

Pacific Journal of Mathematics

**TORSION OF RATIONAL ELLIPTIC CURVES
OVER THE MAXIMAL ABELIAN EXTENSION OF \mathbb{Q}**

MICHAEL CHOU

TORSION OF RATIONAL ELLIPTIC CURVES OVER THE MAXIMAL ABELIAN EXTENSION OF \mathbb{Q}

MICHAEL CHOU

Let E be an elliptic curve defined over \mathbb{Q} , and let \mathbb{Q}^{ab} be the maximal abelian extension of \mathbb{Q} . In this article we classify the groups that can arise as $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ up to isomorphism. The method illustrates techniques for finding explicit models of modular curves of mixed level structure. Moreover, we provide an explicit algorithm to compute $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ for any elliptic curve E/\mathbb{Q} .

1. Introduction and notation

Let K denote a number field, and let E be an elliptic curve over K . The Mordell–Weil theorem states that the group of K -rational points on E form a finitely generated abelian group. In particular, letting $E(K)$ denote the K -rational points on E , we have that

$$E(K) \cong \mathbb{Z}^{r_K} \oplus E(K)_{\text{tors}}$$

for some finite group $E(K)_{\text{tors}}$, called the torsion of E over K . In fact, due to a theorem of Merel [1996], there is a bound on the size of the torsion subgroup that depends only on the degree of K over \mathbb{Q} . Thus, there is a finite list of torsion subgroups that appear as $E(K)_{\text{tors}}$ as K varies over number fields of a fixed degree d and E/K varies. Let $\Phi(d)$ denote the set of torsion subgroups (up to isomorphism) that appear as $E(K)_{\text{tors}}$ for some elliptic curve E/K as K ranges over all number fields of a fixed degree d over \mathbb{Q} . In particular, Mazur [1978] determined $\Phi(1)$. Not many other values of $\Phi(d)$ have been determined. The set $\Phi(2)$ was classified by Kamienny [1992] and Kenku and Momose [1988], and the set $\Phi(3)$ was classified by Derickx, Etropolski, Morrow, van Hoeij, and Zureick-Brown [Derickx et al. \geq 2019].

Classifying torsion subgroups of elliptic curves over number fields is equivalent to classifying points on the modular curves $X_1(M, N)$ defined over these number fields. Thus, the classification of $\Phi(d)$ involves determining all such modular curves with K -rational points for any number field K of degree d over \mathbb{Q} .

MSC2010: primary 11G05; secondary 14H52.

Keywords: elliptic curves, torsion, abelian, extension.

One may also ask a more refined question. Let $\Phi_{\mathbb{Q}}(d)$ denote the set of torsion subgroups (up to isomorphism) that appear as $E(K)_{\text{tors}}$ for some elliptic curve E/\mathbb{Q} as K ranges over all number fields of degree d over \mathbb{Q} . Notice that necessarily $\Phi_{\mathbb{Q}}(d) \subseteq \Phi(d)$ since we are restricting the set of elliptic curves we are considering. Of course, $\Phi_{\mathbb{Q}}(1) = \Phi(1)$. The sets $\Phi_{\mathbb{Q}}(2)$ and $\Phi_{\mathbb{Q}}(3)$ were determined by Najman [2016]. A subset of $\Phi_{\mathbb{Q}}(4)$, namely $E(K)_{\text{tors}}$ for $[K : \mathbb{Q}] = 4$ and K/\mathbb{Q} abelian, was classified by the author [Chou 2016], and $\Phi_{\mathbb{Q}}(4)$ has been determined by González-Jiménez and Najman [2016]. For a more in-depth summary of what is known about torsion of elliptic curves over number fields of a fixed degree d , see for instance the introduction of [Chou 2016].

In the setting of modular curves, these torsion subgroups can be viewed as K -rational points for some $[K : \mathbb{Q}] = d$ on $X_1(M, N)$ whose image under the j -map is in \mathbb{Q} . These elliptic curves obtain the torsion structure $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ over a degree- d number field as they correspond to a K -rational point on $X_1(M, N)$, but their j -invariants are in \mathbb{Q} , as each elliptic curve can be defined over \mathbb{Q} .

One can also consider torsion over an infinite extension L of \mathbb{Q} . For a fixed algebraic extension L of \mathbb{Q} , let $\Phi_{\mathbb{Q}}(L)$ denote the set of torsion subgroups $E(L)_{\text{tors}}$ up to isomorphism that appear as E/\mathbb{Q} varies. The Mordell–Weil theorem no longer applies, and so a priori it is not guaranteed that the size of $E(L)_{\text{tors}}$ is finite, let alone uniformly bounded as E varies. Even so, in certain infinite extensions the number of torsion points is finite and, in fact, uniformly bounded as E varies. Fujita determined $\Phi_{\mathbb{Q}}(\mathbb{Q}(2^{\infty}))$ where $\mathbb{Q}(2^{\infty})$ is the compositum of all degree-2 extensions of \mathbb{Q} , i.e., $\mathbb{Q}(2^{\infty}) := \mathbb{Q}(\{\sqrt{m} : m \in \mathbb{Z}\})$.

Theorem 1.1 [Fujita 2005, Theorem 2].

$$\Phi_{\mathbb{Q}}(\mathbb{Q}(2^{\infty})) = \begin{cases} \mathbb{Z}/N_1\mathbb{Z}, & N_1 = 1, 3, 5, 7, 9, 15, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 1, 2, 3, 4, 5, 6, 8, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4N_4\mathbb{Z}, & N_4 = 1, 2, 3, 4, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}. \end{cases}$$

Torsion over a similar infinite extension, $\mathbb{Q}(3^{\infty})$, the compositum of all cubic number fields, was studied by Daniels, Lozano-Robledo, Najman, and Sutherland [Daniels et al. 2018]. They classify $\Phi_{\mathbb{Q}}(\mathbb{Q}(3^{\infty}))$. Moreover, they determine which of these torsion structures appear infinitely often and which appear for only finitely many isomorphism classes of elliptic curves.

Here is some notation that will be used throughout the paper: $E[p^{\infty}]$ denotes torsion points of order a power of p and \mathbb{Q}^{ab} denotes the maximal abelian extension

of \mathbb{Q} . By the Kronecker–Weber theorem we have that $\mathbb{Q}^{\text{ab}} = \mathbb{Q}(\{\zeta_n : n \in \mathbb{Z}^+\})$ where ζ_n denotes a primitive n -th root of unity.

Given an abelian variety A/\mathbb{Q} , the torsion subgroup of $A(\mathbb{Q}^{\text{ab}})$ is finite (this is due to a theorem of Ribet [1981]). Thus, one can ask if there is a uniform bound for the size of such a torsion subgroup or whether there are possibly infinitely many torsion structures that appear. If we restrict to genus-1 abelian varieties, we prove there are only finitely many groups that appear as $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ for any elliptic curve E/\mathbb{Q} . In fact, we completely determine $\Phi_{\mathbb{Q}}(\mathbb{Q}^{\text{ab}})$.

Theorem 1.2. *Let E/\mathbb{Q} be an elliptic curve. Then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ is isomorphic to one of the following groups:*

$$\begin{aligned} \mathbb{Z}/N_1\mathbb{Z}, & \quad N_1 = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 37, 43, 67, 163, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, & \quad N_2 = 1, 2, \dots, 9, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3N_3\mathbb{Z}, & \quad N_3 = 1, 3, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4N_4\mathbb{Z}, & \quad N_4 = 1, 2, 3, 4, \\ \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, & \\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}. & \end{aligned}$$

Each of these groups appears as $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ for some elliptic curve over \mathbb{Q} .

A uniform bound on the size of $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ for all elliptic curves E/\mathbb{Q} is an easy corollary of the classification.

Corollary 1.3. *Let E/\mathbb{Q} be an elliptic curve. Then $\#E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \leq 163$. This bound is sharp, as the curve 26569a1 has a point of order 163 over \mathbb{Q}^{ab} .*

In Section 2 we discuss what is known about isogenies of elliptic curves over \mathbb{Q} . We then discuss the intimate connection between isogenies and torsion points over \mathbb{Q}^{ab} . In Section 4 we use the results from Section 2 to prove bounds on the group $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ based on the isogenies E has over \mathbb{Q} . In Section 5 we further refine the bounds to eliminate the possibility of any group not appearing in Theorem 1.2. In Section 6 we construct an algorithm to determine $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ for any elliptic curve E/\mathbb{Q} . Finally, Section 7 has, for each subgroup T appearing in Theorem 1.2, an example of an elliptic curve E/\mathbb{Q} such that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong T$, completing the proof of Theorem 1.2. We use Cremona labels for our elliptic curves, and more information on each curve can be found on the LMFDB [2013].

2. Isogenies

In the rest of the paper, when we refer to an isogeny, we will mean a cyclic \mathbb{Q} -rational isogeny. The classification of \mathbb{Q} -rational n -isogenies is an integral part of the classification of torsion of elliptic curves E/\mathbb{Q} over \mathbb{Q}^{ab} .

Theorem 2.1 (Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, and Ogg, among others). *If E/\mathbb{Q} has an n -isogeny, $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$. If E does not have complex multiplication, then $n \leq 18$ or $n \in \{21, 25, 37\}$.*

See [Lozano-Robledo 2013, §9] for a more detailed discussion of this theorem. Moreover, there is a detailed bound on the number of \mathbb{Q} -isogenies an elliptic curve can have. The following theorem is from [Kenku 1982], combining Theorem 2 and the surrounding discussion.

Theorem 2.2 [Kenku 1982]. *There are at most eight \mathbb{Q} -isomorphism classes of elliptic curves in each \mathbb{Q} isogeny class.*

Let $C_p(E)$ denote the number of distinct \mathbb{Q} -rational cyclic subgroups of order p^n for any $n \geq 0$ of E . Then, we have the following table for bounds on C_p for any elliptic curve over \mathbb{Q} :

p	2	3	5	7	11	13	17	19	37	43	67	163	else
C_p	8	4	3	2	2	2	2	2	2	2	2	2	1

In particular, fix a \mathbb{Q} -isogeny class and a representative E of that class. Let $C(E) = \prod_p C_p(E)$.

- *If $C_p(E) = 2$ for some prime $p \geq 11$, then $C_q(E) = 1$ for all other primes. So $C(E) = 2$.*
- *If $C_7(E) = 2$, then $C_5(E) = 1$ and either $C_3(E) \leq 2$ and $C_2(E) = 1$ or $C_3(E) = 1$ and $C_2(E) \leq 2$. All these yield $C(E) \leq 4$.*
- *If $C_5(E) = 3$, then $C_p(E) = 1$ for all primes $p \neq 5$.*
- *If $C_5(E) = 2$, then either $C_3(E) \leq 2$ and $C_2(E) = 1$ or $C_3(E) = 1$ and $C_2(E) \leq 2$. Hence, $C(E) \leq 4$.*
- *If $C_3(E) = 4$, then there exists a representative of the class of E with a \mathbb{Q} -rational cyclic subgroup of order 27, and $C_2(E) = 1$ so $C(E) \leq 4$.*
- *If $C_3(E) = 3$, then $C_2(E) \leq 2$ so that $C(E) \leq 6$.*
- *If $C_3(E) \leq 2$, then $C_2(E) \leq 4$ so that $C(E) \leq 8$.*

Note the fact that $C(E) = 8$ is possible only if $C_2(E) = 8$ or $C_3(E) = 2$ and $C_2(E) = 4$.

The first connection between isogenies and points over \mathbb{Q}^{ab} is shown in the following lemma.

Lemma 2.3. *If E/\mathbb{Q} has an n -isogeny defined over \mathbb{Q} , then $E(\mathbb{Q}^{\text{ab}})$ has a point of order n .*

Proof. Let φ denote the n -isogeny over \mathbb{Q} . Then $\ker(\varphi) = \langle P \rangle$ for some point $P \in E(\overline{\mathbb{Q}})$ of order n such that $\langle P \rangle^\sigma = \langle P \rangle$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This induces a character

$$\psi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

defined by $\sigma \mapsto a \bmod n$ where a is given by $\sigma(P) = aP$. The kernel of ψ is precisely $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(P))$, and thus, we have that $\text{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, and hence abelian. Therefore, $P \in E(\mathbb{Q}^{\text{ab}})$. \square

Given an elliptic curve E/\mathbb{Q} , due to Ribet's theorem we know that there exists $m, n \in \mathbb{Z}^{\geq 0}$ such that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$. We wish to understand what possible m and n can occur together.

In regards to the values of m , normally one could use an argument via the Weil pairing which implies that our field must contain ζ_m ; however, this is not very restrictive when looking at torsion over \mathbb{Q}^{ab} . Instead, we have the following theorem.

Theorem 2.4 [González-Jiménez and Lozano-Robledo 2016, Theorem 1.1]. *Let E/\mathbb{Q} be an elliptic curve. If there is an integer $n \geq 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4$, or 5 . More generally, if $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian, then $n = 2, 3, 4, 5, 6$, or 8 . Moreover, $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is isomorphic to one of the following groups:*

n	2	3	4	5	6	8
$\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$	$\{0\}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^4$
	$\mathbb{Z}/2\mathbb{Z}$	$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$(\mathbb{Z}/2\mathbb{Z})^3$	$(\mathbb{Z}/2\mathbb{Z})^5$
	$\mathbb{Z}/3\mathbb{Z}$		$(\mathbb{Z}/2\mathbb{Z})^3$	$(\mathbb{Z}/4\mathbb{Z})^2$		$(\mathbb{Z}/2\mathbb{Z})^6$
			$(\mathbb{Z}/2\mathbb{Z})^4$			

Furthermore, each possible Galois group occurs for infinitely many distinct j -invariants.

In fact, if $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$, both values m and n are controlled primarily by isogenies. For instance, in the proof of Theorem 2.4, González-Jiménez and Lozano-Robledo make use of a key corollary relating full- p -torsion over \mathbb{Q}^{ab} to \mathbb{Q} -rational p -isogenies.

Corollary 2.5 [González-Jiménez and Lozano-Robledo 2016, Corollary 3.9]. *Let E/\mathbb{Q} be an elliptic curve, let $p > 2$ be a prime, and suppose that $\mathbb{Q}(E[p])/\mathbb{Q}$ is abelian. Then, the \mathbb{Q} -isogeny class of E contains at least three distinct \mathbb{Q} -isomorphism classes, and $C_p(E) \geq 3$. In particular $p \leq 5$.*

In particular, the proof of Corollary 2.4 in [González-Jiménez and Lozano-Robledo 2016] shows that for all $p > 2$, if $\mathbb{Q}(E[p])/\mathbb{Q}$ is abelian for some E/\mathbb{Q} , then E has two independent p -isogenies over \mathbb{Q} . Note that the converse is also true.

Lemma 2.6. *Let E/\mathbb{Q} be an elliptic curve, let p be a prime, and suppose that E has two distinct p -isogenies over \mathbb{Q} . Then $\mathbb{Q}(E[p])/\mathbb{Q}$ is abelian.*

Proof. Let $\rho_{E,p} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(E[p]) \cong \text{GL}(2, p)$ denote the mod p Galois representation associated to E . Since E has two independent p -isogenies, there exists a basis $\{P, Q\}$ of $E[p]$ so that the image of $\rho_{E,p}$ is contained in a split Cartan subgroup of $\text{GL}(2, p)$. Now, since $\ker \rho_{E,p} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(E[p]))$, it follows that

$$\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(P, Q)/\mathbb{Q}) \cong \rho_{E,p}(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$$

which is contained in split Cartan subgroup and thus abelian. \square

Note that we can see in [González-Jiménez and Lozano-Robledo 2016, Table 1] a complete table showing which elliptic curves with complex multiplication (CM) can have $\mathbb{Q}(E[n])$ abelian for which n . We also have the following lemma to help understand the possible values of n .

Lemma 2.7. *Let K be a Galois extension of \mathbb{Q} and E an elliptic curve over \mathbb{Q} . If $E(K)_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$, then E has an n -isogeny over \mathbb{Q} .*

Proof. Suppose $E(K)_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z} = \langle P, Q \rangle$ where P has order m and Q has order mn . Then $[m]E(K)_{\text{tors}} = \langle mP, mQ \rangle = \langle mQ \rangle \cong \mathbb{Z}/n\mathbb{Z}$. Let $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Since K is Galois over \mathbb{Q} and E is defined over \mathbb{Q} , we have

$$Q^\sigma \in E(K)_{\text{tors}},$$

and since the action of Galois commutes with multiplication by m ,

$$(mQ)^\sigma = m(Q^\sigma) \in [m]E(K)_{\text{tors}} = \langle mQ \rangle.$$

Thus, $\langle mQ \rangle$ is a cyclic subgroup of order n that is stable under the action of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, which implies E has an n -isogeny over \mathbb{Q} . \square

Thus, the possible values for m (up to a power of 2) and n are controlled by the \mathbb{Q} -isogenies of the elliptic curve.

3. Points of order 2^n

In order to understand $E(\mathbb{Q}_{\text{ab}})[2^\infty]$ and its connection to isogenies, we will use the database of Rouse and Zureick-Brown [2015]. First we prove a simple lemma concerning quadratic twists.

Lemma 3.1. *Let E/\mathbb{Q} be an elliptic curve, let d be a square-free integer, and let E_d denote the quadratic twist of E by d . Then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong E_d(\mathbb{Q}^{\text{ab}})_{\text{tors}}$.*

Proof. Since E and E_d become isomorphic over $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}^{\text{ab}}$ for any d , the lemma follows immediately. \square

Note that the minimal field of definition of the torsion for E and E_d may differ, but by the previous lemma their torsion over \mathbb{Q}^{ab} will always be isomorphic. In particular, when examining elliptic curves with j -invariant not equal to 0 or 1728, it suffices to fix a specific curve E , and examine $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$.

The following lemma gives a criterion for a point to be halved which will be handy to explicitly compute $\mathbb{Q}(E[2^k])$ for various k :

Lemma 3.2 [Knapp 1992, Theorem 4.2, p. 85]. *Let K be a field of characteristic not equal to 2 or 3 and E an elliptic curve over K given by $y^2 = (x - \alpha)(x - \beta)(x - \gamma)$ with α, β, γ in K . For $P = (x, y) \in E(K)$, there exists a K -rational point $Q = (x', y')$ on E such that $[2]Q = P$ if and only if $x - \alpha$, $x - \beta$, and $x - \gamma$ are all squares in K . In this case, if we fix the sign of $\sqrt{x - \alpha}$, $\sqrt{x - \beta}$, and $\sqrt{x - \gamma}$, then x' equals one of*

$$\sqrt{x - \alpha}\sqrt{x - \beta} \pm \sqrt{x - \alpha}\sqrt{x - \gamma} \pm \sqrt{x - \beta}\sqrt{x - \gamma} + x$$

or

$$-\sqrt{x - \alpha}\sqrt{x - \beta} \pm \sqrt{x - \alpha}\sqrt{x - \gamma} \mp \sqrt{x - \beta}\sqrt{x - \gamma} + x$$

where the signs are taken simultaneously.

In particular, we can prove a nice criterion for an elliptic curve having a point of order 4 over \mathbb{Q}^{ab} , but not full 4-torsion. We will make use of the following proposition describing the Galois group of various degree-4 polynomials.

Proposition 3.3 [Conrad 2012, Corollary 4.5]. *Let $f(X) = X^4 + bX^2 + d$ be irreducible in $K[X]$, where K does not have characteristic 2. Its Galois group over K , denoted G_f , is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, or D_4 according to the following conditions:*

- (1) *If $d \in (K^\times)^2$, then $G_f = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*
- (2) *If $d \notin (K^\times)^2$ and $(b^2 - 4d)d \in (K^\times)^2$, then $G_f = \mathbb{Z}/4\mathbb{Z}$.*
- (3) *If $d \notin (K^\times)^2$ and $(b^2 - 4d)d \notin (K^\times)^2$, then $G_f = D_4$.*

We combine this result with Lemma 3.2 to prove the following lemma.

Lemma 3.4. *Suppose E is an elliptic curve over \mathbb{Q} that has a point of order 4 over \mathbb{Q}^{ab} but does not have full 4-torsion defined over \mathbb{Q}^{ab} . Then, either $C_2(E) \geq 4$, or there is a model of E of the form*

$$E : y^2 = x(x^2 + bx + d)$$

and either d or $(b^2 - 4d)d$ is a nonzero perfect square in \mathbb{Q} .

Proof. Suppose that $C_2(E) < 4$. By Lemma 2.7 if E has a point of order 4 but not full 4-torsion defined over \mathbb{Q}^{ab} , then E has at least one 2-isogeny over \mathbb{Q} . Thus, there exists a point P of order 2 defined over \mathbb{Q} , and by moving that point to $P = (0, 0)$

we obtain a model for E of the form $y^2 = x(x^2 + bx + d) = x(x - \alpha)(x - \bar{\alpha})$ with $b, d \in \mathbb{Q}$ and $\alpha, \bar{\alpha} \notin \mathbb{Q}$. If $\alpha, \bar{\alpha} \in \mathbb{Q}$, then $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which would imply $C_2(E) \geq 4$.

Over \mathbb{Q}^{ab} we have a point of order 4, say Q . Suppose first that this point lies above a rational point of order 2. Without loss of generality we have $2Q = P = (0, 0)$. Writing $E : y^2 = x(x - \alpha)(x - \bar{\alpha})$, Lemma 3.2 says that we have that $\sqrt{-\alpha}$ and $\sqrt{-\bar{\alpha}}$ must be elements in \mathbb{Q}^{ab} . Notice that $\sqrt{-\alpha}$ and $\sqrt{-\bar{\alpha}}$ satisfy the polynomial

$$f = x^4 - bx^2 + d.$$

We prove that this polynomial is irreducible, and hence the minimal polynomial of $\sqrt{-\alpha}$ and $\sqrt{-\bar{\alpha}}$ over \mathbb{Q} .

Suppose f is reducible; then $[\mathbb{Q}(x(Q)) : \mathbb{Q}] = 1$ or 2 . If $[\mathbb{Q}(x(Q)) : \mathbb{Q}] = 1$, then there is a quadratic twist of E , say E' , with $E'(\mathbb{Q})_{\text{tors}}$ having a point of order 4. Then, E' has a 4-isogeny, so E' is 2-isogenous to an elliptic curve E'' with full 2-torsion over \mathbb{Q} by [González-Jiménez and Najman 2016, Lemma 8.14]. Since E'' has full 2-torsion over \mathbb{Q} , it has isogenies of degrees 1, 2, 2, and 2, with one of those curves being E' . Therefore, E' has isogenies of degrees 1, 2, 4, and 4. Since E is a quadratic twist of E' , it also has isogenies of degrees 1, 2, 4, and 4. This contradicts the assumption that $C_2(E) < 4$. If $[\mathbb{Q}(x(Q)) : \mathbb{Q}] = 2$, then f factors over $\mathbb{Q}[x]$ as

$$f = (x^2 + \alpha)(x^2 + \bar{\alpha}),$$

which implies $\alpha \in \mathbb{Q}$. As mentioned above, this contradicts $C_2(E) < 4$. Thus, f is irreducible, and is the minimal polynomial of $\sqrt{-\alpha}$ and $\sqrt{-\bar{\alpha}}$ over \mathbb{Q} .

Since $Q \in E(\mathbb{Q}^{\text{ab}})$, the Galois group of f over \mathbb{Q} is abelian. Therefore, $G_f = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. Now by Proposition 3.3 the two cases above follow.

Suppose instead that our point of order 4 is halving a point of order 2 that is not rational. Without loss of generality we may assume $2Q = (\alpha, 0)$. By Lemma 3.2 we have that α and $\alpha - \bar{\alpha}$ are squares in \mathbb{Q}^{ab} . However, since $\sqrt{-1} \in \mathbb{Q}^{\text{ab}}$ it also follows that $-\alpha$ and $-\bar{\alpha}$ are squares in \mathbb{Q}^{ab} . Thus, the point $(0, 0)$ is also halved in \mathbb{Q}^{ab} , contradicting our original assumption that E does not have full 4-torsion over \mathbb{Q}^{ab} . \square

We now prove our proposition relating 2-powered torsion to the isogenies of an elliptic curve.

Proposition 3.5. *Let E/\mathbb{Q} be an elliptic curve. Table 1 gives the possibilities for $E(\mathbb{Q}^{\text{ab}})[2^\infty]$, the 2-powered isogenies attached to each case, and also $C_2(E)$.*

Proof. If E does not have CM, it must be in one of the families given in the Rouse–Zureick-Brown database [2015]. We compute for each family the 2-powered

$E(\mathbb{Q}^{\text{ab}})[2^\infty]$	isogeny degrees	$C_2(E)$
$\{\mathbb{O}\}$	1	1
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	1	1
	1, 2	2
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	1, 2	2
	1, 2, 4, 4	4
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	1, 2, 4, 4	4
	1, 2, 4, 4, 8, 8	6
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	1, 2, 2, 2	4
	1, 2, 4, 4	4
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$	1, 2, 4, 4, 8, 8, 16, 16	8
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	1, 2, 2, 2, 4, 4	6
	1, 2, 4, 4, 8, 8, 8, 8	8
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$	1, 2, 2, 2, 4, 4, 8, 8	8
$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	1, 2, 2, 2, 4, 4, 4, 4	8

Table 1. Possible 2-primary torsion over \mathbb{Q}^{ab} .

torsion over \mathbb{Q}^{ab} . We do this as follows: for each family let G be the image of $\rho_{E,32}$, that is $G = \rho_{E,32}(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$. In fact,

$$G = \rho_{E,32}(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) \cong \text{Gal}(\mathbb{Q}(E[32])/\mathbb{Q})$$

since $\ker \rho_{E,32} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(E[32]))$. Then the commutator subgroup $[G, G]$ has fixed field equal to $\mathbb{Q}(E[32]) \cap \mathbb{Q}^{\text{ab}}$. We fix a $\mathbb{Z}/32\mathbb{Z}$ -basis $\{P, Q\}$ of $E[32]$ and identify G with a subgroup of $\text{GL}(2, 32)$. We then compute the vectors fixed in $(\mathbb{Z}/32\mathbb{Z})^2$ by $[G, G]$, which gives the structure of the points on E defined over $\mathbb{Q}(E[32]) \cap \mathbb{Q}^{\text{ab}}$, that is the structure of $E(\mathbb{Q}^{\text{ab}})[32]$. Here, a vector $[a, b] \in (\mathbb{Z}/32\mathbb{Z})^2$ corresponds to a point $aP + bQ \in E[32]$. Since the largest-order point found in $E(\mathbb{Q}^{\text{ab}})[32]$ has order 16, we see that $E(\mathbb{Q}^{\text{ab}})[2^\infty] = E(\mathbb{Q}^{\text{ab}})[16]$.

For elliptic curves with CM we examine the finitely many j -invariants over \mathbb{Q} [González-Jiménez and Lozano-Robledo 2016, Table 1]. The table is broken up into quadratic twist families by j -invariant. For $j \neq 0, 1728$, there are only finitely many quadratic twist families, and so by Lemma 3.1 it suffices to fix a single curve within each family and examine its torsion over \mathbb{Q}^{ab} .

Let E be such a curve. From that table we can see the largest m such that $\mathbb{Q}(E[2^m])$ is abelian, as well as the isogenies each \mathbb{Q} -isomorphism class has. Let 2^n denote the largest degree-2-powered isogeny E has. Then from Lemma 2.7 it follows that $E(\mathbb{Q}^{\text{ab}})[2^\infty] \subseteq \mathbb{Z}/2^m\mathbb{Z} \times \mathbb{Z}/2^{n+m}\mathbb{Z}$.

Thus, to find the structure of $E(\mathbb{Q}^{\text{ab}})[2^\infty]$ it simply remains to find the largest 2-powered torsion E has over some abelian number field, up to 2^{n+m} . We do this by using the division polynomial method. For each $0 < k \leq n + m$ we use Magma [Bosma et al. 1997] to compute the (2^k) -th-division polynomial of E , whose roots are the x -coordinates of the points of order 2^k on E . From the x -coordinates, we can compute the corresponding y -coordinates and get a list of all points of order 2^k on E . Now we simply compute the field of definition of these points and check whether each field is abelian or not. If k_0 is the first value where no points of order 2^{k_0} are defined over an abelian extension, then $E(\mathbb{Q}^{\text{ab}})[2^\infty] \cong \mathbb{Z}/2^m\mathbb{Z} \times \mathbb{Z}/2^{k_0-1}\mathbb{Z}$.

We run through each quadratic twist family. Once computed we find that we do not gain any new groups nor do we add any new 2-powered isogeny degree combinations to the list originally found for non-CM curves. Note that the code used to do these computations is available at <https://sites.tufts.edu/michaelchou/research/>.

For $j = 0$, the cases $y^2 = x^3 + t^3$ and $y^2 = x^3 + 16t^3$, where $t \in \mathbb{Q}$, are single quadratic twist families, so may be treated as above. For the case $y^2 = x^3 + s$ with $s \neq t^3, 16t^3$, [González-Jiménez and Lozano-Robledo 2016, Table 1] already shows that $E(\mathbb{Q}^{\text{ab}})[2] = \{\mathcal{O}\}$ for any of these quadratic twist families.

Similarly for $j = 1728$, the cases $y^2 = x^3 \pm t^2x$ for $t \in \mathbb{Q}$ are in two separate quadratic twist families, so may be treated as before. Finally, we consider the case $E : y^2 = x^3 + sx$, with $s \neq \pm t^2$ for any $t \in \mathbb{Q}$. We see from [González-Jiménez and Lozano-Robledo 2016, Table 1] that the largest division field that is abelian is $\mathbb{Q}(E[2])$. Suppose that E has a point of order 4 over \mathbb{Q}^{ab} ; then since $C_2(E) < 4$, Lemma 3.4 gives that s is a square in \mathbb{Q} or $-4s^2$ is a square in \mathbb{Q} , contradicting our assumption that $s \neq \pm t^2$ for any $t \in \mathbb{Q}$. Thus, $E(\mathbb{Q}^{\text{ab}})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus, the table above is complete. \square

From Table 1 we can make a simple observation:

Lemma 3.6. *Let E/\mathbb{Q} be an elliptic curve and suppose that $E(\mathbb{Q}^{\text{ab}})[2^\infty] \not\cong \{\mathcal{O}\}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then E has at least one 2-isogeny over \mathbb{Q} , that is, $C_2(E) \geq 2$.*

4. Bounding torsion

We begin with a proposition that bounds $E(\mathbb{Q}^{\text{ab}})[p^\infty]$ for all primes p .

Proposition 4.1. *Let E/\mathbb{Q} be an elliptic curve, and \mathbb{Q}^{ab} be the maximal abelian extension of \mathbb{Q} . Then the following table gives a bound on $E(\mathbb{Q}^{\text{ab}})[p^\infty]$ for all primes p , i.e., the p -power torsion is contained in the following subgroups:*

p	2	3	5	7, 11, 13, 17, 19, 37, 43, 67, 163	else
$E(\mathbb{Q}^{\text{ab}})[p^\infty] \subseteq$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$	$\mathbb{Z}/p\mathbb{Z}$	$\{\mathcal{O}\}$

Proof. Note that $E(\bar{\mathbb{Q}})[p^n] \cong \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$; thus, $E(\mathbb{Q}^{\text{ab}})[p^n] \subseteq \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ for any n . However, by Theorem 2.4, if $\mathbb{Q}(E[p^n])$ is abelian, then $p = 2, 3$, or 5 , and therefore, for any prime except $2, 3$, and 5 , we must have that E does not have full p torsion defined over \mathbb{Q}^{ab} . Thus, if $p > 5$, then $E(\mathbb{Q}^{\text{ab}})[p^\infty] \subseteq \mathbb{Z}/p^n\mathbb{Z}$ for some n . However, since \mathbb{Q}^{ab} is a Galois extension of \mathbb{Q} , Lemma 2.7 combined with Theorem 2.1 shows that $E(\mathbb{Q}^{\text{ab}})[p^\infty] \subseteq \mathbb{Z}/p\mathbb{Z}$ for $p = 7, 11, 13, 17, 19, 37, 43, 67$, and 163 , and for all other primes l larger than 5 , $E(\mathbb{Q}^{\text{ab}})[l^\infty] \cong \{0\}$.

For the prime $p = 2$, we simply refer to Table 1.

For the prime $p = 3$, first notice that E cannot have full 9-torsion over \mathbb{Q}^{ab} because of Theorem 2.4. Thus, $E(\mathbb{Q}^{\text{ab}})[3^\infty] \subseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^e\mathbb{Z}$ for some natural number e . By Lemma 2.7 if $E(\mathbb{Q}^{\text{ab}})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^e\mathbb{Z}$, then E has a 3^{e-1} isogeny. By Theorem 2.1, the largest 3-power degree rational isogeny is 27 , and so $e - 1 \leq 3$, i.e., $E(\mathbb{Q}^{\text{ab}})[3^\infty] \subseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/81\mathbb{Z}$. However, suppose that in fact $E(\mathbb{Q}^{\text{ab}})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/81\mathbb{Z}$. Then by the above argument, E has a rational 27 -isogeny. However, the only elliptic curves over \mathbb{Q} that have a 27 -isogeny are CM curves (those with j -invariant $-2^{15} \cdot 3 \cdot 5^3$ [Lozano-Robledo 2013, Table 4]). By [González-Jiménez and Lozano-Robledo 2016, Table 1] we see that such a curve does not have $\mathbb{Q}(E[n])$ abelian for any $n \geq 2$. Thus, $E(\mathbb{Q}^{\text{ab}})[3^\infty] \subseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$.

For the prime $p = 5$, first notice that E cannot have full 25-torsion over \mathbb{Q}^{ab} because of Theorem 2.4. By an identical argument as in the $p = 3$ case, we have that $E(\mathbb{Q}^{\text{ab}})[5^\infty] \subseteq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$, since the largest 5-power degree rational isogeny is 25 . However, suppose that $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \hookrightarrow E(\mathbb{Q}^{\text{ab}})[5^\infty]$. Consider the Galois representation $\rho_{E,25} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(E[25]) \cong \text{GL}(2, 25)$. Let G denote the image of $\rho_{E,25}$. Since full 5-torsion is defined over \mathbb{Q}^{ab} , Corollary 2.5 says there is a basis of $E[5]$ such that $G \bmod 5$ is contained in a split Cartan subgroup of $\text{GL}(2, 5)$. Thus, we have that

$$G \leq \mathcal{G} := \left\{ \begin{bmatrix} a & 5b \\ 5c & d \end{bmatrix} : a, d \in (\mathbb{Z}/25\mathbb{Z})^\times, b, c \in \mathbb{Z}/5\mathbb{Z} \right\}.$$

Now, let H denote the image $\rho_{E,25}(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(E[25]) \cap \mathbb{Q}^{\text{ab}}))$. Notice that $H = [G, G]$, the commutator subgroup of G . Since E has a point of order 25 over \mathbb{Q}^{ab} , we have that H must fix a vector of order 25 in $(\mathbb{Z}/25\mathbb{Z})^2$, and therefore, $[G, G]$ must also fix a vector of order 25 in $(\mathbb{Z}/25\mathbb{Z})^2$.

By the Weil pairing the image of $\rho_{E,25}$ must have determinant equal to the full group $(\mathbb{Z}/25\mathbb{Z})^\times$, and therefore, G must be a subgroup of \mathcal{G} with full determinant, and whose commutator subgroup fixes a vector of order 25 in $(\mathbb{Z}/25\mathbb{Z})^2$. Using Magma we can compute all such subgroups of $\text{GL}(2, 25)$, and further we can also compute, given a subgroup of $\text{GL}(2, 25)$, the isogenies of an elliptic curve associated with that image.

We thus compute that in fact all subgroups of \mathcal{G} with the described properties all yield a 25-isogeny, and thus, any elliptic curve with such an image must in fact have a 25-isogeny. However, since full 5-torsion was defined over \mathbb{Q}^{ab} , Corollary 2.5 gives two isogenies of degree 5 and thus it is impossible for E to have a 25-isogeny, otherwise $C_5(E) = 4$ contradicting Theorem 2.2. Thus, $E(\mathbb{Q}^{\text{ab}})[5^\infty] \subseteq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. \square

To prove bounds on the structure of $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ we will need a lemma about full 6-torsion.

Lemma 4.2 [González-Jiménez and Lozano-Robledo 2016, Lemma 3.12]. *Let E/\mathbb{Q} be an elliptic curve. If $\mathbb{Q}(E[6])/\mathbb{Q}$ is abelian, then $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.*

As has been noted in Section 2, the structure of torsion over \mathbb{Q}^{ab} is closely tied to the \mathbb{Q} -isogenies an elliptic curve has. We now prove bounds on $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ based on these isogenies.

Proposition 4.3. *Let E/\mathbb{Q} be an elliptic curve. Suppose $C_p(E) = 1$ for all primes $p \neq 2$. Then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} = E(\mathbb{Q}^{\text{ab}})[2^\infty]$ and is contained in either $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ or $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$*

Proof. By Corollary 2.5 and Lemma 2.7 it follows that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} = E(\mathbb{Q}^{\text{ab}})[2^\infty]$. Thus, $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ is one of the groups on Table 1 from Proposition 3.5. \square

Proposition 4.4. *Let E/\mathbb{Q} be an elliptic curve. Suppose E has a 3-isogeny and $C_p(E) = 1$ for all primes $p > 3$. Then*

$$E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 12, 18, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4N_4\mathbb{Z}, & N_4 = 1, 3, \text{ or} \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}. \end{cases}$$

Proof. By Theorem 2.2 we have either

- $C_3(E) = 4$ and $C_p(E) = 1$ for all primes $p \neq 3$,
- $C_3(E) = 3$ and $C_2(E) \leq 2$, or
- $C_3(E) = 2$ and $C_2(E) \leq 4$.

Suppose $C_3(E) = 4$ and $C_p(E) = 1$ for all primes $p \neq 3$. Then by Proposition 4.1 we know that $E(\mathbb{Q}^{\text{ab}})[3^\infty] \subseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$. Suppose E has full 3-torsion over \mathbb{Q}^{ab} . If E also has full 2-torsion over \mathbb{Q}^{ab} , then it has full 6-torsion over \mathbb{Q}^{ab} . Thus, by Lemma 4.2 we must have $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. This is possible only if E has a point of order 2 defined over \mathbb{Q} , but that would give a Galois stable subgroup of order 2, and hence $C_2(E) \geq 2$, a contradiction. Therefore, by Lemma 3.6 we have that $E(\mathbb{Q}^{\text{ab}})[2^\infty] \cong \{0\}$ and so $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$. Suppose instead that E does not have full 3-torsion over \mathbb{Q}^{ab} . Then $E(\mathbb{Q}^{\text{ab}})[3^\infty] \subseteq \mathbb{Z}/27\mathbb{Z}$. If

$E(\mathbb{Q}^{\text{ab}})[3^\infty] \cong \mathbb{Z}/27\mathbb{Z}$, then E has a 27-isogeny and all such curves have CM (for instance see [Lozano-Robledo 2013, Table 4]). By [González-Jiménez and Lozano-Robledo 2016, Table 1] we see that such a curve does not have full n torsion defined over \mathbb{Q}^{ab} for any n . Thus, $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} = E(\mathbb{Q}^{\text{ab}})[3^\infty] \cong \mathbb{Z}/27\mathbb{Z}$ or $E(\mathbb{Q}^{\text{ab}})[3^\infty] \subseteq \mathbb{Z}/9\mathbb{Z}$ and $E(\mathbb{Q}^{\text{ab}})[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which yields $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$.

Suppose $C_3(E) = 3$ and $C_2(E) \leq 2$. Then we have that $E(\mathbb{Q}^{\text{ab}})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$. From Table 1 the largest $E(\mathbb{Q}^{\text{ab}})[2^\infty]$ can be so that $C_2(E) = 2$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Therefore, $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$.

Suppose that $C_3(E) = 2$ and $C_2(E) \leq 4$. Then $E(\mathbb{Q}^{\text{ab}})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z}$. From Proposition 3.5 the largest $E(\mathbb{Q}^{\text{ab}})[2^\infty]$ can be so that $C_2(E) = 4$ is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Thus, $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$. \square

Proposition 4.5. *Let E/\mathbb{Q} be an elliptic curve. Suppose E has a 5-isogeny. Then*

$$E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \begin{cases} \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}. \end{cases}$$

Proof. By Theorem 2.2 we have either

- $C_5(E) = 3$ and $C_p(E) = 1$ for all primes $p \neq 5$,
- $C_5(E) = 2$, $C_3(E) \leq 2$, and $C_2(E) = 1$, or
- $C_5(E) = 2$, $C_3(E) = 1$, and $C_2(E) \leq 2$.

Suppose $C_5(E) = 3$ and $C_p(E) = 1$ for all primes $p \neq 5$. By Corollary 2.5 we see that E does not have full 3-torsion over \mathbb{Q}^{ab} . By Lemma 3.6 we have $E(\mathbb{Q}^{\text{ab}})[2^\infty] \cong \{0\}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $E(\mathbb{Q}^{\text{ab}})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, then $E(\mathbb{Q}^{\text{ab}})[2^\infty] \cong \{0\}$, since otherwise E would have full 10-torsion over \mathbb{Q}^{ab} , contradicting Theorem 2.4. Thus, if $E(\mathbb{Q}^{\text{ab}})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} = E(\mathbb{Q}^{\text{ab}})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. If E does not have full 5-torsion over \mathbb{Q}^{ab} , then $E(\mathbb{Q}^{\text{ab}})[5^\infty] \cong \mathbb{Z}/25\mathbb{Z}$ in order for $C_5(E) = 3$. Then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/25\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.

Suppose $C_5(E) = 2$ and $C_3(E) \leq 2$ and $C_2(E) = 1$. Then $E(\mathbb{Q}^{\text{ab}})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z}$ and $E(\mathbb{Q}^{\text{ab}})[3^\infty] \subseteq \mathbb{Z}/3\mathbb{Z}$ by Lemma 2.3. Again by Lemma 3.6 we have $E(\mathbb{Q}^{\text{ab}})[2^\infty] \cong \{0\}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus, $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$.

Suppose $C_5(E) = 2$ and $C_3(E) = 1$ and $C_2(E) \leq 2$. Then again $E(\mathbb{Q}^{\text{ab}})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z}$. By Table 1, the largest $E(\mathbb{Q}^{\text{ab}})[2^\infty]$ can be so that $C_2(E) = 2$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Further, E does not have full torsion of any order prime to 2 by Corollary 2.5. Thus, $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$. \square

Proposition 4.6. *Let E/\mathbb{Q} be an elliptic curve. Suppose E has a 7-isogeny. Then either $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \mathbb{Z}/21\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$.*

Proof. By Theorem 2.2 we have $C_p(E) = 1$ for all primes $p \neq 2, 3, 7$ and either $C_3(E) \leq 2$ and $C_2(E) = 1$, or $C_3(E) = 1$ and $C_2(E) \leq 2$.

Suppose $C_3(E) = 2$ and $C_2(E) = 1$. Then E has a 7-isogeny and a 3-isogeny and so E has a 21-isogeny. Since there are only finitely many rational points on $X_0(21)$, there are only a finite number of j -invariants for elliptic curves over \mathbb{Q} with a 21-isogeny. We can fix a model for each of these curves and explicitly check that none of these families have full m -torsion for any $2 \leq m \leq 8$. Thus, by Lemma 2.3, Lemma 2.7, and Theorem 2.4 we have $E(\mathbb{Q}^{\text{ab}}) \cong \mathbb{Z}/21\mathbb{Z}$.

Suppose instead that $C_3(E) = 1$ and $C_2(E) = 2$. Since $C_3(E) = 1$, Corollary 2.5 tells us that E does not have full 3-torsion. Further, since $C_2(E) = 2$, by Proposition 3.5, it follows that $E(\mathbb{Q}^{\text{ab}})[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Therefore, by Lemma 2.7 we have that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$.

Finally if $C_3(E) = C_2(E) = 1$, then by Lemma 2.7, Corollary 2.5, and Lemma 3.6 we have that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$. \square

Proposition 4.7. *Let E/\mathbb{Q} be an elliptic curve, let $p = 11, 17, 19, 37, 43, 67$, or 163 , and suppose that E has a p -isogeny. Then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. By Lemma 2.3 we have that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \supseteq \mathbb{Z}/p\mathbb{Z}$. For these values of p , note that there are no rational isogenies of degree divisible by p besides isogenies of degree exactly p , and therefore, by Lemma 2.7 it follows that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \subseteq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for some m with $(m, p) = 1$. However, from Theorem 2.2 it follows that E has no other rational isogenies. Thus, Corollary 2.5 implies that m is a power of 2. Combining that with Lemma 3.6 shows that $m = 1$ or 2 .

For any given p in this list there are only finitely many j -invariants of elliptic curves having a p -isogeny, as $X_0(p)$ has genus greater than 0. Given that these j -invariants are not 0 or 1728, by Lemma 3.1 it suffices to fix a representative E_j and compute (via Magma) that E_j does not have full 2-torsion defined over \mathbb{Q}^{ab} . \square

Proposition 4.8. *Let E/\mathbb{Q} be an elliptic curve. Suppose E has a 13-isogeny. Then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/13\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$.*

Proof. Since there are no curves over \mathbb{Q} with rational isogenies of degree properly divisible by 13, it follows from Lemma 2.7 that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ for some $m \geq 1$. However, by Theorem 2.2 we have that $C_p(E) = 1$ for all primes $p \neq 13$. Thus, by Corollary 2.5 and Lemma 3.6 we have that $m = 1$ or 2 . \square

Note that from here a quick count of the possible sizes of the torsion subgroups along with Lemma 2.3 for the example of 26569a1 having a point of order 163 over \mathbb{Q}^{ab} is already enough to prove Corollary 1.3.

5. Eliminating possible torsion

We restate the classification theorem for convenience.

Theorem 5.1. *Let E/\mathbb{Q} be an elliptic curve. Then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ is isomorphic to one of the following groups:*

$$\begin{aligned} \mathbb{Z}/N_1\mathbb{Z}, & \quad N_1 = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 37, 43, 67, 163, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, & \quad N_2 = 1, 2, \dots, 9, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3N_3\mathbb{Z}, & \quad N_3 = 1, 3, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4N_4\mathbb{Z}, & \quad N_4 = 1, 2, 3, 4, \\ \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, & \\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}. & \end{aligned}$$

Each of these groups appear as $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ for some elliptic curve over \mathbb{Q} .

We now eliminate the possibility of many of the groups appearing in the previous propositions as possible torsion subgroups over \mathbb{Q}^{ab} for some elliptic curve E/\mathbb{Q} . We begin with a simple observation about 2-torsion over \mathbb{Q}^{ab} from Proposition 3.5.

Lemma 5.2. *Let E/\mathbb{Q} be an elliptic curve. If $E(\mathbb{Q}^{\text{ab}})[2] \neq \{0\}$ then $E(\mathbb{Q}^{\text{ab}})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus, $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \not\cong \mathbb{Z}/2N\mathbb{Z}$ for any $N \geq 1$.*

This eliminates many possible torsion structures over \mathbb{Q}^{ab} . In particular, after we combine the possibilities for $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ from Propositions 4.8, 4.6, 4.5, 4.4, 4.3, and 4.7, and eliminate those groups ruled out by Lemma 5.2, we can compare them to the classification in Theorem 1.2 to see that it remains to rule out the following groups as possibilities for $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$:

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, & \quad N_2 = 10, 12, 13, 14, 15, 18, 25, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}. & \end{aligned}$$

Proposition 5.3. *Let E/\mathbb{Q} be an elliptic curve. Then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$.*

Proof. In the case $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$ the curve has a 14-isogeny by Lemma 2.7 of which there are only two possible isomorphism classes of curves given by the j -invariants -3^35^3 and $3^35^317^3$ (see for instance [Lozano-Robledo 2013, Table 4]). Using division polynomials we can check that in both cases there are no points of order 4 defined over an abelian extension of \mathbb{Q} .

In the case $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ the curve has a 15-isogeny by Lemma 2.7. Here there are four possible j -invariants, $-5^2/2$, $-5^2 \cdot 241^3/2^3$, $-5 \cdot 29^3/2^5$, and $5 \cdot 211^3/2^{15}$. Again using division polynomials we can check that none of these curves have a point of order 2 defined over an abelian extension of \mathbb{Q} . \square

Proposition 5.4. *Let E/\mathbb{Q} be an elliptic curve. Then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$.*

Proof. Suppose that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$. Then E has a 13-isogeny, and so by [Lozano-Robledo 2013, Table 3] the curve has a j -invariant of the form

$$j(E) = \frac{(h^2 + 5h + 13)(h^4 + 7h^3 + 20h^2 + 19h + 1)^3}{h}$$

for some $h \in \mathbb{Q}$ with $h \neq 0$. Thus, E must be a twist of the curve

$$E' : y^2 + xy = x^3 - \frac{36}{j(E) - 1728}x - \frac{1}{j(E) - 1728}.$$

Since $E(\mathbb{Q}^{\text{ab}})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ but E does not have any 2-isogenies by Theorem 2.2, we must have $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ by Theorem 2.4, implying that the discriminant of E is a square. Since E is a twist of E' , the discriminant of E differs from the discriminant of E' by at most a square. Thus, we obtain a formula $y^2 = \text{Disc}(E')$, which we compute in terms of h . By absorbing squares into the y^2 term we obtain a curve

$$C : Y^2 = h(h^2 + 6h + 13)$$

which is a modular curve describing precisely when E has a 13-isogeny and $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. This curve is actually an elliptic curve with $C(\mathbb{Q}) = \{(0 : 0 : 1), (0 : 1 : 0)\} \cong \mathbb{Z}/2\mathbb{Z}$, both points being cusps. Therefore, there are no elliptic curves with $E(\mathbb{Q}^{\text{ab}}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$. \square

Proposition 5.5. *Let E/\mathbb{Q} be an elliptic curve; then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.*

Proof. Suppose that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$. Then E has a 25-isogeny, and so by [Lozano-Robledo 2013, Table 3] the curve has a j -invariant of the form

$$j(E) = \frac{(h^{10} + 10h^8 + 35h^6 - 12h^5 + 50h^4 - 60h^3 + 25h^2 - 60h + 16)^3}{(h - 1)(h^4 + h^3 + 6h^2 + 6h + 11)}$$

for some $h \in \mathbb{Q}$ with $h \neq 1$. By a similar argument made in Proposition 5.4 we have that the discriminant of E must be a square. We again obtain a formula $y^2 = \text{Disc}(E)$, and by absorbing squares into the y^2 term we obtain a curve

$$C : Y^2 = h^7 + 9h^5 + 25h^3 - 11h^2 + 20h - 44$$

which is a modular curve describing precisely when E has a 25-isogeny and $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. This is a genus-3 hyperelliptic curve. We write the curve in projective coordinates using $h = \frac{X}{Z}$.

We can construct a map π from C to an elliptic curve $\tilde{C} : y^2 = x^3 + x^2 - x$ given by

$$(*) \quad (X : Y : Z) \mapsto (x^3 - x^2z + 4xz^2 - 4z^3 : yz^2 : x^2z - 2xz^2 + z^3).$$

The curve \tilde{C} has Cremona label 20a2 and rank 0 with torsion isomorphic to $\mathbb{Z}/6\mathbb{Z}$. It has rational points

$$\tilde{C}(\mathbb{Q}) = \{(0 : 1 : 0), (0 : 0 : 1), (-1 : -1 : 1), (1 : -1 : 1), (-1 : 1 : 1), (1 : 1 : 1)\}$$

and we can use (*) to explicitly compute the preimage of each point under π to see that the only rational points on C are $(1 : 0 : 1)$ and $(0 : 1 : 0)$. Note that $h = \frac{X}{Z}$ for points $(X : Y : Z) \in C$. The first point corresponds to $h = 1$, which is a zero of the denominator of $j(E)$, and the second point is the point at infinity, which corresponds to $h = \infty$, which is not a value we can consider. Thus, both of these points are cusps, and therefore, there are no elliptic curves with $E(\mathbb{Q}^{\text{ab}}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$. \square

Proposition 5.6. *Let E/\mathbb{Q} be an elliptic curve; then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.*

Proof. Suppose for the sake of contradiction that E is an elliptic curve over \mathbb{Q} such that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$. Then, E has a \mathbb{Q} -rational 10-isogeny, and so by [Lozano-Robledo 2013, Table 3] the curve has a

$$j(E) = \frac{(h^6 - 4h^5 + 16h + 16)^3}{(h + 1)^2(h - 4)h^5}$$

for some $h \in \mathbb{Q}$ with $h \neq -1, 0, 4$. Thus, E must be a twist of the curve

$$E' : y^2 + xy = x^3 - \frac{36}{j(E) - 1728}x - \frac{1}{j(E) - 1728}.$$

Moving the 2-torsion point to $(0,0)$ yields a model of E' of the form

$$E' : y^2 = x^3 + b(h)x^2 + d(h)x$$

for the rational functions

$$\begin{aligned} b(h) &= \frac{-9h^{12} + 72h^9 - 144h^3 - 144}{h^{12} - 8h^9 - 8h^3 - 8}, \\ d(h) &= (1296h^{27} - 19440h^{24} + 62208h^{21} + 124416h^{18} - 248832h^{15} \\ &\quad - 622080h^{12} + 995328h^6 + 995328h^3 + 331776) \\ &\quad / (h^{36} - 24h^{33} + 192h^{30} - 464h^{27} - 720h^{24} + 2304h^{21} + 2112h^{18} \\ &\quad + 5760h^{15} + 14400h^{12} + 11776h^9 + 12288h^6 + 12288h^3 + 4096). \end{aligned}$$

Note that $j(E) \neq 0, 1728$ since E has a 10-isogeny, and thus, E is a quadratic twist of E' . By Lemma 3.1 we have that $E'(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$. Now, since $E'(\mathbb{Q}^{\text{ab}})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, Lemma 3.4 tells us that either $C_2(E) \geq 4$ or

$$d(h) \in (\mathbb{Q}^\times)^2 \quad \text{or} \quad (b(h)^2 - 4d(h))d(h) \in (\mathbb{Q}^\times)^2.$$

Note that since $C_5(E) \geq 2$, by Theorem 2.2 it is impossible for $C_2(E) \geq 4$. Denote the 4-torsion point over \mathbb{Q}^{ab} by Q .

Suppose $d(h) \in (\mathbb{Q}^\times)^2$. We obtain a formula $Y^2 = d(h)$, and by absorbing squares we obtain the curve

$$C : Y'^2 = h^3 + h^2 + 4h + 4$$

which is a modular curve describing precisely when E has a 10-isogeny and $\text{Gal}(\mathbb{Q}(x(Q))/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This is the elliptic curve with Cremona label 20a1 and rational points

$$C(\mathbb{Q}) = \{(0:1:0), (0:-2:1), (0:2:1), (4:-10:1), (4:10:1), (-1:0:1)\} \cong \mathbb{Z}/6\mathbb{Z}.$$

However, all of these points are cusps as they correspond to $h = 0, -1, 4$, which are all zeros of the denominator of $j(E)$. Therefore, there are no such elliptic curves.

Suppose instead that $(b(h)^2 - 4d(h))d(h) \in (\mathbb{Q}^\times)^2$. Again we obtain a formula $Y^2 = (b(h)^2 - 4d(h))d(h)$, and by absorbing squares we obtain the curve

$$\widehat{C} : Y'^2 = h^3 - 3h^2 - 4h$$

which is a modular curve describing precisely when E has a 10-isogeny and $\text{Gal}(\mathbb{Q}(x(Q))/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. This is an elliptic curve with Cremona label 40a1 and rational points

$$\widehat{C}(\mathbb{Q}) = \{(0:0:1), (0:1:0), (-1:0:1), (4:0:1)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Again, all of these points are cusps as they correspond to $h = 0, -1, 4$. Therefore, there are no such elliptic curves. Thus, we can conclude that no such curve E exists. \square

Proposition 5.7. *Let E/\mathbb{Q} be an elliptic curve; then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$.*

Proof. Suppose for the sake of contradiction that E is an elliptic curve over \mathbb{Q} such that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$. Then, E has a \mathbb{Q} -rational 18-isogeny, and so by [Lozano-Robledo 2013, Table 3] the curve has a j -invariant of the form

$$j(E) = \frac{(h^3 - 2)^3(h^9 - 6h^6 - 12h^3 - 8)^3}{h^9(h^3 - 8)(h^3 + 1)^2}$$

for some $h \in \mathbb{Q}$ with $h \neq -1, 0, 2$. Thus, E must be a twist of the curve

$$E' : y^2 + xy = x^3 - \frac{36}{j(E) - 1728}x - \frac{1}{j(E) - 1728}.$$

Moving the 2-torsion point to $(0,0)$ yields a model of E' of the form

$$E' : y^2 = x(x^2 + b(h)x + d(h))$$

for the rational functions

$$b(h) = \frac{(h^3 - 2)(h^9 - 6h^6 - 12h^3 - 8)}{h^{12} - 8h^9 - 8h^3 - 8},$$

$$d(h) = \frac{(h + 1)(h^2 - h + 1)(h^3 - 2)^2(h^9 - 6h^6 - 12h^3 - 8)^2}{(h^6 - 4h^3 - 8)^2(h^{12} - 8h^9 - 8h^3 - 8)^2}.$$

Note that $j(E) \neq 0, 1728$ since E has an 18-isogeny, and thus, E is a quadratic twist of E' . By Lemma 3.1 we have that $E'(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$. Now, since $E'(\mathbb{Q}^{\text{ab}})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, Lemma 3.4 tells us that either $C_2(E) \geq 4$,

$$d(h) \in (\mathbb{Q}^\times)^2, \quad \text{or} \quad (b(h)^2 - 4d(h))d(h) \in (\mathbb{Q}^\times)^2.$$

Note that, since $C_3(E) \geq 3$, Theorem 2.2 implies that $C_2(E) < 4$. Denote the 4-torsion point over \mathbb{Q}^{ab} by Q .

Suppose $d(h) \in (\mathbb{Q}^\times)^2$. We obtain a formula $Y^2 = d(h)$, and by absorbing squares we obtain the curve

$$C : Y^2 = h^3 + 1$$

which is a modular curve describing precisely when E has an 18-isogeny and $\text{Gal}(\mathbb{Q}(x(Q))/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This is an elliptic curve with Cremona label 36a1 and rational points

$$C(\mathbb{Q}) = \{(0 : 1 : 0), (0 : 1 : 1), (0 : -1 : 1), (2 : 3 : 1), (2 : -3 : 1), (-1 : 0 : 1)\} \cong \mathbb{Z}/6\mathbb{Z}.$$

However, all of these points are cusps as they correspond to $h = -1, 0, 2$. Therefore, there are no such elliptic curves.

Suppose instead that $(b(h)^2 - 4d(h))d(h) \in (\mathbb{Q}^\times)^2$. Again we obtain a formula $Y^2 = (b(h)^2 - 4d(h))d(h)$, and by absorbing squares we obtain the curve

$$\widehat{C} : Y'^2 = h^7 - 7h^4 - 8h$$

which is a modular curve describing precisely when E has an 18-isogeny and $\text{Gal}(\mathbb{Q}(x(Q))/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. This is a genus-3 hyperelliptic curve with an automorphism φ defined by

$$(x : y : z) \mapsto (2x^4 - 10x^3z + 12x^2z^2 + 8xz^3 - 16z^4 : 36yz^3 : x^4 - 8x^3z + 24x^2z^2 - 32xz^3 + 16z^4)$$

and taking the quotient of \widehat{C} by φ gives a map π from \widehat{C} to an elliptic curve $\widehat{C}_\varphi : y^2 = x^3 - x^2 + x$ given by

$$(**) \quad (x : y : z) \mapsto (xz(x^2 - xz - 2z^2) : yz^3 : x^2(x + z)^2).$$

The curve \widehat{C}_φ has Cremona label 24a4 and has rational points

$$\widehat{C}_\varphi(\mathbb{Q}) = \{(0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1), (1 : -1 : 1)\}.$$

We can use (**) to explicitly compute the preimage of each point under π to compute the rational points on \widehat{C} . We find that $\widehat{C}(\mathbb{Q}) = \{(-1 : 0 : 1), (0 : 0 : 1), (2 : 0 : 1), (0 : 1 : 0)\}$. These points correspond to $h = 0, -1, 2$, which are zeros of the denominator of $j(E)$ and so are cusps. Thus, we can conclude that no such curve E exists. \square

Proposition 5.8. *Let E/\mathbb{Q} be an elliptic curve; then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \not\cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.*

Proof. Suppose that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. Since $E(\mathbb{Q}^{\text{ab}})[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, Corollary 2.5 gives that $C_3(E) \geq 3$. In particular, the comment after Corollary 2.5 shows that E has two independent 3-isogenies over \mathbb{Q} . Thus, Theorem 2.2 gives that $C_2(E) \leq 2$, and so $E(\mathbb{Q})[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z}$. By Lemma 4.2 we also have that $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, and thus, E has a single nontrivial point P of order 2 over \mathbb{Q} . Therefore, E corresponds to a point on the modular curve $X_0(3, 6)$. We can find the j -map for $X_0(3, 6)$ as follows. Start with the j -map for $X_0(18)$ via [Lozano-Robledo 2013, Table 3] and create an elliptic curve over the function field $\mathbb{Q}(h)$ as done in previous propositions. This curve has a 9-isogeny. We can factor this 9-isogeny as the composition of two 3-isogenies and, using Velu's formulas, compute a model and the j -invariant for the intermediate elliptic curve, which has two independent 3-isogenies. The point of order 2 is preserved under the 3-isogeny, and so this is the j -map from $X_0(3, 6)$. Note that Magma has the functionality to do these computations.

We arrive at the following: an elliptic curve with two independent 3-isogenies has j -invariant of the form

$$j(E) = \frac{(h^3 - 2)^3(h^3 + 6h - 2)^3(h^6 - 6h^4 - 4h^3 + 36h^2 + 12h + 4)^3}{(h - 2)^3h^3(h + 1)^6(h^2 - h + 1)^6(h^2 + 2h + 4)^3}$$

for some $h \in \mathbb{Q}$ with $h \neq 2, 0, -1$. Thus, E must be a twist of the curve

$$E' : y^2 + xy = x^3 - \frac{36}{j(E) - 1728}x - \frac{1}{j(E) - 1728}.$$

Moving the 2-torsion point to $(0,0)$ yields a model of E' of the form

$$E' : y^2 = x(x^2 + b(h)x + d(h))$$

for the rational functions

$$\begin{aligned} b(h) &= \frac{(h^3 - 2)(h^3 + 6h - 2)(h^6 - 6h^4 - 4h^3 + 36h^2 + 12h + 4)}{(h^4 - 2h^3 - 8h - 2)(h^8 + 2h^7 + 4h^6 - 16h^5 - 14h^4 + 8h^3 + 64h^2 - 16h + 4)}, \\ d(h) &= ((h + 1)^3(h^2 - h + 1)^3(h^3 - 2)^2(h^3 + 6h - 2)^2 \\ &\quad \times (h^6 - 6h^4 - 4h^3 + 36h^2 + 12h + 4)^2) \\ &\quad / ((h^2 + 2h - 2)^2(h^4 - 2h^3 - 8h - 2)^2(h^4 - 2h^3 + 6h^2 + 4h + 4)^2 \\ &\quad \times (h^8 + 2h^7 + 4h^6 - 16h^5 - 14h^4 + 8h^3 + 64h^2 - 16h + 4)^2). \end{aligned}$$

Note that $j(E) \neq 0, 1728$ since E is a quadratic twist of E' . By Lemma 3.1 we have that $E'(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. Now, since $E'(\mathbb{Q}^{\text{ab}})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, Lemma 3.4 tells us that

$$d(h) \in (\mathbb{Q}^\times)^2, \quad \text{or} \quad (b(h)^2 - 4d(h))d(h) \in (\mathbb{Q}^\times)^2.$$

Suppose $d(h) \in (\mathbb{Q}^\times)^2$. We obtain a formula $Y^2 = d(h)$, and by absorbing squares we obtain the curve

$$C : Y'^2 = h^3 + 1.$$

If instead $(b(h)^2 - 4d(h))d(h) \in (\mathbb{Q}^\times)^2$, then we obtain $Y^2 = (b(h)^2 - 4d(h))d(h)$ and by absorbing squares we obtain the curve

$$\widehat{C} : Y'^2 = h^7 - 7h^4 - 8h.$$

Notice that both of these are the exact same hyperelliptic curves that appeared in the proof of Proposition 5.7. We have already found all rational points on these two curves, and again they all correspond to cusps. Thus, we can conclude that there do not exist any E/\mathbb{Q} with $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. \square

Note that it should not be too surprising that the same modular curves appear in the proof of Proposition 5.7 and Proposition 5.8. Indeed, elliptic curves with these torsion subgroups are linked via a 3-isogeny. One may attempt an alternative proof of Proposition 5.8 by making this connection rigorous and explicit.

Proposition 5.9. *Let E/\mathbb{Q} be an elliptic curve; then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$.*

Proof. Suppose for the sake of contradiction that E is an elliptic curve over \mathbb{Q} such that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$. Since $E(\mathbb{Q}^{\text{ab}})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, Table 1 shows that E has 2-powered isogenies of degrees 1, 2, 4, 4 or 1, 2, 4, 4, 8, 8. However, Lemma 2.7 implies that E has a 12-isogeny as well. Thus, Theorem 2.2 gives that the 2-powered isogenies of E must be restricted to ones of degree 1, 2, 4, and 4. Hence, $E(\mathbb{Q})[2^\infty] \subseteq \mathbb{Z}/4\mathbb{Z}$, and E has a point of order 2 over \mathbb{Q} . Moving the point of order 2 to $(0, 0)$ we obtain a model for E of the form

$$E : y^2 = x(x^2 + bx + d).$$

A similar argument to that made in the proof of Lemma 3.4 shows that any point $Q \in E(\mathbb{Q}^{\text{ab}})$ of order 4 must lie over a \mathbb{Q} -rational point of order 2, otherwise $E[4] \subseteq E(\mathbb{Q}^{\text{ab}})$. The argument is as follows: let α and $\bar{\alpha}$ be the two roots of $x^2 + bx + d$. By Lemma 3.2, a point that halves $(0, 0) \in E[2]$ is defined over \mathbb{Q}^{ab} if and only if $-\alpha$ and $-\bar{\alpha}$ are squares in \mathbb{Q}^{ab} . Similarly, a point that halves $(\alpha, 0) \in E[2]$ is defined over \mathbb{Q}^{ab} if and only if α and $\alpha - \bar{\alpha}$ are squares in \mathbb{Q}^{ab} . However, if α is a square in \mathbb{Q}^{ab} , then since $\sqrt{-1} \in \mathbb{Q}^{\text{ab}}$, it follows that $-\alpha$ and $-\bar{\alpha}$ are also squares in \mathbb{Q}^{ab} . Thus, if a point of order 4 that halves $(\alpha, 0)$ exists in \mathbb{Q}^{ab} ,

then so does a point of order 4 that halves $(0, 0)$, implying that E has full 4-torsion over \mathbb{Q}^{ab} .

Now, E has a \mathbb{Q} -rational 12-isogeny, and so by [Lozano-Robledo 2013, Table 3] the curve has a j -invariant of the form

$$j(E) = \frac{(h^2 - 3)^3(h^6 - 9h^4 + 3h^2 - 3)^3}{h^4(h^2 - 9)(h^2 - 1)^3}$$

for some $h \in \mathbb{Q}$ with $h \neq 0, \pm 1, \pm 3$. Thus, E must be a twist of the curve

$$E' : y^2 + xy = x^3 - \frac{36}{j(E) - 1728}x - \frac{1}{j(E) - 1728}.$$

Moving the 2-torsion point to $(0,0)$ yields a model of E' of the form

$$E' : y^2 = x(x^2 + b(h)x + d(h))$$

for the rational functions

$$b(h) = \frac{(h^2 - 3)(h^6 - 9h^4 + 3h^2 - 3)}{h^8 - 12h^6 + 30h^4 - 36h^2 + 9},$$

$$d(h) = \frac{h^2(h^2 - 3)^2(h^6 - 9h^4 + 3h^2 - 3)^2}{(h^4 - 6h^2 - 3)^2(h^8 - 12h^6 + 30h^4 - 36h^2 + 9)^2}.$$

For ease of notation going forward, we will write $b = b(h)$ and $d = d(h)$, and it should be understood that many of the following variables are functions of h . Let α and $\bar{\alpha}$ be roots of $x^2 + bx + d$ (over $\mathbb{Q}[h]$) so that $E' : y^2 = x(x - \alpha)(x - \bar{\alpha})$.

From our argument above we may assume that any point Q of order 4 in $E'(\mathbb{Q}^{\text{ab}})$ satisfies $2Q = (0, 0)$. Then, from Lemma 3.2 we have (without loss of generality) that Q has x -coordinate

$$(\sqrt{0-0})(\sqrt{0-\alpha}) \pm (\sqrt{0-0})(\sqrt{0-\bar{\alpha}}) \pm (\sqrt{0-\alpha})(\sqrt{0-\bar{\alpha}}) + 0 = \pm \sqrt{\alpha\bar{\alpha}} = \pm \sqrt{d}.$$

Suppose that the x -coordinate of Q is \sqrt{d} . Since there is a point of order 8 in $E(\mathbb{Q}^{\text{ab}})$, there exists a point $R \in E(\mathbb{Q}^{\text{ab}})$ such that $2R = Q$. Denote

$$\alpha = \frac{-b + \sqrt{b^2 - 4d}}{2} \quad \text{and} \quad \bar{\alpha} = \frac{-b - \sqrt{b^2 - 4d}}{2}$$

so that we have

$$E' : y^2 = x(x - \alpha)(x - \bar{\alpha}).$$

Since E does not have full 2-torsion over \mathbb{Q} , neither does E' , and so in particular $\alpha \notin \mathbb{Q}$. For ease of notation we denote $\delta = \sqrt{d}$. We can apply Lemma 3.2 again to deduce that since such an R exists, we must have that δ , $\delta - \alpha$, and $\delta - \bar{\alpha}$ are all squares in \mathbb{Q}^{ab} . Notice that through some simplification we have that $(\delta - \alpha)(\delta - \bar{\alpha}) = (b + 2\delta)\delta$ and so it suffices to prove that δ , $(b + 2\delta)\delta$, and $\delta - \alpha$ are squares in \mathbb{Q}^{ab} .

For any $h \in \mathbb{Q}$ we have $\delta \in \mathbb{Q}$ and so clearly $\sqrt{\delta} \in \mathbb{Q}^{\text{ab}}$. Similarly, for all $h \in \mathbb{Q}$, we have that $(b + 2\delta)\delta \in \mathbb{Q}$, and so $\sqrt{(b + 2\delta)\delta} \in \mathbb{Q}^{\text{ab}}$.

To see when $\delta - \alpha$ is square in \mathbb{Q}^{ab} we will find the minimal polynomial of $\sqrt{\delta - \alpha}$ over \mathbb{Q} , and find when this defines an abelian extension of \mathbb{Q} . Notice that $\delta - \alpha = \frac{1}{2}(b + 2\delta - \sqrt{b^2 - 4d})$. Let

$$\xi = \sqrt{\delta - \alpha} = \sqrt{\frac{b + 2\delta - \sqrt{b^2 - 4d}}{2}}.$$

We claim that $[\mathbb{Q}(\xi) : \mathbb{Q}(\alpha)] = 2$, which we will justify at the end of the proof, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, so $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$. Moreover, we find that ξ satisfies the polynomial

$$f(X) = X^4 - (b + 2\delta)X^2 + (b + 2\delta)\delta,$$

and so this is a minimal polynomial of ξ over \mathbb{Q} .

Now, we apply Proposition 3.3 and see that f defines an abelian extension of \mathbb{Q} if and only if

$$(b + 2\delta)\delta \in (\mathbb{Q}^\times)^2$$

or

$$((b + 2\delta)^2 - 4(b + 2\delta)\delta)(b + 2\delta)\delta \in (\mathbb{Q}^\times)^2,$$

which by absorbing squares is equivalent to

$$(b - 2\delta)\delta \in (\mathbb{Q}^\times)^2.$$

These yield the curves

$$C_1 : y^2 = h^3 - 2h^2 - 3h \quad \text{and} \quad C_2 : y^2 = h^3 + 2h^2 - 3h,$$

respectively.

Now it remains to classify all rational points on C_1 and C_2 . These are curves with Cremona labels 48a1 and 24a1, respectively, and have rank 0 with rational points

$$C_1(\mathbb{Q}) = \{(0 : 0 : 1), (0 : 1 : 0), (3 : 0 : 1), (-1 : 0 : 1)\}$$

and

$$C_2(\mathbb{Q}) = \{(0 : 0 : 1), (0 : 1 : 0), (-1 : -2 : 1), (3 : -6 : 1), (1 : 0 : 1), \\ (3 : 6 : 1), (-1 : 2 : 1), (-3 : 0 : 1)\}.$$

Note that all of these points correspond to $h = 0, \pm 1, \pm 3$, which are zeros of the denominator of $j(E)$ and hence are cusps. Therefore, there are no curves over \mathbb{Q} with $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$.

To see that $[\mathbb{Q}(\xi) : \mathbb{Q}(\alpha)] = 2$, suppose otherwise, that $\delta - \alpha$ was a square in $\mathbb{Q}(\alpha)$. Then the norm of $\delta - \alpha$,

$$\text{Nm}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\delta - \alpha) = (b + 2\delta)\delta,$$

would be a square in \mathbb{Q} . This is precisely what we checked above, that this does not happen for any noncuspidal values of h . \square

The following theorem applies broadly to any elliptic curve over $\overline{\mathbb{Q}}$ with complex multiplication, but we will use it to show specifically that the torsion subgroup $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$ does not appear over \mathbb{Q}^{ab} .

Theorem 5.10 [Bourdon and Clark 2016, Theorem 2.7]. *Let \mathbb{O}_K denote the ring of integers of a quadratic imaginary number field K . Let E/\mathbb{C} be an \mathbb{O}_K -CM elliptic curve, and let $M \subset E(\mathbb{C})$ be a finite \mathbb{O}_K -submodule. Then:*

- (a) *We have $M = E[\text{ann } M]$; hence,*
- (b) *$M \cong \mathbb{O}_K/(\text{ann } M)$ and*
- (c) *$\#M = |\text{ann } M|$.*

This gives us an understanding of \mathbb{O}_K -submodules of $E(\mathbb{C})$ for an elliptic curve with CM by the maximal order. We use these results to prove the following proposition.

Proposition 5.11. *Let E/\mathbb{Q} be an elliptic curve; then $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \not\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$.*

Proof. Suppose that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$. Then by Lemma 2.7 the curve E has a 9-isogeny over \mathbb{Q} . By the discussion in the paragraph following Corollary 2.5, E has an independent 3-isogeny as well. Thus, we have the isogeny graph

$$E' \xleftarrow{3} E \xrightarrow{9} E''.$$

Taking the dual isogeny also of degree 3 from E' to E and composing it with 9-isogeny from E to E'' shows that E' has a 27-isogeny. Note that this degree-27 isogeny is cyclic as the 9-isogeny and 3-isogeny are independent, i.e., their kernels have trivial intersection. The modular curve $X_0(27)$ has genus 1, and there is a unique 27-isogeny class of elliptic curves up to isomorphism. Examining the 27-isogeny class shows that E has CM by the maximal order of $K = \mathbb{Q}(\sqrt{-3})$.

Now, notice that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ is an \mathbb{O}_K -submodule of $E(\mathbb{C})$, since $K \subseteq \mathbb{Q}^{\text{ab}}$. Since the prime $p = 3$ ramifies in K , there is a unique prime ideal \mathfrak{p} of \mathbb{O}_K with $|\mathfrak{p}| = 3$ and we have $(3) = \mathfrak{p}^2$. By Theorem 5.10(b) we have that $E[27] \cong \mathbb{O}_K/(3)^3 \cong \mathbb{O}_K/\mathfrak{p}^6$. Suppose I is an ideal of $\mathbb{O}_K/\mathfrak{p}^6$. Then $\mathfrak{p}^6 \subseteq I$ so $I \mid \mathfrak{p}^6$ and therefore $I = \mathfrak{p}^b$ for some $0 \leq b \leq 6$ by the unique factorization of ideals into prime ideals. Thus, the \mathbb{O}_K -submodules of $E[27]$ are all of the form $\mathfrak{p}^b/\mathfrak{p}^6$ for some $0 \leq b \leq 6$. Moreover, the exponent of $\mathbb{O}_K/\mathfrak{p}^b$ is the smallest power of 3 contained in \mathfrak{p}^b . Since $(3)^d = \mathfrak{p}^{2d}$,

this smallest power is $3^{\lceil b/2 \rceil}$. Further, by Theorem 5.10(c) we have $\#\mathbb{O}_K/\mathfrak{p}^b = 3^b$, and we deduce that

$$\mathbb{O}_K/\mathfrak{p}^b \cong_{\mathbb{Z}} \mathbb{Z}/3^{\lfloor b/2 \rfloor} \mathbb{Z} \times \mathbb{Z}/3^{\lceil b/2 \rceil} \mathbb{Z}.$$

Notice that since $E(\mathbb{Q}^{\text{ab}})[27]$ is an \mathbb{O}_K -submodule of $E[27]$, we have that $\lfloor \frac{b}{2} \rfloor = 1$, implying $b = 2$ or $b = 3$, but also $\lceil \frac{b}{2} \rceil = 3$, implying $b = 5$ or $b = 6$, a contradiction. Thus, no such curve exists. \square

6. Algorithm

We can combine our results to form an explicit algorithm to compute $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ for any elliptic curve E/\mathbb{Q} . Note that this algorithm only relies on the information about subgroups excluded from appearing as $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ by Sections 4 and 5. See <https://sites.tufts.edu/michaelchou/research/> for the Magma code that implements this algorithm.

The algorithm uses Lemma 2.3 and Lemma 2.6 repeatedly, as well as Table 1. Moreover, the algorithm works for any elliptic curve E/\mathbb{Q} because we exhaustively deal with all isogeny graphs possible by Theorem 2.2. We denote $T := E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$.

- Compute the isogeny graph of E . Let I denote the degrees of the isogenies E has. Let N denote the largest value in I . Let I_2 and T_2 denote the 2-primary part of I and T , respectively.
- Lemmas 2.3 and 2.6 show that:
 - If $N = 11, 13, 15, 17, 19, 21, 25, 27, 37, 43, 67$, or 163 , then $T \cong \mathbb{Z}/N\mathbb{Z}$.
 - If $N = 10, 14, 16$, or 18 , then $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.
 - If $I = [1, 5, 5]$, then $T \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.
 - If $I = [1, 3, 3, 9]$, then $T \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$.
 - If $I = [1, 3, 3]$, then $T \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Note that we cannot have $T \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ because Lemma 4.2 would imply a 2-isogeny.
 - If $I = [1, 2, 3, 3, 6, 6]$, then $T \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
- Table 1 shows that:
 - If $I = [1, 2, 2, 2, 4, 4, 4, 4]$, then $T \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.
 - If $I = [1, 2, 2, 2, 4, 4, 8, 8]$, then $T \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$.
 - If $I = [1, 2, 4, 4, 8, 8, 8, 8]$ or $[1, 2, 2, 2, 4, 4]$, then $T \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.
 - If $I = [1, 2, 4, 4, 8, 8, 16, 16]$, then $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$.
 - If $I = [1, 2, 4, 4, 8, 8]$, then $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.
 - If $I = [1, 2, 2, 2, 3, 6, 6, 6]$, then $T_2 \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $3 \in I$ shows that $T \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.
 - If $I = [1, 2, 2, 2]$, then $T_2 \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

- The remaining cases require extra steps beyond simply computing I , as I does not uniquely determine T .
 - If $N = 1, 3, 5, 7$, or 9 , then compute $E[2]$ to check whether $\mathbb{Q}(E[2])$ is abelian or not. If not, then $T \cong \mathbb{Z}/N\mathbb{Z}$. If so, then $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$.
 - If $I_2 = [1, 2, 4, 4]$, then compute $E[8]$ and $E[4]$ to determine whether E has a point of order 8 over \mathbb{Q}^{ab} and whether $\mathbb{Q}(E[4])$ is abelian. This distinguishes between the following three cases:
 - * $T_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. If $3 \in I$, then $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. If $3 \notin I$, then $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
 - * $T_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. This implies $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.
 - * $T_2 \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. If $3 \in I$, then $T \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. If $3 \notin I$, then $T \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
 - If $I_2 = [1, 2]$, then we compute $E[4]$ to determine whether E has a point of order 4 defined over \mathbb{Q}^{ab} . This distinguishes between the following two cases:
 - * $T_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $3 \in I$, then $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. If $5 \in I$, then $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. If $I = I_2 = 1, 2$ then $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
 - * $T_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. If $3 \in I$, then $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. If $3 \notin I$, then $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

7. Examples

We first examine all examples of curves with an n -isogeny where $X_0(n)$ has finitely many noncuspidal points over \mathbb{Q} in Table 2. We refer to Table 4 of [Lozano-Robledo 2013] for the j -invariants. We give the torsion subgroup over \mathbb{Q}^{ab} , the j -invariant, the Cremona labels of the elliptic curves, and the Galois group of the field of definition of the abelian torsion. We then find examples for all the other torsion subgroups appearing in Theorem 1.2 in Table 3, computing the torsion subgroup over \mathbb{Q}^{ab} using the method described in Section 6.

Acknowledgements

This work was inspired by [González-Jiménez and Lozano-Robledo 2016], and the author would like to thank Álvaro Lozano-Robledo for his invaluable guidance and input. The author would like to thank Jeremy Rouse and David Zureick-Brown for their helpful advice concerning modular curves. The author would also like to thank Pete Clark and Drew Sutherland for their interest and support for this project. Also, thanks to Harris Daniels and Filip Najman for their comments and suggestions. Finally, the author would like to thank the anonymous referees for their helpful comments.

$E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$	$j(E)$	Cremona label	$\text{Gal}(\mathbb{Q}(E(\mathbb{Q}^{\text{ab}})_{\text{tors}})/\mathbb{Q})$
$\mathbb{Z}/11\mathbb{Z}$	$-11 \cdot 131^3$	121a1	$\mathbb{Z}/10\mathbb{Z}$
		121c2	$\mathbb{Z}/5\mathbb{Z}$
	-2^{15}	121b1	$\mathbb{Z}/5\mathbb{Z}$
		121b2	$\mathbb{Z}/10\mathbb{Z}$
	-11^2	121c1	$\mathbb{Z}/10\mathbb{Z}$
		121a2	$\mathbb{Z}/5\mathbb{Z}$
$\mathbb{Z}/15\mathbb{Z}$	$-5^2/2$	50a1	$\mathbb{Z}/4\mathbb{Z}$
		50b3	$\mathbb{Z}/4\mathbb{Z}$
	$-5^2 \cdot 241^3/2^3$	50a2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
		50b4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
	$-5 \cdot 29^3/2^5$	50a3	$\mathbb{Z}/2\mathbb{Z}$
		50b1	$\mathbb{Z}/2\mathbb{Z}$
	$5 \cdot 211^3/2^{15}$	50a4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
		50b2	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/17\mathbb{Z}$	$-17^2 \cdot 101^3/2$	14450p1	$\mathbb{Z}/16\mathbb{Z}$
	$-17 \cdot 373^3/2^{17}$	14450p2	$\mathbb{Z}/8\mathbb{Z}$
$\mathbb{Z}/19\mathbb{Z}$	$-2^{15} \cdot 3^3$	361a1	$\mathbb{Z}/9\mathbb{Z}$
		361a2	$\mathbb{Z}/18\mathbb{Z}$
$\mathbb{Z}/21\mathbb{Z}$	$-3^2 \cdot 5^6/2^3$	162b1	$\mathbb{Z}/3\mathbb{Z}$
		162c2	$\mathbb{Z}/6\mathbb{Z}$
	$3^3 \cdot 5^3/2$	162b2	$\mathbb{Z}/6\mathbb{Z}$
		162c1	$\mathbb{Z}/6\mathbb{Z}$
	$-3^2 \cdot 5^3 \cdot 101^3/2^{21}$	162b3	$\mathbb{Z}/6\mathbb{Z}$
		162c4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
	$-3^3 \cdot 5^3 \cdot 383^3/2^7$	162b4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
		162c3	$\mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z}/27\mathbb{Z}$	$-2^{15} \cdot 3 \cdot 5^3$	27a2	$\mathbb{Z}/18\mathbb{Z}$
		27a4	$\mathbb{Z}/9\mathbb{Z}$
$\mathbb{Z}/37\mathbb{Z}$	$-7 \cdot 11^3$	1225h1	$\mathbb{Z}/12\mathbb{Z}$
	$-7 \cdot 137^3 \cdot 2083^3$	1225h2	$\mathbb{Z}/36\mathbb{Z}$
$\mathbb{Z}/43\mathbb{Z}$	$-2^{18} \cdot 3^3 \cdot 5^3$	1849a1	$\mathbb{Z}/21\mathbb{Z}$
		1849a2	$\mathbb{Z}/42\mathbb{Z}$
$\mathbb{Z}/67\mathbb{Z}$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	4489a1	$\mathbb{Z}/33\mathbb{Z}$
		4489a2	$\mathbb{Z}/66\mathbb{Z}$
$\mathbb{Z}/163\mathbb{Z}$	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	26569a1	$\mathbb{Z}/81\mathbb{Z}$
		26569a2	$\mathbb{Z}/162\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$	$-3^3 \cdot 5^3$	49a1	$\mathbb{Z}/6\mathbb{Z}$
		49a3	$\mathbb{Z}/6\mathbb{Z}$
	$-3^3 \cdot 5^3 \cdot 17^3$	49a2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
		49a4	$\mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$	0	27a1	$\mathbb{Z}/6\mathbb{Z}$
		27a3	$\mathbb{Z}/6\mathbb{Z}$

Table 2. Torsion from n -isogenies with $X_0(n)$ genus > 0 .

$E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$	$j(E)$	Cremona label	$\text{Gal}(\mathbb{Q}(E(\mathbb{Q}^{\text{ab}})_{\text{tors}})/\mathbb{Q})$
$\{\mathcal{O}\}$	$2^{12} \cdot 3^3/37$	37a1	$\{1\}$
$\mathbb{Z}/3\mathbb{Z}$	$2^{13}/11$	44a1	$\{1\}$
$\mathbb{Z}/5\mathbb{Z}$	$-1/2^5 \cdot 19$	38b1	$\{1\}$
$\mathbb{Z}/7\mathbb{Z}$	$3^3 \cdot 4^3/2^7 \cdot 13$	26b1	$\{1\}$
$\mathbb{Z}/9\mathbb{Z}$	$-3 \cdot 73^3/2^9$	54b3	$\{1\}$
$\mathbb{Z}/13\mathbb{Z}$	$-2^{12} \cdot 7/3$	147b1	$\mathbb{Z}/3\mathbb{Z}$
$\mathbb{Z}/25\mathbb{Z}$	$-2^{12}/11$	11a3	$\mathbb{Z}/5\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$-5^6/3^2 \cdot 23$	69a1	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$11^6/3 \cdot 5 \cdot 7$	315b1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$2^8 \cdot 7$	196a1	$\mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$12721^3/3 \cdot 5 \cdot 7 \cdot 11^2$	3465e1	$(\mathbb{Z}/2\mathbb{Z})^3$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$	$2161^3/2^{10} \cdot 3^5 \cdot 11$	66c1	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	$71^3/2^4 \cdot 3^3 \cdot 5$	30a1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$	$103681^3/3^4 \cdot 5$	15a5	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$	$-5^3 \cdot 1637^3/2^{18} \cdot 7$	14a3	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$-2^{18} \cdot 7^3/19^3$	19a1	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$19^6/3^2 \cdot 5^2 \cdot 7^2$	315b2	$(\mathbb{Z}/2\mathbb{Z})^4$
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$37^3 \cdot 109^3/2^4 \cdot 3^4 \cdot 7^2$	126b2	$(\mathbb{Z}/2\mathbb{Z})^4$
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	$7^3 \cdot 127^3/2^2 \cdot 3^6 \cdot 5^2$	30a2	$(\mathbb{Z}/2\mathbb{Z})^4$
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$	$241^3/3^2 \cdot 5^2$	735e2	$(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$	$-2^{12} \cdot 31^3/11^5$	11a1	$\mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$5^3 \cdot 43^4/2^6 \cdot 7^3$	14a1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$13^3 \cdot 17^3/3^4 \cdot 5^4$	735e4	$(\mathbb{Z}/2\mathbb{Z})^5$

Table 3. Examples of remaining torsion subgroups

References

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, “The Magma algebra system, I: The user language”, *J. Symbolic Comput.* **24**:3–4 (1997), 235–265. MR Zbl

[Bourdon and Clark 2016] A. Bourdon and P. L. Clark, “Torsion points and Galois representations on CM elliptic curves”, preprint, 2016. arXiv

[Chou 2016] M. Chou, “Torsion of rational elliptic curves over quartic Galois number fields”, *J. Number Theory* **160** (2016), 603–628. MR Zbl

[Conrad 2012] K. Conrad, “Galois groups of cubics and quartics (not in characteristic 2)”, preprint, 2012, Available at <http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf>.

[Daniels et al. 2018] H. B. Daniels, Á. Lozano-Robledo, F. Najman, and A. V. Sutherland, “Torsion subgroups of rational elliptic curves over the compositum of all cubic fields”, *Math. Comp.* **87**:309 (2018), 425–458. MR Zbl

[Derickx et al. ≥ 2019] M. Derickx, A. Etropolski, J. Morrow, M. van Hoeij, and D. Zureick-Brown, “Sporadic cubic torsion”, in preparation.

[Fujita 2005] Y. Fujita, “Torsion subgroups of elliptic curves in elementary abelian 2-extensions of \mathbb{Q} ”, *J. Number Theory* **114**:1 (2005), 124–134. MR Zbl

- [González-Jiménez and Lozano-Robledo 2016] E. González-Jiménez and Á. Lozano-Robledo, “Elliptic curves with abelian division fields”, *Math. Z.* **283**:3–4 (2016), 835–859. MR Zbl
- [González-Jiménez and Najman 2016] E. González-Jiménez and F. Najman, “Growth of torsion groups of elliptic curves upon base change”, preprint, 2016. arXiv
- [Kamienny 1992] S. Kamienny, “Torsion points on elliptic curves and q -coefficients of modular forms”, *Invent. Math.* **109**:2 (1992), 221–229. MR Zbl
- [Kenku 1982] M. A. Kenku, “On the number of \mathbb{Q} -isomorphism classes of elliptic curves in each \mathbb{Q} -isogeny class”, *J. Number Theory* **15**:2 (1982), 199–202. MR Zbl
- [Kenku and Momose 1988] M. A. Kenku and F. Momose, “Torsion points on elliptic curves defined over quadratic fields”, *Nagoya Math. J.* **109** (1988), 125–149. MR Zbl
- [Knapp 1992] A. W. Knap, *Elliptic curves*, Math. Notes **40**, Princeton University, 1992. MR Zbl
- [LMFDB 2013] The LMFDB Collaboration, “The L -functions and modular forms database”, 2013, Available at <http://www.lmfdb.org>.
- [Lozano-Robledo 2013] Á. Lozano-Robledo, “On the field of definition of p -torsion points on elliptic curves over the rationals”, *Math. Ann.* **357**:1 (2013), 279–305. MR Zbl
- [Mazur 1978] B. Mazur, “Rational isogenies of prime degree”, *Invent. Math.* **44**:2 (1978), 129–162. MR Zbl
- [Merel 1996] L. Merel, “Bornes pour la torsion des courbes elliptiques sur les corps de nombres”, *Invent. Math.* **124**:1–3 (1996), 437–449. MR Zbl
- [Najman 2016] F. Najman, “Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$ ”, *Math. Res. Lett.* **23**:1 (2016), 245–272. MR Zbl
- [Ribet 1981] K. Ribet, “Torsion points of abelian varieties in cyclotomic extensions”, *Enseign. Math.* **27**:1–2 (1981), 315–319.
- [Rouse and Zureick-Brown 2015] J. Rouse and D. Zureick-Brown, “Elliptic curves over \mathbb{Q} and 2-adic images of Galois”, *Res. Number Theory* **1** (2015), art. id. 12. MR Zbl

Received April 12, 2018. Revised January 4, 2019.

MICHAEL CHOU
 DEPARTMENT OF MATHEMATICS
 TUFTS UNIVERSITY
 MEDFORD, MA
 UNITED STATES
michael.chou@tufts.edu

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

EDITORS

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Matthias Aschenbrenner
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
matthias@math.ucla.edu

Daryl Cooper
Department of Mathematics
University of California
Santa Barbara, CA 93106-3080
cooper@math.ucsb.edu

Jiang-Hua Lu
Department of Mathematics
The University of Hong Kong
Pokfulam Rd., Hong Kong
jhlu@maths.hku.hk

Paul Balmer
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
balmer@math.ucla.edu

Wee Teck Gan
Mathematics Department
National University of Singapore
Singapore 119076
matgwt@nus.edu.sg

Sorin Popa
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
popa@math.ucla.edu

Paul Yang
Department of Mathematics
Princeton University
Princeton NJ 08544-1000
yang@math.princeton.edu

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Kefeng Liu
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
liu@math.ucla.edu

Jie Qing
Department of Mathematics
University of California
Santa Cruz, CA 95064
qing@cats.ucsc.edu

PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org

SUPPORTING INSTITUTIONS

ACADEMIA SINICA, TAIPEI
CALIFORNIA INST. OF TECHNOLOGY
INST. DE MATEMÁTICA PURA E APLICADA
KEIO UNIVERSITY
MATH. SCIENCES RESEARCH INSTITUTE
NEW MEXICO STATE UNIV.
OREGON STATE UNIV.

STANFORD UNIVERSITY
UNIV. OF BRITISH COLUMBIA
UNIV. OF CALIFORNIA, BERKELEY
UNIV. OF CALIFORNIA, DAVIS
UNIV. OF CALIFORNIA, LOS ANGELES
UNIV. OF CALIFORNIA, RIVERSIDE
UNIV. OF CALIFORNIA, SAN DIEGO
UNIV. OF CALIF., SANTA BARBARA

UNIV. OF CALIF., SANTA CRUZ
UNIV. OF MONTANA
UNIV. OF OREGON
UNIV. OF SOUTHERN CALIFORNIA
UNIV. OF UTAH
UNIV. OF WASHINGTON
WASHINGTON STATE UNIVERSITY

These supporting institutions contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its contents or policies.


See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2019 is US \$490/year for the electronic version, and \$665/year for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2019 Mathematical Sciences Publishers

PACIFIC JOURNAL OF MATHEMATICS

Volume 302 No. 2 October 2019

An A_∞ version of the Poincaré lemma	385
CAMILO ARIAS ABAD, ALEXANDER QUINTERO VÉLEZ and SEBASTIÁN VÉLEZ VÁSQUEZ	
Wonderful compactification of character varieties	413
INDRANIL BISWAS, SEAN LAWTON and DANIEL RAMRAS	
What do Frobenius's, Solomon's, and Iwasaki's theorems on divisibility in groups have in common?	437
ELENA K. BRUSYANSKAYA, ANTON A. KLYACHKO and ANDREY V. VASIL'EV	
On homogeneous and inhomogeneous Diophantine approximation over the fields of formal power series	453
YANN BUGEAUD and ZHENLIANG ZHANG	
Torsion of rational elliptic curves over the maximal abelian extension of \mathbb{Q}	481
MICHAEL CHOU	
Local estimates for Hörmander's operators of first kind with analytic Gevrey coefficients and application to the regularity of their Gevrey vectors	511
MAKHLOUF DERRIDJ	
Boundedness of singular integrals with flag kernels on weighted flag Hardy spaces	545
YONGSHENG HAN, CHIN-CHENG LIN and XINFENG WU	
Exceptional sequences and spherical modules for the Auslander algebra of $k[x]/(x^t)$	599
LUTZ HILLE and DAVID PLOOG	
The topological biquandle of a link	627
EVA HORVAT	
An endpoint estimate of the Kunze–Stein phenomenon on $SU(n, m)$	645
TAKESHI KAWAZOE	
Mabuchi metrics and properness of the modified Ding functional	659
YAN LI and BIN ZHOU	
A generalization of Maloo's theorem on freeness of derivation modules	693
CLETO B. MIRANDA-NETO and THYAGO S. SOUZA	
τ -tilting finite gentle algebras are representation-finite	709
PIERRE-GUY PLAMONDON	
Yamabe equation on some complete noncompact manifolds	717
GUODONG WEI	
Weighted infinitesimal unitary bialgebras on rooted forests and weighted cocycles	741
YI ZHANG, DAN CHEN, XING GAO and YAN-FENG LUO	



0030-8730(201910)302:2;1-K