of a chosen non-core 3-edge

of S, or a chosen row of $R_6(18)$. Taking $[u] = [d]$ or $[u] = [-3d]$ makes its intersection field M or M', respectively. By lemma 5.8 and corollary 5.5, all other intersections remain trivial. The parameters r and v remain free, leading to infinitely many distinct j-invariants.

In the remaining cases, where the only possible nontrivial intersection field is W_q, we obtain the all-$\mathbb{Q}$ pattern by avoiding certain squareclass equalities. Each nonconstant expression f in (8.2), (8.3), (8.4), (5.10), and (5.12) has a zero or pole of odd order. Thus, the condition $[f] = [w]$ defines a nontrivial quadratic cover of the corresponding parameter line. The constant class $[-1]$ in (8.4) is never $[w]$ for an odd prime q. By Hilbert irreducibility, infinitely many rational parameters avoid these equalities. Since the corresponding j-maps are nonconstant, we get infinitely many distinct source j-invariants with all intersection fields trivial.

For the remaining graphs, we must also rule out additional rational isogenies. We do this using modular covers that parametrize these isogenies. An irreducible cover of degree d cannot acquire a rational section after a base change of degree $e < d$: such a section would embed a degree-d function field extension into one of degree e. In the cases below, the parameters giving additional isogenies therefore form a thin set, which Hilbert irreducibility allows us to avoid [18, Chapter 3].

For T_6, the family $t = wr^2$ gives one marked leaf. The only possible enlargement is T_8, which would require another leaf squareclass in (8.3) to be trivial. The constant classes $[w]$ and $[-w]$ are nontrivial, while $w^2r^4 - 1$ and $1 - w^2r^4$ are nonsquares in $\mathbb{Q}(r)$. We can therefore choose infinitely many parameters for which the exact graph is T_6.

For T_4, the family $t = wr^2$ also gives one marked leaf. The other two leaf squareclasses are nonsquares in $\mathbb{Q}(r)$, so we can avoid introducing another core. The only other possible enlargement is S, which requires a rational 3-isogeny.

The modular cover parametrizing a rational 3-isogeny is irreducible of degree four over $X(2)$, since the level 2 and level 3 conditions are independent. As $t = wr^2$ defines a degree-two base change, this cover cannot acquire a rational section. Hilbert irreducibility therefore gives infinitely many curves with exact graph T_4.

The construction with two marked leaves already has exact graph T_4 by lemma 5.8.

For $R_4(6)$, the families giving intersection field W_q on one 3-edge for $q \geq 5$ have degree at most two over the t-line. The same holds for the families realizing the eleven $(2, 3)$-intersection pairs in theorem 5.7. When only the twist parameter u is prescribed, t remains free, and varying u does not affect rational isogenies.

An enlargement involving additional 3-isogenies would require either two distinct rational 3-isogenies from the same curve or a rational cyclic 9-isogeny extending an existing 3-isogeny. These possibilities are parametrized by two covers of $X_0(6)$: the cover imposing a second rational 3-isogeny, which requires split Cartan mod 3 image, and $X_0(18)$, respectively. Both covers are irreducible of degree three, which follows from their congruence subgroup descriptions. Neither acquires a rational section after a base change of degree at most two.

An additional core on $R_4(6)$ would require t or $d = (t-1)(t-9)$ to be square. In a family where t/w or d/w is made square, the corresponding class remains $[w]$ and is therefore nontrivial. The other radicand also remains nonsquare: neither it nor its quotient by the radicand defining the quadratic base change is square in $\mathbb{Q}(t)$, as each has a zero or pole of odd order. When only the twist parameter u is prescribed, both t and d remain nonsquares in $\mathbb{Q}(t)$.

Hilbert irreducibility allows us to exclude these additional isogenies while preserving the prescribed intersection fields, giving exact graph $R_4(6)$. When $K_3(E)$ has only one quadratic subfield, take $u = 1$ or $u = -3$ in the same parameter families. For the families with exact mod 3 image $\mathsf{B}(3)$, the examples in table 3 and lemma 2.6 ensure that this image is retained for infinitely many specializations.

Finally, consider $L_2(2)$. The split and nonsplit-Cartan normalizer cases at $q = 3$ automatically have this exact graph by section 2.2: the larger 2-isogeny trees and $R_4(10)$ have full mod 3 image, while the other mixed graphs admit rational 3-isogenies.

For the cases with full mod q image, the $(\mathbb{Q}, \mathbb{Q})$ pattern is obtained from the $X_0(2)$ family. The families in proposition 4.5 with exactly one nontrivial intersection field have degree two over $X_0(2)$. The modular covers parametrizing an additional rational 3 or 5-isogeny are irreducible of degrees four and six, respectively, over $X_0(2)$, since the level conditions are independent. Neither cover acquires a rational section after these base changes.

An additional core is also excluded: the remaining 2-division radicand is nonsquare over the corresponding parameter function fields, as follows from the formulas in proposition 4.5. Hilbert irreducibility therefore gives infinitely many specializations with exact graph $L_2(2)$, the prescribed intersection fields, and full mod q image.

If both intersection fields are W_q, the endpoints have the same nontrivial 2-division field. This rules out T_4, T_6, and T_8. The equal field obstructions for $X_0(6)$ and $X_0(10)$ also rule out the mixed graphs. Thus these curves have exact graph $L_2(2)$. □

Proof of theorem 1.1. By lemma 2.4, any two curves in $\mathcal{C}$ are connected by prime degree isogenies. If p and q are odd, a 2-isogeny preserves both division fields by lemma 2.1. Across an odd-prime isogeny, division fields at other primes are unchanged. At the isogeny prime, corollary 3.7 excludes nonabelian intersections for odd prime pairs, and theorem 2.3 preserves the abelian intersection. This proves part (1).

Suppose next that $\mathcal{C}$ has no rational 2-isogeny and that $F_{p,q}$ is not constant on $\mathcal{C}$. Then some odd-prime isogeny changes the intersection field. By theorems 2.3 and 3.14 and corollary 3.7, this must be a 3-isogeny with $\{p, q\} = \{2, 3\}$, and the two fields are the stated S_3-extension and W_3. By proposition 3.17, the entire isogeny graph is $L_2(3)$. Infinitely many such classes exist by theorem 3.14. This proves part (2).

Now suppose that $\mathcal{C}$ contains a rational 2-isogeny. By proposition 2.5, $A_q(\mathcal{C})$ is constant throughout the class, and proposition 4.1 gives the intersection formula and the remaining assertions of part (3).

For $q \geq 7$, proposition 4.4 gives $\rho_{E,q}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_q)$. Hence, $A_q(\mathcal{C}) = \mathbb{Q}(\zeta_q)$ by [5, Corollary 5.3]. Since W_q is the unique quadratic subfield of $\mathbb{Q}(\zeta_q)$, the degree bound in proposition 4.1 implies $F_{2,q}(E) \in \{\mathbb{Q}, W_q\}$.

The graph and image classifications in section 2.2 leave exactly the graphs listed in tables 4 and 5. The patterns on $L_2(2)$ follow from proposition 4.5 and theorems 6.4 and 6.8. The 2-isogeny trees are treated in section 8, and the mixed graphs in sections 5.3 to 5.5 and 7.4. By proposition 9.1, every listed pattern occurs for infinitely many distinct j-invariants on the stated graph. Since each isogeny class contains finitely many vertices, these give infinitely many distinct isogeny classes. This completes part (4). □

9.2. **Cyclic composite degrees.** For quadratic fields D, D', with $D \neq D'$, write

$$\mathcal{P}(D) = \{(\mathbb{Q},\mathbb{Q}), (D,\mathbb{Q}), (\mathbb{Q},D)\},$$
$$\mathcal{P}(D,D') = \{(\mathbb{Q},\mathbb{Q}), (D,\mathbb{Q}), (D',\mathbb{Q}), (\mathbb{Q},D), (\mathbb{Q},D')\}.$$

Corollary 9.2. *Let $\phi : E \to E'$ be a rational cyclic isogeny of composite degree N between non-CM elliptic curves over $\mathbb{Q}$. The possible degrees are*

$$N \in \{4, 6, 8, 9, 10, 12, 15, 16, 18, 21, 25\}.$$

If N is odd, then $F_{p,q}(E) = F_{p,q}(E')$ for every distinct prime pair. If N is even, only intersections at pairs $\{2, q\}$ can differ, and the possible ordered pairs are given in tables 6 and 7. Every pair allowed by these tables occurs for infinitely many distinct source j-invariants.

We list the possible ordered pairs $(F_{2,q}(E), F_{2,q}(E'))$ for a cyclic N-isogeny $E \to E'$ in two tables. For $q \geq 7$, the only possible nontrivial intersection field is W_q. We treat $q = 3, 5$ separately because additional quadratic intersection fields can occur.

N	Pairs for $q \geq 7$	Conditions for occurrence
4	$\{\mathbb{Q}, W_q\}^2$	(W_q, W_q) occurs exactly when $q \equiv 1 \pmod 4$.
6, 8	$\mathcal{P}(W_q)$	No further restriction.
10, 12, 16, 18	$\mathcal{P}(W_q)$	A nontrivial pair occurs exactly when $r_N(q) > 0$; otherwise only $(\mathbb{Q},\mathbb{Q})$ occurs.

TABLE 6. The $(2, q)$-intersection fields across a cyclic composite-degree isogeny, for $q \geq 7$.

N	$q = 3$	$q = 5$
4	$\mathcal{P}(W_3)$ for full mod 3 image; $\mathcal{P}(M, M')$ when a rational 3-isogeny is present.	$\{\mathbb{Q}, W_5\}^2$
6	The pairs in the Borel rows of table 1.	$\mathcal{P}(W_5)$
8	$\mathcal{P}(W_3)$	$\mathcal{P}(W_5)$
10	$(\mathbb{Q},\mathbb{Q})$	$\mathcal{P}(T_5, T_5')$
12	$\mathcal{P}(M, M')$	$(\mathbb{Q},\mathbb{Q})$
16	$(\mathbb{Q},\mathbb{Q})$	$\mathcal{P}(W_5)$
18	$\mathcal{P}(M, M')$	$(\mathbb{Q},\mathbb{Q})$

TABLE 7. Possible endpoint intersection pairs for cyclic composite degree isogenies at $q = 3, 5$. The fields M, M' and T_5, T_5' appear only when the corresponding non-Weil quadratic subfields exist.

Proof. The possible degrees follow from the classification of rational cyclic isogenies [4, Theorem 4.6 and Remark 5.19]. The odd-degree assertion follows from proposition 3.17, while theorem 1.1(1) handles odd prime pairs.

To determine the endpoint fields, we use the isogeny matrices in [1, Table 2] to identify which vertices are connected by cyclic isogenies of each degree.

A cyclic 4-isogeny factors into two successive 2-isogenies. The graph T_4 gives the possibilities involving W_q, with the larger 2-isogeny trees contributing no additional patterns. At $q = 3$, two non-core vertices attached to the same core of S also give the pairs involving M or M'.

A cyclic 8-isogeny connects the endpoints of a path of three 2-isogenies in T_6 or T_8. At most one endpoint can have a nontrivial intersection, and T_6 realizes all such pairs. A cyclic 16-isogeny joins leaves at opposite ends of T_8, so a nontrivial intersection occurs precisely when $r_{16}(q) > 0$.

Cyclic isogenies of degrees 6 and 10 join opposite corners of $R_4(6)$ and $R_4(10)$, respectively. Their endpoint fields were determined in sections 5.3 and 7.4. Larger graphs containing a cyclic 6-isogeny give no additional patterns.

A cyclic 12-isogeny in S joins non-core vertices attached to different cores and lying on different 3-edges. Two non-core vertices joined by a 3-edge instead have cyclic degree 3; the longer path through the cores gives a noncyclic isogeny. A cyclic 18-isogeny joins opposite corners of $R_6(18)$, in different rows and at opposite ends.

Finally, section A gives

$$r_{10}(3) = r_{10}(5) = r_{12}(3) = r_{12}(5) = r_{18}(3) = r_{18}(5) = r_{16}(3) = 0.$$

On the other hand, $r_{16}(5) > 0$, as witnessed by $(45, 300)$ on $Y^2 = X^3 - 25X$. These calculations give the entries for $q = 3, 5$. Infinitude follows from proposition 9.1, and taking dual isogenies gives both orders. □

Proof of theorem 1.2. Cyclic isogenies of degrees 10, 12, 16, and 18 occur on $R_4(10)$, S, T_8, and $R_6(18)$, respectively.

In sections 5.4, 5.5, 7.4 and 8, we reduced the condition that an endpoint have intersection field W_q to a rational point problem on a genus one curve. For degrees 10, 12, and 18, these curves are birational to $\mathscr{E}_{N,q}$. For degree 16, the quartic (8.5) is isogenous to $\mathscr{E}_{16,q}$. In each case, rational torsion points correspond only to excluded parameters, as shown in those sections and lemma A.1. Thus, an intersection equal to W_q occurs if and only if $r_N(q) > 0$.

In particular, calculations in section A account for the exclusion of W_5 in degree 10 and W_3 in degrees 12 and 18.

The graph restrictions show that the other endpoint has intersection field $\mathbb{Q}$. When $r_N(q) > 0$, proposition 9.1 yields infinitely many distinct source j-invariants realizing these intersections. Taking dual isogenies gives both ordered pairs. □

9.3. **Arbitrary isogeny degrees.**

Proposition 9.3. *Let $\psi : E \to E'$ be a rational cyclic isogeny of degree N between non-CM elliptic curves over $\mathbb{Q}$. Then the degrees of all rational isogenies $E \to E'$ are exactly Nm^2, with $m \geq 1$.*

Thus, to determine the possible intersection fields at the endpoints of an isogeny of degree d, it suffices to consider cyclic isogenies of degrees N such that $d = Nm^2$ for some positive integer m.

Proof. Since E is non-CM, $\mathrm{Hom}_{\mathbb{Q}}(E, E')$ is free of rank one. The cyclic isogeny ψ generates this group: otherwise ψ would factor through multiplication by an integer greater than one, contradicting the kernel being cyclic. Thus, every rational isogeny $E \to E'$ is an

integer multiple of ψ and has degree Nm^2 for some $m \geq 1$. Conversely, all these degrees occur. Since multiplication does not change the endpoint curves, their intersection fields are unchanged. □

In particular, an odd degree rational isogeny can change a prime-level intersection only for $\{p, q\} = \{2, 3\}$ and only in degree $3m^2$, with m odd. Conversely, composing the exceptional 3-isogenies of theorem 3.14 with $[m]$ realizes the same two intersection fields for every odd m, with infinitely many distinct source j-invariants.

Thus, the cyclic hypothesis in proposition 3.17 is essential: a noncyclic isogeny of degree 27 can change a prime-level intersection. Likewise, composing an exceptional 3-isogeny with [2] gives a noncyclic isogeny of degree 12 with unequal $(2, 3)$-intersection fields, one of which is nonabelian. For cyclic degree 12 isogenies, both intersection fields have degree at most two.

Appendix A. Rational point calculations

We record the torsion groups of the four auxiliary families and the rational points on twenty fixed curves. The accompanying code [3] verifies the descent and point count calculations for the fixed curves.

A.1. **Torsion on the four auxiliary curves.**

Lemma A.1. *For an odd prime q and $w = q^*$, the rational torsion groups of $\mathscr{E}_{10,q}$ and $\mathscr{E}_{18,q}$ are C_2, and those of $\mathscr{E}_{12,q}$ and $\mathscr{E}_{16,q}$ are $C_2 \times C_2$.*

Proof. For $\mathscr{E}_{10,q}$, the only rational point of order 2 is $(0, 0)$; the other roots require $\sqrt{-1}$. Halving $(0, 0)$ would require $5w^2$ to be square, so there is no rational point of order 4.

The curve $Y^2 = X^3 - 2X^2 + 5X$, whose quadratic twist by w is $\mathscr{E}_{10,q}$, has a rational point of order 3 at $(1, 2)$. Its 3-division polynomial factors as

$$(X - 1)(3X^3 - 5X^2 + 25X + 25).$$

The cubic factor is irreducible over $\mathbb{Q}$, so this gives the only rational 3-isogeny. On $\mathscr{E}_{10,q}$, the nonzero points in its kernel have $X = w$ and $Y^2 = 4w^3$. Since $w = q^*$ is nonsquare, these points are not rational. Thus, there is no rational 3-torsion.

A rational point of order 5 or 7 would, together with the existing rational 2 and 3-isogenies, give a forbidden cyclic isogeny of degree 30 or 42. Mazur's torsion theorem [4, Theorem 4.1] therefore gives C_2.

For $\mathscr{E}_{12,q}$, the roots are $0, w, -3w$. A point $(e_i, 0)$ can be halved over $\mathbb{Q}$ only if both $e_i - e_j$ and $e_i - e_k$ are rational squares. This fails at all three roots, so there is no rational 4-torsion. For $w = 1$, the 3-division polynomial is $3X^4 + 8X^3 - 18X^2 - 9$, which is irreducible mod 5. Thus, this curve has no rational 3-isogeny, and neither does any of its quadratic twists. In particular, $\mathscr{E}_{12,q}$ has no rational 3-torsion. Mazur's theorem now gives $C_2 \times C_2$.

For $\mathscr{E}_{16,q}$, the same halving criterion at the roots $0, q, -q$ excludes rational 4-torsion. A rational point of order 3 would give a rational solution to $3z^4 - 6z^2 - 1 = 0$, obtained from the 3-division polynomial by setting $X = qz$. There is no such solution. Again, Mazur's theorem gives $C_2 \times C_2$.

For $\mathscr{E}_{18,q}$, the only rational point of order 2 is $(-w, 0)$. Translating this point to the origin gives $Y^2 = X^3 - 3wX^2 + 3w^2X$. Halving $(0, 0)$ would require $3w^2$ to be square, so there is no rational 4-torsion. The 3-division polynomial in the original coordinates is

$3X(X^3+4w^3)$. The cubic factor has no rational root, while $X=0$ would require $Y^2=w^3$, which is impossible. Thus, there is no rational 3-torsion.

Finally, for each prime $p\in\{5,11,17\}$ with $p\neq q$, the curve has good reduction and $\#\mathscr{E}_{18,q}(\mathbb{F}_p)=p+1$, since cubing is bijective over $\mathbb{F}_p$. At least two of these primes differ from q, and any two of the corresponding group orders $6,12,18$ have greatest common divisor 6. Thus, the rational torsion subgroup has order dividing 6. Since it contains a point of order 2 but no point of order 3, it is C_2.

□

A.2. **The fixed obstruction curves.** Write $E(a,b):Y^2=X^3+aX^2+bX$.

Lemma A.2. *Every curve in table 8 has rank zero. Its rational points are O, the points $(x,0)$ at the rational roots of x^3+ax^2+bx, and the additional points listed in the table.*

a	b	Additional points	a	b	Additional points
0	−1	none	−15	75	none
0	−4	none	9	27	none
−3	3	$(1,\pm1),(3,\pm3)$	0	−9	none
2	−3	$(-1,\pm2),(3,\pm6)$	−10	9	none
−2	−3	none	30	81	none
6	−27	none	−6	5	none
−6	−27	none	−1	1	$(1,\pm1)$
6	45	none	3	9	$(3,\pm9)$
−10	125	none	−18	−27	none
10	−75	none	−30	125	none

TABLE 8. The fixed rank-zero curves. "Additional points" means points with nonzero Y-coordinate.

Proof. The accompanying code [3] provides the calculations for all twenty curves, including certificates for the descent computations. The listed points therefore give the complete rational point sets. □

For the short Weierstrass models used in the normalizer and $X_0(10)$ arguments, the changes $X=x-6$, $X=x-2$, and $X=x-10$ identify $Y^2=X^3-135X-594$, $Y^2=X^3-7X-6$, and $Y^2=X^3-175X-750$ with $E(-18,-27)$, $E(-6,5)$, and $E(-30,125)$, respectively. The changes $X=x+3$ and $X=x-1$ identify $Y^2=X^3-27$ and $Y^2=X^3+1$ with $E(9,27)$ and $E(-3,3)$.

The rank-zero calculations in table 8 imply

$$r_{10}(3)=r_{10}(5)=r_{12}(3)=r_{12}(5)=r_{18}(3)=r_{18}(5)=r_{16}(3)=0.$$

For $N=18$, we obtain the models in the table by translating the rational 2-torsion point $(-w,0)$ to $(0,0)$.

References

1. Alexander J. Barrios, *Explicit classification of isogeny graphs of rational elliptic curves*, Int. J. Number Theory **19** (2023), no. 4, 913–936.
2. Julio Brau and Nathan Jones, *Elliptic curves with* 2*-torsion contained in the* 3*-torsion field*, Proc. Amer. Math. Soc. **144** (2016), no. 3, 925–936.
3. Michael Cerchia, *Verification code for Prime-level entanglements under rational isogeny*, Accompanying source files, 2026.
4. Garen Chiloyan and Álvaro Lozano-Robledo, *A classification of isogeny-torsion graphs of* $\mathbb{Q}$*-isogeny classes of elliptic curves*, Trans. London Math. Soc. **8** (2021), no. 1, 1–34.
5. Harris B. Daniels and Álvaro Lozano-Robledo, *Coincidences of division fields*, Ann. Inst. Fourier (Grenoble) **73** (2023), no. 1, 163–202.
6. Harris B. Daniels, Álvaro Lozano-Robledo, and Jackson S. Morrow, *Towards a classification of entanglements of Galois representations attached to elliptic curves*, Rev. Mat. Iberoam. **39** (2023), no. 3, 803–844, Updated version available as arXiv:2105.02060v4.
7. Harris B. Daniels and Jackson S. Morrow, *A group theoretic perspective on entanglements of division fields*, Trans. Amer. Math. Soc. Ser. B **9** (2022), 827–858.
8. Tim Evink, Jaap Top, and Jakob Dirk Top, *A remark on prime (non)congruent numbers*, Quaest. Math. **45** (2022), no. 12, 1841–1853.
9. Kate Finnerty, Tyler Genao, Jacob Mayle, and Rakvi, *The possible adelic indices for elliptic curves admitting a rational cyclic isogeny*, 2026, arXiv:2512.00652v2.
10. Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.
11. Nathan Jones and Ken McMurdy, *Elliptic curves with non-abelian entanglements*, New York J. Math. **28** (2022), 182–229.
12. M. A. Kenku, *On the number of* $\mathbb{Q}$*-isomorphism classes of elliptic curves in each* $\mathbb{Q}$*-isogeny class*, J. Number Theory **15** (1982), no. 2, 199–202.
13. Pedro Lemos, *Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies*, Trans. Amer. Math. Soc. **371** (2019), no. 1, 137–146.
14. Álvaro Lozano-Robledo, *Division fields of elliptic curves with minimal ramification*, Rev. Mat. Iberoam. **31** (2015), no. 4, 1311–1332.
15. Barry Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), no. 2, 129–162.
16. Rakvi, *On possibilities of* 3*-adic Galois images associated to isogeny-torsion graphs*, 2025, arXiv:2307.04074v2.
17. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
18. ———, *Topics in Galois theory*, 2 ed., Research Notes in Mathematics, vol. 1, A K Peters, Ltd., Wellesley, MA, 2008.
19. Andrew V. Sutherland, *Computing images of galois representations attached to elliptic curves*, Forum of Mathematics, Sigma **4** (2016), e4.
20. The LMFDB Collaboration, *The L-functions and modular forms database*, https://www.lmfdb.org, 2026, Accessed July 2026.
21. Jacques Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241.
22. David Zywina, *On the possible images of the mod* ℓ *representations associated to elliptic curves over* $\mathbb{Q}$, 2015, arXiv:1508.07660.
23. ———, *On the surjectivity of mod* ℓ *representations associated to elliptic curves*, Bull. Lond. Math. Soc. **54** (2022), no. 6, 2404–2417.

Department of Mathematics, The University of Maine, Orono, ME 04469
Email address: mjcerchia@gmail.com