ON THE TORSION OF RATIONAL ELLIPTIC CURVES OVER SEXTIC FIELDS

HARRIS B. DANIELS AND ENRIQUE GONZÁLEZ-JIMÉNEZ

ABSTRACT. Given an elliptic curve $E/\mathbb{Q}$ with torsion subgroup $G = E(\mathbb{Q})_{\mathrm{tors}}$ we study what groups (up to isomorphism) can occur as the torsion subgroup of E base-extended to K, a degree 6 extension of $\mathbb{Q}$. We also determine which groups $H = E(K)_{\mathrm{tors}}$ can occur infinitely often and which ones occur for only finitely many curves. This article is a first step towards a complete classification of torsion growth over sextic fields.

1. INTRODUCTION

A fundamental theorem in the field of arithmetic geometry states that given a number field K and an elliptic curve E defined over K, the set of K-rational points on E, denoted $E(K)$, can be given the structure of a finitely generated abelian group. Further, it is well known that the torsion subgroup of this group $E(K)_{\mathrm{tors}}$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$ for some positive integers m and n. For the sake of brevity we will write $\mathbb{Z}/n\mathbb{Z} = (n)$ and $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z} = (m, mn)$ and call (m, mn) the torsion structure of E over K. By abuse of notation, we write $E(K)_{\mathrm{tors}} = (m, mn)$.

One of the main questions in the theory of elliptic curves is the following.

Question. Given a positive integer d what groups (up to isomorphism) arise as the torsion subgroup of an elliptic curve defined over a number field of degree d over $\mathbb{Q}$?

Beginning with Mazur's classification of torsion structures over $\mathbb{Q}$ in [31], mathematicians have spent considerable time and effort answering different facets of this question. Mazur's result asserts that the possible torsion structures over $\mathbb{Q}$ belong to the set

$$\Phi(1) = \{(n) \ : \ n = 1, \ldots, 10, 12\} \cup \{(2, 2m) \ : \ m = 1, \ldots, 4\}.$$

Over quadratic fields, the classification of torsion structures was completely settled in a series of papers by Kamienny [22] and Kenku and Momose [27]. Currently there is no complete classification for the case over cubic extension in the literature, but there are many significant results towards such a classification. In order to describe what is known we define the following notation:

- Let $\Phi(d)$ be the set of groups up to isomorphism that occur as the torsion structure of an elliptic curve defined over a number field of degree d.

- Let $\Phi^\infty(d) \subseteq \Phi(d)$ be the set of groups that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves defined over number fields of degree d.

For degree $d = 1, 2$, each group in $\Phi(d)$ occurs for infinitely many elliptic curves and so $\Phi^\infty(d) = \Phi(d)$. While determining the set $\Phi(d)$ is still open for $d \geq 3$, the uniform boundedness of torsion on elliptic curves, proved by Merel [32], states that for any d, there exists a bound $B(d)$ depending only on d such that $|G| \leq B(d)$ for all $G \in \Phi(d)$. Thus, the set $\Phi(d)$ is finite for any d. While $\Phi(d)$ is not completely known, $\Phi^\infty(d)$ is known for $d = 3, 4$ thanks to the work of Jeon et al. [20, 21] and $d = 5, 6$ by Derickx and Sutherland [8]. In this article we make use of the case when $d = 6$:

$$\Phi^\infty(6) = \{(n) \,|\, n = 1, \ldots, 22, 24, 26, 27, 28, 30\} \,\cup\, \{(2, 2m) \,|\, m = 1, \ldots, 10\}$$
$$\cup\, \{(3, 3m) \,|\, m = 1, \ldots, 4\} \,\cup \{(4, 4), (4, 8), (6, 6)\}.$$

Unlike in the cases when $d = 1$ or 2 when $d = 3, 5$, or 6 we know that $\Phi^\infty(d) \subsetneq \Phi(d)$ and in the case when $d = 4$, it is not known if $\Phi(4)$ and $\Phi^\infty(4)$ coincide. To illustrate the case when $d = 3$, Najman showed in [34] that the elliptic curve with Cremona label `162b1` has a point of order 21 defined over the field $\mathbb{Q}(\zeta_9)^+ = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, where ζ_9 is a primitive 9th root of unity and therefore $(21) \in \Phi(3)$, but $(21) \notin \Phi^\infty(3)$. For degrees $d = 5, 6$, van Hoeij [18] gives examples of elliptic curves defined over a number field of degree d (not coming from elliptic curves over $\mathbb{Q}$) with torsion structure not belonging to $\Phi^\infty(d)$. With these examples in mind we give the following definition:

- Let $J(d) \subseteq \overline{\mathbb{Q}}$ be the finite set defined by the following property: $j \in J(d)$ if and only if there exist a number field K of degree d and an elliptic curve E/K with $j(E) = j$, such that $E(K)_{\text{tors}}$ is isomorphic to a group in $\Phi(d)$ that is not in $\Phi^\infty(d)$. We let $J_{\mathbb{Q}}(d) = J(d) \cap \mathbb{Q}$ be the subset of $J(d)$ where we restrict to the case of elliptic curves E defined over $\mathbb{Q}$.

Since $\Phi(d) = \Phi^\infty(d)$ when $d = 1$ or 2 we have that $J(1) = J(2) = \emptyset$ and Najman's example shows that $-140625/8 \in J_{\mathbb{Q}}(3)$.

The question at the center of this paper is how torsion subgroups of elliptic curves can grow when they are considered over larger fields of definition. In particular, we will consider how the torsion subgroup of elliptic curves defined over $\mathbb{Q}$ can change when we consider them over a sextic extension of $\mathbb{Q}$. The techniques in the paper are closely related to those found in [12] and following that paper we give the following definitions:

- Let $\Phi_{\mathbb{Q}}(d)$ be the subset of $\Phi(d)$ such that $H \in \Phi_{\mathbb{Q}}(d)$ if there is an elliptic curve $E/\mathbb{Q}$ and a number field K of degree d such that $E(K)_{\text{tors}} = H$. Similarly, the set $\Phi_{\mathbb{Q}}^\infty(d)$ is contained inside the set $\Phi^\infty(d)$.
- Let $\Phi_{\mathbb{Q}}^\star(d)$ be the intersection of the sets $\Phi_{\mathbb{Q}}(d)$ and $\Phi^\infty(d)$.
- For a fixed $G \in \Phi(1)$, let $\Phi_{\mathbb{Q}}(d, G)$ be the subset of $\Phi_{\mathbb{Q}}(d)$ such that E runs through all elliptic curves over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} = G$. Also, let $\Phi_{\mathbb{Q}}^\star(d, G) = \Phi_{\mathbb{Q}}(d, G) \cap \Phi^\infty(d)$.
- Let $R_{\mathbb{Q}}(d)$ be the set of all primes p such that there exists a number field K of degree d and an elliptic curve $E/\mathbb{Q}$ such that E has a point of order p defined over K.

In the case when $d = 2$, or 3, the sets $\Phi_{\mathbb{Q}}(d)$ have been completely described by Najman [34]:

$$\Phi_{\mathbb{Q}}(2) = \{(n) \mid n = 1, \ldots, 10, 12, 15, 16\} \cup \{(2, 2m) \mid m = 1, \ldots, 6\}$$
$$\cup \{(3, 3), (3, 6), (4, 4)\}$$

and

$$\Phi_{\mathbb{Q}}(3) = \{(n) \mid n = 1, \ldots, 10, 12, 13, 14, 18, 21\} \cup \{(2, 2m) \mid m = 1, 2, 3, 4, 7\}.$$

The sets $\Phi_{\mathbb{Q}}(4)$, $\Phi_{\mathbb{Q}}(5)$, and $\Phi_{\mathbb{Q}}(7)$ have been completely classified in [3, 13], [10], and [13], respectively. Moreover in [13] it has been[1] established that $\Phi_{\mathbb{Q}}(d) = \Phi(1)$ for any positive integer d whose prime divisors are greater than 7.

For any $G \in \Phi(1)$ the set $\Phi_{\mathbb{Q}}(d, G)$ has been determined for $d = 2$ in [16], for $d = 3$ in [15], for $d = 4$ in [12], for $d = 5$ in [10], for $d = 7$ in [13], and for any d whose prime divisors are greater than 7 in [13].

Further, in [13] the second author and Najman determine all the possible degrees of $[\mathbb{Q}(P) : \mathbb{Q}]$, where P is a point of prime order p for a set of density $1535/1536$ of all primes and in particular for all $p < 3167$. In particular, we have that

$$R_{\mathbb{Q}}(6) = \{2, 3, 5, 7, 13\}.$$

Finally, we point out that obtaining the set $\Phi_{\mathbb{Q}}^{\star}(4)$ was a main tool to the determination of the whole classification of $\Phi_{\mathbb{Q}}(4)$. Thus, a first attempt to obtain $\Phi_{\mathbb{Q}}(6)$ is to obtain $\Phi_{\mathbb{Q}}^{*}(6)$ and that is our first main result.

Theorem 1. *The set $\Phi_{\mathbb{Q}}^{\star}(6)$ is given by*

$$\Phi_{\mathbb{Q}}^{\star}(6) = \{(n) \mid n = 1, \ldots, 21, \, n \neq 11, 17, 19, 20\} \cup \{(30)\}$$
$$\cup \{(2, 2n) \mid n = 1, \ldots, 7, 9\} \cup \{(3, 3n) \mid n = 1, \ldots, 4\} \cup \{(4, 4), (6, 6)\},$$

and $\Phi_{\mathbb{Q}}^{\infty}(6) = \Phi_{\mathbb{Q}}^{\star}(6) \setminus \{(15), (21), (30)\}$. In particular, if $E/\mathbb{Q}$ is an elliptic curve with $j(E) \notin J_{\mathbb{Q}}(6)$, then $E(K)_{\mathrm{tors}} \in \Phi_{\mathbb{Q}}^{\star}(6)$ for any number field $K/\mathbb{Q}$ of degree 6. Moreover, if $E/\mathbb{Q}$ is an elliptic curve with $E(K)_{\mathrm{tors}} = H \in \{(15), (21), (30)\}$ over some sextic field K, then

(i) $H = (21)$: $j(E) \in \{3^3 \cdot 5^3/2, -3^2 \cdot 5^3 \cdot 101^3/2^{21}, -3^3 \cdot 5^3 \cdot 382^3/2^7, -3^2 \cdot 5^6/2^3\}$.

(ii) $H = (15)$: *then E has Cremona label* **50a3, 50a4, 50b1, 50b2, 450b4,** *or* **450b3.**

(iii) $H = (30)$: *then E has Cremona label* **50a3, 50b1, 50b2,** *or* **450b4.**

Our second result determines $\Phi_{\mathbb{Q}}^{\star}(6, G)$ for each $G \in \Phi(1)$.

Theorem 2. *For each $G \in \Phi(1)$, the set $\Phi_{\mathbb{Q}}^{\star}(6, G)$ is given in Table 1.*

Remark 1. In [14], the second author and Najman show that $(4, 12) \in \Phi_{\mathbb{Q}}(6) \setminus \Phi_{\mathbb{Q}}^{\star}(6)$. In particular, $(4, 12) \in \Phi(6) \setminus \Phi^{\infty}(6)$. Moreover, they show that if $E/\mathbb{Q}$ is an elliptic curve and $K/\mathbb{Q}$ is a sextic extension such that $E(K)_{\mathrm{tors}} = (4, 12)$, then the Cremona label of E is **162d1** or **1296h1** and $K = \mathbb{Q}(\alpha, i)$, where $\alpha^3 - 3\alpha - 4$. In particular, these elliptic curves are $\overline{\mathbb{Q}}$-isomorphic and $j(E) = 109503/64 \in J_{\mathbb{Q}}(6)$.

Corollary 3. *If $J_{\mathbb{Q}}(6) = \{109503/64\}$, then $\Phi_{\mathbb{Q}}(6) = \Phi_{\mathbb{Q}}^{\star}(6) \cup \{(4, 12)\}$ and $\Phi_{\mathbb{Q}}(6, G) = \Phi_{\mathbb{Q}}^{\star}(6, G)$ if $G \neq (1), (3)$ or $\Phi_{\mathbb{Q}}(6, G) = \Phi_{\mathbb{Q}}^{\star}(6, G) \cup \{(4, 12)\}$ if $G = (1)$ or (3).*

---

[1]Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a number field of degree d whose prime divisors are greater than 7. Then $E(K)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$ (see Remark 7.5 in [13]).

TABLE 1

G	$\Phi_{\mathbb{Q}}^{\star}(6, G)$
(1)	$\{(1), (2), (3), (4), (5), (6), (7), (9), (10), (12), (13), (14), (15),$ $(18), (21), (2,2), (2,6), (2,10), (2,14), (2,18), (3,3), (3,9), (4,4), (6,6)\}$
(2)	$\{(2), (4), (6), (8), (10), (12), (14), (16), (18), (2,2),$ $(2,6), (2,10), (2,14), (2,18), (3,6), (3,12), (6,6)\}$
(3)	$\{(3), (6), (9), (12), (15), (21), (30), (2,6),$ $(3,3), (3,6), (3,9), (6,6)\}$
(4)	$\{(4), (8), (12), (2,4), (2,8), (2,12), (3,12), (4,4)\}$
(5)	$\{(5), (10), (15), (30), (2,10)\}$
(6)	$\{(6), (12), (18), (2,6), (2,18), (3,6), (3,12), (6,6)\}$
(7)	$\{(7), (14), (2,14)\}$
(8)	$\{(8), (16), (2,8)\}$
(9)	$\{(9), (18), (2,18), (3,9)\}$
(10)	$\{(10), (2,10)\}$
(12)	$\{(12), (2,12), (3,12)\}$
(2,2)	$\{(2,2), (2,4), (2,6), (2,8), (2,12), (6,6)\}$
(2,4)	$\{(2,4), (2,8), (4,4)\}$
(2,6)	$\{(2,6), (2,12), (6,6)\}$
(2,8)	$\{(2,8)\}$

Conjecture. $\Phi_{\mathbb{Q}}(6) = \Phi_{\mathbb{Q}}^{\star}(6) \cup \{(4,12)\}$
$$= \Phi_{\mathbb{Q}}(2) \cup \Phi_{\mathbb{Q}}(3) \cup \{(30), (2,18), (3,9), (3,12), (4,12), (6,6)\}.$$

Notation. Any specific elliptic curves mentioned in this paper will be referred to by Cremona label [5] and a link to the corresponding LMFDB page [29] will be included for the ease of the reader. Conjugacy classes of subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ will be referred to by the labels introduced by Sutherland in [39, §6.4]. We write $G = H$ (or $G \subseteq H$) for the fact that G is isomorphic to H (or to a subgroup of H, resp.) without further detail on the precise isomorphism. By abuse of notation, we write $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} = (n_1, \ldots, n_r)$.

Remark 2. All of the computations in this paper have been performed using Magma [2] and some of the code has been taken from [7]. All of the code needed to reproduce these computations can be found at [6].

2. BACKGROUND INFORMATION

Central to proving the main results of this paper is understanding fields of definition of the points of order n on an elliptic curve defined over $\mathbb{Q}$. In order to do this we introduce an auxiliary object called the mod n Galois representations associated to the torsion points of elliptic curves. First, fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Given an elliptic curve $E/\mathbb{Q}$ and an integer $n \geq 2$ we let $E[n] = \{P \in E(\overline{\mathbb{Q}}) \mid [n]P = \mathcal{O}\}$ be the subgroup of $E(\overline{\mathbb{Q}})$ consisting of the point of order dividing n. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts coordinatewise on the point of $E[n]$ and this action induces a representation

$$\rho_{E,n} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]).$$

It is a classical result that $E[n]$ is a free rank two $\mathbb{Z}/n\mathbb{Z}$-module and thus fixing a basis $\{P, Q\}$ for $E[n]$ we have that $\mathrm{Aut}(E[n])$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Therefore, we can write the Galois representation as

$$\rho_{E,n} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

where the image of $\rho_{E,n}$, denoted $G_E(n)$, is determined up to conjugacy (i.e., a choice of basis for $E[n]$). If we let $\mathbb{Q}(E[n]) = \mathbb{Q}(\{x, y \mid (x, y) \in E[n]\})$ be the field of definition of the n-torsion points on E, then $\mathbb{Q}(E[n])/\mathbb{Q}$ is a Galois extension and since $\ker \rho_{E,n} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$, from elementary Galois theory we have that $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \simeq G_E(n)$.

Given a point $R \in E[n]$, we will denote the x- and y-coordinates of R by $x(R)$ and $y(R)$, respectively, and the field of definition for R will be denoted by $\mathbb{Q}(R) = \mathbb{Q}(x(R), y(R))$. From Galois theory, we know that there is a subgroup $\mathcal{H}_R$ of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ such that $\mathbb{Q}(R)$ is the subfield of $\mathbb{Q}(E[n])$ fixed by $\mathcal{H}_R$. Letting $H_R = \rho_{E,n}(\mathcal{H}_R)$ we have the following two facts:

(1) $[\mathbb{Q}(R) : \mathbb{Q}] = [G_E(n) : H_R]$.
(2) If $\widehat{\mathbb{Q}(R)}$ is the Galois closure of $\mathbb{Q}(R)$ in $\overline{\mathbb{Q}}$ and $N_{G_E(n)}(H_R)$ is the normalizer of H_R in $G_E(n)$, then $\mathrm{Gal}(\widehat{\mathbb{Q}(R)}/\mathbb{Q}) \simeq G_E(n)/N_{G_E(n)}(H_r)$.

Practically, if we are given $G_E(n)$ up to conjugation, one can deduce many algebraic properties of $\mathbb{Q}(E[n])$. In particular, since $E[n]$ is a free rank two $\mathbb{Z}/n\mathbb{Z}$-module the n-torsion points of E can be (non-canonically) identified with elements of $(\mathbb{Z}/n\mathbb{Z})^2$ by taking their coordinate vectors with respect to a fixed basis. With this identification, the group H_R is exactly the stabilizer of the coordinate vector of R with respect to the action of $G_E(n)$ on $(\mathbb{Z}/n\mathbb{Z})^2$. With this we can compute all possible degrees of $\mathbb{Q}(R)/\mathbb{Q}$ where R is a point of exact order n, by computing the index of the stabilizer of each element of $(\mathbb{Z}/n\mathbb{Z})^2$ of order n inside $G_E(n)$. Lastly, as a consequence of the Weil pairing we always have that the determinant map $\det \colon G_E(n) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is surjective and because $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ contains complex conjugation, $G_E(n)$ must contain an element of trace 0 and determinant -1. For more details about this see [40, Proposition 2.2].

2.1. Classifications of the possible images of Galois representations.

One of the first major results that will be regularly used is the complete classification of elliptic curves with cyclic isogenies. We remind the reader that an elliptic curve E/K has an n-isogeny if there is a degree n map $\phi \colon E \to E'$ such that $\ker \phi$ is a cyclic subgroup of $E[n]$ of order n. If E/K has a cyclic n-isogeny, we know that $E[n]$ contains a Galois-stable cyclic subgroup of order n, and thus $G_E(n)$ is conjugate to a subgroup of the Borel group of upper triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. For the sake of concision, whenever $E/\mathbb{Q}$ has a cyclic n-isogeny defined over $\mathbb{Q}$, we will simply say that E has a *rational n-isogeny*.

Theorem 4 (Mazur [31] and Kenku [23–26]). *Let $E/\mathbb{Q}$ be an elliptic curve with a rational n-isogeny. Then*

$$(1) \qquad\qquad n \in \{1, \ldots, 19, 21, 25, 27, 37, 43, 67, 163\}.$$

Further, there are infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves with a rational n-isogeny for all $n \in \{1, \ldots, 10, 12, 13, 16, 18, 25\}$ and only finitely many for all the other n listed in (1) and if $n \in \{14, 19, 27, 43, 67, 163\}$, then E has complex multiplication.

The next results that we will need are related to the classification of possible images of Galois representations associated to rational elliptic curves of various levels. The first set of results are contained in [40] where Zywina classifies (among other things) the complete list of possible images of the mod ℓ Galois representations associated to rational elliptic curves for all $\ell \leq 13$. We only need the classification up to $\ell = 13$ because as mentioned above $R_{\mathbb{Q}}(6) = \{2, 3, 5, 7, 13\}$. For all of the possible images except three, Zywina gives a complete description of the elliptic curves over $\mathbb{Q}$ whose mod p Galois representation has image conjugate to a subgroup of a given group. Two of the three remaining cases were handled in [1] by Balakrishnan et al. using the Chabauty-Kim method to determine all the rational points on the "cursed" genus 3 modular curve. While a classification for the last remaining image (13S4 in Sutherland's notation) is still just a conjecture, since any curve with this image does not have a point of order 13 defined over a sextic extension for our purposes the classification is complete. The second set of results we will use is contained in [37] where Rouse and Zureick-Brown give a complete account of the possible 2-adic[2] images of Galois representations of elliptic curves without complex multiplication defined over $\mathbb{Q}$. Besides listing each of the possible images they give a complete description of the associated moduli spaces as well; this includes describing all of the rational points on each modular curve.

Finally we give a specific result about rational isogenies for torsion growth over sextic field.

Lemma 5. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication, $K/\mathbb{Q}$ a sextic field, and $P_p \in E(K)_{\text{tors}}$ a point of odd prime order p. Then E has a rational p-isogeny, except if E has Cremona label* 2450ba1 *or* 2450bd1, *and $p = 7$, where there are no rational 7-isogenies. Moreover, in those last cases, the unique sextic fields where the torsion grows are $K = \mathbb{Q}(E[2])$ and $K' = \mathbb{Q}(P_7)$ ($K'/\mathbb{Q}$ is non-Galois), where $E(K)_{\text{tors}} = (2, 2)$ and $E(K')_{\text{tors}} = (7)$, respectively.*

Proof. We have that $p \in R_{\mathbb{Q}}(6) = \{2, 3, 5, 7, 13\}$. Looking at Table 2 we see that, unless $G_E(7)$ is conjugate to 7Ns.2.1, it must be that E has a rational p-isogeny. For the case 7Ns.2.1, [40, Theorem 1.5 (iii)] says that E has Cremona label 2450ba1 or 2450bd1. For those two curves we have that they have no rational isogenies and the unique prime where $\rho_{E,p}$ is non-surjective is $p = 7$. Then by Table 2 we have that the sextic fields where the torsion grows are $K = \mathbb{Q}(E[2])$ and $K' = \mathbb{Q}(P_7)$ and computing the torsion over that number field we obtain the desired result. □

2.2. **Elliptic curves with complex multiplication.** Let $\Phi^{\text{CM}}(d)$ be the set consisting of the torsion subgroups of elliptic curves with complex multiplication (or CM for short) defined over a field of degree d. Table 3 lists the sets $\Phi^{\text{CM}}(d)$ such that $d \mid 6$ since these will be the ones that we use in this article. Proofs of the results in Table 3 can be found in [4, 9, 33, 35, 36].

3. PROOF OF THE MAIN AUXILIARY RESULTS

The determination of $\Phi^{\star}_{\mathbb{Q}}(6)$ and $\Phi^{\star}_{\mathbb{Q}}(6, G)$ will rest on Propositions 6 and 7 for the non-CM and CM cases, respectively.

---

[2]The p-adic Galois representations associated to an elliptic curve are constructed by taking the inverse image of the mod p^n Galois representations.

TABLE 2. Image groups $G_E(p) = \rho_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, for $p \leq 13$, for non-CM elliptic curves $E/\mathbb{Q}$.

Sutherland	Zywina	d_0	d_v	d
2Cs	G_1	1	1	1
2B	G_2	1	1, 2	2
2Cn	G_3	3	3	3
$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$		3	3	6
3Cs.1.1	$H_{1,1}$	1	1, 2	2
3Cs	G_1	1	2, 4	4
3B.1.1	$H_{3,1}$	1	1, 6	6
3B.1.2	$H_{3,2}$	1	2, 3	6
3Ns	G_2	2	4	8
3B	G_3	1	2, 6	12
3Nn	G_4	4	8	16
$\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$		4	8	48
5Cs.1.1	$H_{1,1}$	1	1, 4	4
5Cs.1.3	$H_{1,2}$	1	2, 4	4
5Cs.4.1	G_1	1	2, 4, 8	8
5Ns.2.1	G_3	2	8, 16	16
5Cs	G_2	1	4	16
5B.1.1	$H_{6,1}$	1	1, 20	20
5B.1.2	$H_{5,1}$	1	4, 5	20
5B.1.4	$H_{6,2}$	1	2, 20	20
5B.1.3	$H_{5,2}$	1	4, 10	20
5Ns	G_4	2	8, 16	32
5B.4.1	G_6	1	2, 20	40
5B.4.2	G_5	1	4, 10	40
5Nn	G_7	6	24	48
5B	G_8	1	4, 20	80
5S4	G_9	6	24	96
$\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$		6	24	480

Sutherland	Zywina	d_0	d_v	d
7Ns.2.1	$H_{1,1}$	2	6, 9, 18	18
7Ns.3.1	G_1	2	12, 18	36
7B.1.1	$H_{3,1}$	1	1, 42	42
7B.1.3	$H_{4,1}$	1	6, 7	42
7B.1.2	$H_{5,2}$	1	3, 42	42
7B.1.5	$H_{5,1}$	1	6, 21	42
7B.1.6	$H_{3,2}$	1	2, 21	42
7B.1.4	$H_{4,2}$	1	3, 14	42
7Ns	G_2	2	12, 36	72
7B.6.1	G_3	1	2, 42	84
7B.6.3	G_4	1	6, 14	84
7B.6.2	G_5	1	6, 42	84
7Nn	G_6	8	48	96
7B.2.1	$H_{7,2}$	1	3, 42	126
7B.2.3	$H_{7,1}$	1	6, 21	126
7B	G_7	1	6, 42	252
$\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$		8	48	2016
13S4	G_7	6	72, 96	288
13B.3.1	$H_{5,1}$	1	3, 156	468
13B.3.2	$H_{4,1}$	1	12, 39	468
13B.3.4	$H_{5,2}$	1	6, 156	468
13B.3.7	$H_{4,2}$	1	12, 78	468
13B.5.1	G_2	1	4, 156	624
13B.5.2	G_1	1	12, 52	624
13B.5.4	G_3	1	12, 156	624
13B.4.1	G_5	1	6, 156	936
13B.4.2	G_4	1	12, 78	936
13B	G_6	1	12, 156	1872
$\mathrm{GL}_2(\mathbb{Z}/13\mathbb{Z})$		14	168	26208

TABLE 3. $\Phi^{\mathrm{CM}}(d)$ for $d \mid 6$.

d	$\Phi^{\mathrm{CM}}(d)$
1	$\{(1), (2), (3), (4), (6), (2,2)\}$
2	$\Phi^{\mathrm{CM}}(1) \cup \{(7), (10), (2,4), (2,6), (3,3)\}$
3	$\Phi^{\mathrm{CM}}(1) \cup \{(9), (14)\}$
6	$\Phi^{\mathrm{CM}}(2) \cup \Phi^{\mathrm{CM}}(3) \cup \{(18), (19), (26), (2,14), (3,6), (3,9), (6,6)\}$

Proposition 6. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and $K/\mathbb{Q}$ a sextic number field such that $E(\mathbb{Q})_{\mathrm{tors}} = G$ and $E(K)_{\mathrm{tors}} = H$.*

(a) *$11, 17$, and 19 do not divide the order of H.*

(b) *Let G_2 (resp., H_2) denote the 2-primary part of G (resp., H). Then the only possible 2-primary torsion growth are given in Table 4. For each entry in the table a $(-)$ indicates that the growth from G_2 to H_2 cannot happen. If the growth from G_2 to H_2 is possible, we give the modular curve in the notation of [37] that parameterizes elliptic curves with this growth. That*

TABLE 4. Classification of the possible growth in the 2-primary component over a sextic field.

G_2 \ H_2	(1)	(2)	(4)	(8)	(16)	(2,2)	(2,4)	(2,8)	(4,4)
(1)	X_1	X_1	X_{20}	–	–	X_1	–	–	X_{20b}
(2)	–	X_6	X_{13}	X_{102}, X_{36a}	X_{235m}	X_6	–	–	–
(4)	–	–	X_{13h}	X_{36n}	–	–	X_{13h}	X_{102k}	X_{60d}
(8)	–	–	–	X_{102p}	X_{235l}	–	–	X_{102p}	–
(2,2)	–	–	–	–	–	X_8	X_{25}, X_{8d}	$X_{193}, X_{96q}, X_{98o}$	–
(2,4)	–	–	–	–	–	–	X_{25n}	X_{96t}, X_{98e}	X_{58i}
(2,8)	–	–	–	–	–	–	–	X_{193n}	–

is, $E(\mathbb{Q})_{\mathrm{tors}}$ contains a subgroup isomorphic to G_2 and there is a sextic extension $K/\mathbb{Q}$ such that $E(K)_{\mathrm{tors}}$ contains a subgroup isomorphic to H_2 if and only if E corresponds to a rational point on the given modular curves.

(c) If $(4) \subseteq G$, then $(20) \nsubseteq H$.
(d) If $(8) \subseteq G$, then $(24) \nsubseteq H$.
(e) If $(2,2) \subseteq G$, then $(2,10) \nsubseteq H$.
(f) If $(2,4) \subseteq G$, then $(2,12) \nsubseteq H$.
(g) If $G = (12)$, then $H \neq (24)$.
(h) If $G = (2,2)$, then $(2,14) \nsubseteq H$.
(i) If $G = (1)$ and $(3,6) \subseteq H$, then $(6,6) \subseteq H$.
(j) If $G = (3)$, then $H \neq (3,12)$.
(k) $H \neq (20)$.
(l) If $G = (3)$, then $H \neq (18)$.
(m) If $(2,2) \subseteq G$, then $(2,18) \nsubseteq H$.
(n) If $G = (3)$, then $H \neq (2,18)$.
(o) If $G = (7)$, then $(21) \nsubseteq H$.
(p) If $G = (2), (4),$ or (6), then $H \neq (24)$.
(q) $(26) \nsubseteq H$.
(r) $H \neq (27)$.
(s) $H \neq (28)$.
(t) If $G \neq (3)$ or (5), then $H \neq (30)$.

Proof. (a) By [13] we have $11, 17, 19 \notin R_{\mathbb{Q}}(6) = \{2, 3, 5, 7, 13\}$.

(b) As mentioned in Section 2, Rouse and Zureick-Brown completely classify all of the possible 2-adic images of Galois representations associated to elliptic curves without CM defined over $\mathbb{Q}$ in [37]. For each of the possible images the second author together with Lozano-Robledo computed the degree of the field of definition of the $(2^i, 2^{i+j})$ torsion for $i + j \leq 6$ in [11] and recoded the data in a text file titled `2primary_Ss.txt` (cf. [11]). Using the results of [11] we write a program that takes as its input a degree d and returns an associative array whose keys are all the possible 2-primary parts of $E(\mathbb{Q})_{\mathrm{tors}}$ and $E(K)_{\mathrm{tors}}$ of elliptic curves defined over $\mathbb{Q}$ and base-extended to a degree d number field K over $\mathbb{Q}$. The objects associated with each of these curves are the labels of the modular curves (in the notation of [37]) that parameterize each of the possible growths in two primary components. This algorithm and its output can be found in [6] in the file labeled `RZB_Search.txt`.

(c), (d), (e), and (f): See Remark below Theorem 7 of [12].

(g) The 2-divisibility method [19, Section 3] asserts that if a point Q satisfies $2Q = P$, then $[K(Q) : K] \leq 4$ (see [19, Remark 3.2]). In the particular case of $K = \mathbb{Q}$ and P of order 12, we have that (24) is a subgroup of some group in $\Phi_{\mathbb{Q}}(d)$ for $d \leq 4$. But we know that this can only happen in a quartic extension [13, Corollary 8.7] of $\mathbb{Q}$ and thus cannot happen over a sextic extension.

(h) Suppose that $G = (2, 2)$ and $(2, 14) \subseteq H$. Since $(2, 14)$ is not a subgroup of any group in $\Phi_{\mathbb{Q}}(d, (2, 2))$ for $d = 2, 3$ by [16, Theorem 2] and [15, Theorem 1.2], respectively, we have that E gains a point of order 7 over a sextic field, and not over any number field of degree less than 6. By Lemma 5 we have that, unless $G_E(7)$ is conjugate to 7Ns.2.1, E has a rational 7-isogeny. In the former case we have $G = (1)$ and therefore we can exclude it for the rest of the proof. Now, since $G = (2, 2)$, then E is 2-isogenous (over $\mathbb{Q}$) to two curves E' and E'', such that E, E', and E'' are all non-isomorphic pairwise. Further, there is a rational 4-isogeny from E' to E'' that is necessarily cyclic. Moreover, since E has a rational 7-isogeny, if follows that E' also has a rational 7-isogeny, and therefore E' would have a rational 28-isogeny which is impossible by Theorem 4.

(i) Suppose that $G = (1)$ and $(3, 6) \subseteq H$. Checking Table 2 (see the Appendix) we see that the only way that we can go from trivial torsion to having full 3-torsion over a sextic extension of $\mathbb{Q}$ is for $G_E(3)$ conjugate to 3B.1.2. Therefore, we can pick a basis P_3, P_3' for $E[3]$ such that $[\mathbb{Q}(P_3) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(P_3') : \mathbb{Q}] = 3$ and $K = \mathbb{Q}(P_3, P_3')$ is an S_3-extension of $\mathbb{Q}$, since 3B.1.2 is isomorphic to S_3. Next, in order to pick up a point P_2 not defined over $\mathbb{Q}$, it must be that $[\mathbb{Q}(P_2) : \mathbb{Q}] = 3$, where $G_E(2)$ is conjugate to 2Cn or $\rho_{E,2}$ is surjective. In the first case we have $\mathbb{Q}(P_2) = \mathbb{Q}(E[2]) \subseteq K$. In the second case $\mathbb{Q}(E[2])$ is the Galois closure of $\mathbb{Q}(P_2)$, that is, the S_3-extension of $\mathbb{Q}$ that contains $\mathbb{Q}(P_2)$. Therefore, $\mathbb{Q}(E[2]) = \mathbb{Q}(E[3])$. In both cases we obtain that $(6, 6) \subseteq E(K)_{\mathrm{tors}}$. Therefore H cannot equal $(3, 6)$.

(j) If $G = (3)$ and $H = (3, 12)$, then we know that E must have a rational 3-isogeny and from part (b) in order for $E/\mathbb{Q}$ to gain a point of order 4 over a sextic extension E must correspond to a $\mathbb{Q}$-rational point on the modular curve X_{20}. Taking the fiber product of $X_0(3)$ and X_{20} we get a singular genus 1 curve C whose desingularization is the elliptic curve $E'/\mathbb{Q}$ with Cremona label 48a3 and $E'(\mathbb{Q}) = (2, 4)$. Inspecting the rational points on C we get that there are four non-singular non-cuspidal points corresponding to the j-invariants $109503/64$ and $-35937/4$. For each of these j-invariants there is exactly one $\mathbb{Q}$-isomorphism class that has a point of order 3 defined over $\mathbb{Q}$. Representatives of these classes are the curves with Cremona label 162a1 and 162d1. Checking the 3-division fields of each of these curves, we see that neither gains full 3-torsion and a point of order 6 over the same sextic extension of $\mathbb{Q}$.

(k) If $(2) \subseteq G$, then E has a rational point of order 2 and the 2-power division fields are all 2-extensions of $\mathbb{Q}$. Therefore, if $H = (20)$ it must be that if P_4 is the point of order 4 over K, then $\mathbb{Q}(P_4)$ is a quadratic extension of $\mathbb{Q}$. Further, by Table 2, the only way that E can have a point P_5 of order 5 over K is if $\mathbb{Q}(P_5)$ is defined over a quadratic extension of $\mathbb{Q}$. If K is a sextic extension, then it must be that $\mathbb{Q}(P_4) \subseteq \mathbb{Q}(P_5)$ and E actually has a point of order 20 defined over a quadratic extension which is impossible.

Lastly, if $(2) \not\subset G$ and $H = (20)$, then E gains a point P_4 of order 4 over a degree 3 or 6 field and from part (b), the only way this can happen is if E corresponds to a rational point on the curve X_{20} from [37]. Again by Lemma 5, in order to

gain a point of order 5 over a sextic extension, E must have a rational 5-isogeny. Computing the fiber product of X_{20} and $X_0(5)$ we get a genus 3 hyperelliptic curve C with $\mathrm{Aut}(C) = (2, 2)$. The automorphism group of C is generated by the hyperelliptic involution and another automorphism of order two, call it ϕ. The curve E' obtained by quotienting out by ϕ is the elliptic curve with Cremona label `80a4` which has $E'(\mathbb{Q}) = (4)$. Computing the preimage of the four points on E' we see that $C(\mathbb{Q})$ consists of exactly three points, two of which are singular and one is a cusp at infinity. Thus, there are no elliptic curves over $\mathbb{Q}$ that gain a point of order 4 over a sextic and have a rational 5-isogeny.

(l) Suppose towards a contradiction that $G = (3)$ and $H = (18)$ and let P_2 and P_9 be points in $E(K)$ of order 2 and 9, respectively. Since $E(\mathbb{Q})[2]$ is trivial it must be that $[\mathbb{Q}(P_2) : \mathbb{Q}] = 3$ and from [13, Proposition 4.6] we have that $[\mathbb{Q}(P_9) : \mathbb{Q}] = 2, 3$, or 6. From [16] we know that $[\mathbb{Q}(P_9) : \mathbb{Q}] \neq 2$ and from [15] we know that $[\mathbb{Q}(P_9) : \mathbb{Q}] \neq 3$ since there are no elliptic curves whose torsion grows from (3) to (18) over a cubic. So it must be that $[\mathbb{Q}(P_2) : \mathbb{Q}] = 3$, $[\mathbb{Q}(P_9) : \mathbb{Q}] = 6$, and $K = \mathbb{Q}(P_9)$. So we search in Magma for subgroups of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ that would correspond to an elliptic curve with a rational point of order 3 and a point of order 9 defined over a degree 6 extension of $\mathbb{Q}$. We get that this can happen in three different ways according to the Galois closure of $\mathbb{Q}(P_9)$. That is, $\mathrm{Gal}(\widehat{K}/\mathbb{Q}) \cong \mathcal{C}_6, S_3$, or $\mathcal{C}_3 \times S_3$. In the first two cases, we have that $\widehat{K} = K = \mathbb{Q}(P_9)$ and since $\mathbb{Q}(P_2) \subseteq \mathbb{Q}(P_9)$ we know that the Galois closure of $\mathbb{Q}(P_2)$, which is $\mathbb{Q}(E[2])$, is contained in K and this is a contradiction to the assumption that $H = (18)$, and cyclic. Therefore, it must be that $\mathrm{Gal}(\widehat{K}/\mathbb{Q}) = \mathcal{C}_3 \times S_3$ and we have the field diagram
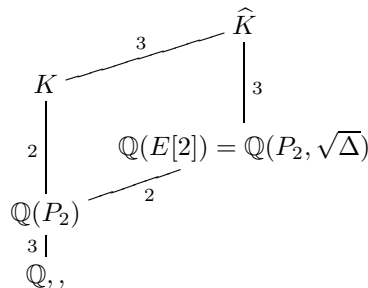
where Δ is the discriminant of E and Δ is not a square since $\mathbb{Q}(E[2]) \nsubseteq K$. But, since there is a unique subgroup of $\mathcal{C}_3 \times S_3$ of index 2, we know that there is a unique quadratic extension of $\mathbb{Q}$ inside $\widehat{K}$ and by the above field diagram it must be that $\mathbb{Q}(\sqrt{\Delta})$ is inside of K. This means that $K = \mathbb{Q}(P_9) = \mathbb{Q}(P_2, \sqrt{\Delta}) = \mathbb{Q}(E[2])$ which is a Galois extension of $\mathbb{Q}$ giving us a contradiction.

(m) We have that $(2, 18)$ is not a subgroup of any group in $\Phi_{\mathbb{Q}}(d)$ for $d = 2, 3$. Therefore we have that there must exist a point P_3 of order 3 such that $[\mathbb{Q}(P_3) : \mathbb{Q}] = 6$ and there is no other point of order 3 defined over a number field of degree less than 6. According to Table 2 this cannot happen.

(n) Suppose towards a contradiction that $G = (3)$ and $H = (2, 18)$. Let P_9 be the point of order 9 defined over K. In this case we have that $[\mathbb{Q}(P_9) : \mathbb{Q}] = 2, 3$, or 6 and $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 3$ or 6. We can exclude the case $[\mathbb{Q}(P_9) : \mathbb{Q}] = 2$ since (9) is not the subgroup of some group in $\Phi_{\mathbb{Q}}(2, (3))$ (see [16, Theorem 2]). From [15] we know that both of these indices cannot be 3. Suppose that $[\mathbb{Q}(P_9) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$. This means that $\mathbb{Q}(P_9)/\mathbb{Q}$ is a degree 3 subfield of $\mathbb{Q}(E[2])$

and so E must have a point of order 2 defined over $\mathbb{Q}(P_9)$. In this case we would have $\mathbb{Q}(P_9)/\mathbb{Q}$ is a cubic extension where $E(\mathbb{Q}(P_9))_{\text{tors}} = (18)$ but this cannot happen from [15, Theorem 1.2]. Therefore it must be that $[\mathbb{Q}(P_9) : \mathbb{Q}] = 6$ and $K = \mathbb{Q}(P_9)$. Just as in part (l) there are only three possible options for $\text{Gal}(\widehat{K}/\mathbb{Q})$; they are $\mathcal{C}_6, S_3$, and $\mathcal{C}_3 \times S_3$. The third case gives the exact same contradiction as in part (l), while if $\text{Gal}(\widehat{K}/\mathbb{Q}) = \mathcal{C}_6$, or S_3, then $\mathbb{Q}(P_9)/\mathbb{Q}$ is a Galois extension and $\langle P_9 \rangle$ is a cyclic Galois stable subgroup of $E(K)$. Therefore $G_E(9)$ must be conjugate to a subgroup of the Borel subgroup of $\text{GL}_2(\mathbb{Z}/9\mathbb{Z})$, implying that $\langle P_9 \rangle$ must be the kernel of a rational n-isogeny and $\mathbb{Q}(P_9)/\mathbb{Q}$ must be a cyclic extension. Therefore, $\text{Gal}(K/\mathbb{Q}) = \mathcal{C}_6$ and E has a rational 9-isogeny. Since $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(P_9)$ and $\mathbb{Q}(E[2])/\mathbb{Q}$ is Galois, it must be that $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq \mathcal{C}_3$ which can only happen if E has square discriminant. Checking in Magma we see that there are no curves with a rational 9-isogeny and square discriminant.

(o) By [16, Theorem 2] and [15, Theorem 1.2] we have that if E gains a point P_3 of order 3 over a sextic field, then $[\mathbb{Q}(P_3) : \mathbb{Q}] = 6$ and there is no other point of order 3 defined over a number field of degree less than 6. But this is impossible by Table 2.

(p) Suppose $G = (2), (4)$, or (6). In all of these cases E has a rational point of order 2 and so the Tate module $T_2(E)$ is a tower of 2-extensions. Therefore, if P_8 is a point of order 8 on E defined over a sextic extension of $\mathbb{Q}$, then it must be that $[\mathbb{Q}(P_8) : \mathbb{Q}] = 2$ and thus, by [7, Lemma 4.6], E has a rational 8-isogeny. Further, if E gains a point of order 3 over a sextic extension of $\mathbb{Q}$, then by Lemma 5 E must have a rational 3-isogeny. Therefore in all of these cases, if $H = (24)$, then E must have a rational 24-isogeny which is impossible by Theorem 4.

(q) Let $P_2, P_{13} \in E(K)_{\text{tors}}$ be of order 2 and 13, respectively. By Lemma 5, E has a rational 13-isogeny. In the case that $\mathbb{Q}(P_2) = \mathbb{Q}$ we have that there is a rational 26-isogeny which cannot happen by Theorem 4. Now, if $\mathbb{Q}(P_2) \neq \mathbb{Q}$, then $[\mathbb{Q}(P_2) : \mathbb{Q}] = 3$ and $\mathbb{Q}(P_2) \subseteq \mathbb{Q}(P_{13})$. Note that $\mathbb{Q}(P_2) \neq \mathbb{Q}(P_{13})$, since (26) is not a subgroup of some group in $\Phi_{\mathbb{Q}}(3)$. Therefore $[\mathbb{Q}(P_{13}) : \mathbb{Q}] = 6$ and Table 2 shows that $G_E(13)$ is conjugate to `13B.3.4` or `13B.4.1`. In both cases we have that the field $\mathbb{Q}(P_{13})$ is Galois and cyclic of order 6 (see (2) from Section 2). If $\rho_{E,2}$ is non-surjective, then the Galois group of $\mathbb{Q}(P_2)$ is isomorphic to $\text{GL}_2(\mathbb{Z}/2\mathbb{Z})$ contradicting the fact that $\mathbb{Q}(P_2) \subsetneq \mathbb{Q}(P_{13})$. The remaining case is when $G_E(2)$ is conjugate to `2Cn`. The fiber product of the genus 0 modular curves $X_0(13)$ and X_{2Cn} is the elliptic curve with Cremona label `52a2` which has only the affine point $(0,0)$. This point does not correspond to an elliptic curve in $X_0(13)$ or X_{2Cn}. Therefore we have proved that $(26) \not\subseteq E(K)_{\text{tors}}$.

(r) Suppose that $H = (27)$; then $G = (1), (3)$, or (9). By Lemma 5, E has a rational 3-isogeny. Therefore, $G_E(27)$ must conjugate to a subgroup of $\pi^{-1}(B(3))$, where $B(3)$ is the Borel subgroup of $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and $\pi\colon \text{GL}_2(\mathbb{Z}/27\mathbb{Z}) \to \text{GL}_2(\mathbb{Z}/3\mathbb{Z})$. Constructing a list of the subgroups of $\pi^{-1}(B(3))$ with surjective determinant, containing an element corresponding to complex conjugation, and not conjugate to a subgroup of $B(27)$ (since the only curves with a rational 27-isogeny have CM), we find there are 687 possible images for $\rho_{E,27}$. Of those 687 images, 42 of them would give rise to an elliptic curve with a point of order 27 over a sextic. Among those 42 possibilities there are exactly seven maximal elements all of which are conjugate to a subgroup of $B(9)$. Five of these seven maximal groups reduce to subgroups of $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ that are conjugate to subgroups of the split Cartan subgroup. If E were

an elliptic curve whose mod 27 Galois representation is conjugate to a subgroup of one of these five groups, then E would have to have independent rational 3- and 9-isogenies. From [34, Lemma 7], any elliptic curve with independent rational 3- and 9-isogenies is isogenous to an elliptic curve with a rational 27-isogeny and from [30, Table 4] there is only one elliptic curve (up to $\overline{\mathbb{Q}}$-isomorphism) with a rational 27-isogeny. The $\overline{\mathbb{Q}}$-isomorphism class of curves with a 27-isogeny has j-invariant equal to $-2^{15} \cdot 3 \cdot 5^3$ and consists of all quadratic twists of the elliptic curve with Cremona Reference 27a2. Since isogeny classes are invariant under quadratic twist it is sufficient to check the isogeny class of 27a2 in the LMFDB database [29] to see the only way that E can have an independent rational 3- and 9-isogeny is if $j(E) = 0$ and E thus has CM. Therefore, $G_E(27)$ must be conjugate to a subgroup of one of the remaining two maximal groups. These two groups are

$$G_1 = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 10 & 22 \\ 18 & 10 \end{pmatrix} \right\rangle$$

and

$$G_2 = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 19 & 4 \\ 9 & 19 \end{pmatrix} \right\rangle.$$

Working in Magma we see that $G_1 \cap \mathrm{SL}_2(\mathbb{Z}/27\mathbb{Z})$ (resp., $G_2 \cap \mathrm{SL}_2(\mathbb{Z}/27\mathbb{Z})$) is conjugate to a subgroup of the group with Cummins-Pauli label $27A^2$ (resp., $27B^4$). The modular curves that correspond to the groups $27A^2$ and $27B^4$ are genus 2 and 4, respectively, and it was shown in the proof of Proposition 5.18 in [7] that the only $\mathbb{Q}$-rational points on these curves are cusps. Therefore there are no elliptic curves over $\mathbb{Q}$ whose mod 27 image is contained in either G_1 or G_2.

(s) If $H = (28)$, then E gains a point of order 7 over a sextic field. Then, by Lemma 5, if E doesn't have a rational 7-isogeny, then $E(K)_{\text{tors}} = (7)$ or $E(K)_{\text{tors}} = (2, 2)$. Therefore we have that E must have a rational 7-isogeny. Now, first suppose that $(2) \subseteq G$. Then E would have a rational 14-isogeny defined over $\mathbb{Q}$ and from Theorem 4 this can only happen if E has complex multiplication.

If $G = (1)$ and $H = (28)$, then E must gain a point of order 4 over a cubic or a sextic extension of $\mathbb{Q}$ which from part (b) can only happen if E corresponds to a rational point on the genus 0 curve X_{20} from [37]. So it must be that E comes from a point on X_{20} and a point on $X_0(7)$. Computing the fiber product of $X_0(7)$ and X_{20}, we get a genus 3 hyperelliptic curve C with $\mathrm{Aut}(C) = (2, 2, 2)$. Quotienting out by one of the automorphisms of order 2 that is not the hyperelliptic involution we get the elliptic curve E' with Cremona label 14a4 satisfying $E'(\mathbb{Q}) = (6)$. Pulling the six points in $E'(\mathbb{Q})$ back to $C(\mathbb{Q})$ we see that there are exactly four non-cuspidal and non-singular rational points on C corresponding to the j-invariants $-3^3 \cdot 13 \cdot 479^3 / 2^{14}$ and $3^3 \cdot 13 / 2^2$. From [40, Theorem 1.5], all of the twists of these curves have the kernel of their rational 7-isogeny defined over a cyclic sextic extension of $\mathbb{Q}$ except for two of them. Further, the only way that E can have the 2-primary component of its torsion grow from trivial to (4) over a cyclic sextic extension of $\mathbb{Q}$ is if it actually grows over a quadratic extension of $\mathbb{Q}$. This is because the point of order 4 would define the kernel of a rational isogeny and hence by [7, Lemma 4.8] the degree of its field of definition would have to divide $\varphi(4) = 2$, but this cannot happen by [16, Theorem 2]. Therefore, we can rule out these curves since $\mathbb{Q}(P_7)$ can never coincide with $\mathbb{Q}(P_4)$. Next from [40, Theorem 1.5], we know that for each of these j-invariants there is exactly one twist (up to $\mathbb{Q}$-isomorphism) such

that the kernel of their rational 7-isogeny is defined over a cyclic cubic extension of $\mathbb{Q}$. The $\mathbb{Q}$-isomorphism classes in question are represented by the elliptic curves with Cremona label `338b1` and `16562be2` and we eliminate these by checking that the 2-division field and the cubic field where the kernel of the rational 7-isogeny intersect only in $\mathbb{Q}$.

Next if $G = (7)$, again E must have a rational 7-isogeny and so in order to gain a point of order 4 it must have j-invariant $-3^3 \cdot 13 \cdot 479^3/2^{14}$ and $3^3 \cdot 13/2^2$, but none of these curves have a rational point of order 7.

(t) By Lemma 5 the only way for a curve to gain a point of order 3 or 5 over a sextic extension is for E to have a rational 3- or 5-isogeny, respectively. Therefore, if $G = (2), (6)$, or (10) and $H = (30)$, E must have rational 30-isogeny which is impossible by Theorem 4.

If $G = (1)$, then again E must have a rational 15-isogeny and $j(E) \in \{-5^2/2,$ $-5^2 \cdot 241^3/2^3, -5^2 \cdot 29^3/2^5, 5 \cdot 211^3/2^{15}\}$ (see [30, Table 4]). Further, by [7, Lemma 4.8] we know that the kernel of the rational 15-isogeny is defined over a field of degree dividing $\varphi(15) = 8$. Therefore, if the kernel of the rational 15-isogeny is defined over a sextic field, it must in fact be defined over a quadratic field. But from [34, Theorem 2 (c)] there are no curves with $G = (1)$ and a point of order 15 over a quadratic field, so this is not possible. Thus the kernel of the rational 15-isogeny cannot be defined over a sextic extension.

Looking at Table 2 we see that the only way to have a point of order 3 and a point of order 5 defined over a sextic field without having any rational points (since we are in the case where $G = (1)$) is for the point of order 5 to be defined over a quadratic extension of $\mathbb{Q}$ (i.e., $G_E(5)$ is conjugate to a subgroup of `5B.4.1`) and the point of order 3 has to be defined over a cubic extension or a sextic extension of $\mathbb{Q}$ (i.e., $G_E(3)$ is conjugate to `3B.2.1` or `3B`, respectively). We point out here that `3B.2.1` is contained inside of `3B` and in fact the group generated by `3B.2.1` and $-I$ is equal to `3B`. Therefore the j-maps from these modular curves are the same and for each $\overline{\mathbb{Q}}$-isomorphism class corresponding to a point on the modular curve $X_{3B} = X_0(3)$ there is a unique twist such that $G_E(3)$ is conjugate to `3B.2.1`. Constructing the fiber product of these two genus 0 modular curves we get the elliptic curve $E'/\mathbb{Q}$ with Cremona label `15a3` and $E'(\mathbb{Q}) = (2, 4)$. The rational points of E' give four non-singular non-cuspidal points corresponding to the two j-invariants $5 \cdot 7 \cdot 11 \cdot 43 \cdot 421/2^{15}$ and $-5 \cdot 29^3/2^5$. Using [40, Theorem 1.2], we see that each of these two curves has exactly one twist (up to $\mathbb{Q}$-isomorphism) with a point of order 3 defined over a cubic field. The $\mathbb{Q}$-isomorphism classes in question are represented by curves with Cremona label `50a4` and `450b3`. Examining the division fields of these curves we see that the cubic fields where they gain a point of order 3 are disjoint from the 2-division fields. Since these division fields are invariant under twisting, no twist of these curves can gain a point of order 30 over a sextic extension of $\mathbb{Q}$.

Before moving on, we point out the following: if $E/\mathbb{Q}$ is either the elliptic curve with Cremona label `50a4` or `450b3` and P_{15} is the point of order 15 defined over a sextic extension of $\mathbb{Q}$, then from [40, Theorems 1.2 and 1.4] twisting E by a square-free integer d can only affect the degree of the field of definition of P_{15} in the following ways. If $d = -3$, then E^d has a rational point of order 3, and if $d = 5$, then E^d has a rational point of order 5 and in both of these cases $G \neq (1)$. If d is any other square-free integers, the field of definition of the point of order 15

becomes $\mathbb{Q}(P_{15}, \sqrt{d})/\mathbb{Q}$ which is a degree 12 extension. Therefore, these are the only two curves with $G = (1)$ and $H = (15)$ up to $\mathbb{Q}$-isomorphism. $\square$

For the case when $E/\mathbb{Q}$ is an elliptic curve with complex multiplication we give the following result.

Proposition 7. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication and $K/\mathbb{Q}$ a sextic number field such that $E(\mathbb{Q})_{\mathrm{tors}} = G$ and $E(K)_{\mathrm{tors}} = H$.*

- (A) $11, 13, 17,$ *and* 19 *do not divide the order of* H.
- (B) *If* $G = (1)$ *or* (2), *then* $H \neq (2,4)$.
- (C) *If* $G = (2,2)$, *then* $(2,14) \not\subseteq H$.
- (D) *If* $G = (1)$, *then* $H \neq (3,6)$.
- (E) *If* $G = (3)$, *then* $H \neq (18)$.

Proof. (A) We know that $R_{\mathbb{Q}}(6) = \{2,3,5,7,13\}$. Then we only need to prove the statement for 13. By [40, §1.8] we have that $G_E(13)$ is 13Ns, 13Nn, or $G^3(13)$. Therefore by Theorem 5.6 in [13] we have an explicit characterization of the degree $[\mathbb{Q}(P_{13}) : \mathbb{Q}]$, where P_{13} is a point of order 13. In particular the minimum degree of $\mathbb{Q}(P_{13})/\mathbb{Q}$ is 24.

(B) First suppose towards a contradiction that $G = (1)$ and $H = (2,4)$. From [15,16] we know that this growth cannot happen over a quadratic or cubic extension of $\mathbb{Q}$. Next since $G = (1)$ we have that $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 3$ or 6 and the only way that $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 3$ is if the discriminant of E is a square. Looking at the tables of CM elliptic curves over $\mathbb{Q}$ in [38, Appendix A, §3] we check that there is only one $\overline{\mathbb{Q}}$-isomorphism class of CM elliptic curves with a square discriminant, all of the form $y^2 = x^3 - r^2 x$ with $r \in \mathbb{Q}$. All of these curves have full 2-torsion over $\mathbb{Q}$ and thus do not have $G = (1)$. So we may assume that $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$ and thus $\mathbb{Q}(E[2]) = K$ is a Galois extension of $\mathbb{Q}$. Now, from [7, Lemma 4.6] since $K/\mathbb{Q}$ is Galois and $E(K)_{\mathrm{tors}} = (2,4)$ we know that E must have a rational 2-isogeny which can only happen if E has a rational point of order 2, contradicting the assumption that $G = (1)$.

Next suppose towards a contradiction that $G = (2)$ and $H = (2,4)$. Again, from [15,16] we know that this growth cannot happen over a quadratic or cubic extension of $\mathbb{Q}$. In this case $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 2$ and so there must be a point of order 2 defined over a quadratic field that becomes divisible by 2 in a cubic extension, but this is impossible by [13, Proposition 4.6].

(C) Since $G = (2,2)$ we have that $E : y^2 = x^3 - r^2 x$ for some $r \in \mathbb{Q}$ (see [40, Proposition 1.15]). In particular $j(E) = 1728$ and [40, Proposition 1.14] shows that $G_E(7)$ is conjugate to 7Nn. In this case, if P is a point of order 7, we have $[\mathbb{Q}(P) : \mathbb{Q}] = 48 > 6$.

(D) Analogous to the proof of Proposition 6(i) we need a point $P_2 \in E[2]$ not defined over $\mathbb{Q}$, no rational points of order 3, and $[\mathbb{Q}(E[3]) : \mathbb{Q}]$ divides 6. By Propositions 1.14, 1.15, and 1.16 from [40] and [13, Theorem 5.7] this is only possible if $\rho_{E,2}$ is non-surjective and $G_E(3)$ is conjugate to 3B.1.2. This gives the same contradiction as Proposition 6(i).

(E) Note that in the proof of the similar statement but without complex multiplication (see Proposition 6(l)) we have not used the condition that the elliptic curve is without complex multiplication. $\square$

Theorem 8. *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose $E(K)_{\text{tors}} = (21)$ over some sextic number field K. Then $j(E) \in \{3^3 \cdot 5^3/2, -3^2 \cdot 5^3 \cdot 101^3/2^{21}, -3^3 \cdot 5^3 \cdot 382^3/2^7, -3^2 \cdot 5^6/2^3\}$.*

Proof. By Lemma 5, if E has Cremona label `2450ba1` or `2450bd1`, then $E(K)_{\text{tors}} \neq (21)$, otherwise if $E(K)_{\text{tors}} = (21)$, then E has a rational 3- and a rational 7-isogeny; therefore a rational 21-isogeny. That is, $j(E) \in \{3^3 \cdot 5^3/2, -3^2 \cdot 5^3 \cdot 101^3/2^{21}, -3^3 \cdot 5^3 \cdot 382^3/2^7, -3^2 \cdot 5^6/2^3\}$ by the classification of the rational points in $X_0(21)$ (see [30, Table 4]). $\square$

Theorem 9. *Let $E/\mathbb{Q}$ be an elliptic curve, $K/\mathbb{Q}$ a sextic number field, and $E(K)_{\text{tors}} = H$. Then:*

    (i) *If $H = (15)$, then E has Cremona label `50a3`, `50a4`, `50b1`, `50b2`, `450b4`, or `450b3`.*

    (ii) *If $H = (30)$, then E has Cremona label `50a3`, `50b1`, `50b2`, or `450b4`.*

Proof. From the proof of Proposition 6(t), we know that the only elliptic curves with $G = (1)$ and $H = (15)$ or (30) are the elliptic curves with `50a4` and `450b3` and they both have $H = (15)$. Therefore, all that remains to classify are the elliptic curve with $G = (3)$ or $G = (5)$ and $H = (15)$ or $H = (30)$.

Starting with an elliptic curve with $G = (3)$, from Table 2 we get that the only way to gain a point of order 5 over a sextic field is to gain it over a quadratic extension of $\mathbb{Q}$. So first classify all elliptic curves with a point of order 3 over $\mathbb{Q}$ and a rational 5-isogeny defined over a quadratic extension. In order to have a rational point of order 3, it must be that $G_E(3)$ is conjugate to a subgroup of `3B.1.1` while having a point of order 5 defined over a quadratic extension requires $G_E(5)$ to be conjugate to a subgroup of `5B.4.1`. Computing the fiber product of the two corresponding genus 0 modular curves we see that there are exactly two curves (up to $\mathbb{Q}$-isomorphism) that simultaneously have these properties and they are ones with Cremona label `450b4` and `50a3`. Because these curves gain a point of order 15 over a quadratic extension and every elliptic curve with trivial 2-torsion gains a point of order 2 over a cubic extension, we know that for each of `450b4` and `50a3` there is a sextic extension of $\mathbb{Q}$ where $H = (15)$ and a sextic extension of $\mathbb{Q}$ where $H = (30)$.

Lastly, we classify the elliptic curves that have $G = (5)$ and a rational 3-isogeny. This time to have a rational point of order 5, $G_E(5)$ must be conjugate to `5B.1.1` while a rational 3-isogeny requires that $G_E(3)$ is conjugate to a subgroup of `3B`. Computing the fiber product of these two genus 0 modular curves we see that there are exactly two elliptic curves (up to $\mathbb{Q}$-isomorphism) with both these properties simultaneously and they are the curves with Cremona label `50b1` and `50b2`. Again for both `50b1` and `50b2` there is a quadratic extension of $\mathbb{Q}$ where E gains a point of order 3 and so for each of these curves there is a sextic extension of $\mathbb{Q}$ where $H = (15)$ and a sextic extension of $\mathbb{Q}$ where $H = (30)$. $\square$

Remark 3. Let α and $\beta \in \overline{\mathbb{Q}}$ be such that $\alpha^3 - \alpha^2 + 2\alpha + 2 = 0$ and $\beta^3 - \beta^2 - 3\beta - 3 = 0$. Table 5 shows the sextic fields (or subfields) where the torsion grows to (15) or (30).

Theorem 10. *There are infinitely many non-isomorphic (over $\overline{\mathbb{Q}}$) elliptic curves $E/\mathbb{Q}$ such that there is a sextic number field K with $E(K)_{\text{tors}} = (2, 18)$ (resp., $(3, 9)$, $(3, 12)$, $(6, 6)$).*

TABLE 5. Data about torsion growth to (15) or (30) over sextic fields.

G $\diagdown$ H E	(15)	(30)
(3) 50a3	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{5}, \alpha)$
(1) 50a4	$\mathbb{Q}(\sqrt[6]{5})$	$-$
(5) 50b1	$\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-15}, \beta)$	$\mathbb{Q}(\sqrt{5}, \alpha)$
(5) 50b2	$\mathbb{Q}(\sqrt{-15})$, $\mathbb{Q}(\sqrt[6]{5})$	$\mathbb{Q}(\sqrt{-15}, \alpha)$
(3) 450b4	$\mathbb{Q}(\sqrt{-15})$	$\mathbb{Q}(\sqrt{-15}, \alpha)$
(1) 450b3	$\mathbb{Q}(\sqrt{-15}, \beta)$	$-$

Proof. Given $G \in \Phi(1)$ there exists a one-parameter family, called the Kubert-Tate normal form,

$$\mathcal{T}_t^G : \ y^2 + (1-c)xy - by = x^3 - bx^2, \qquad \text{where } b, c \in \mathbb{Q}(t),$$

such that G is a subgroup of $\mathcal{T}_t^G(\mathbb{Q}(t))_{\text{tors}}$ for all but finitely many values of $t \in \mathbb{Q}$ (cf. [28, Table 3]). For $G = (9)$ and $G = (12)$ we have

$$\begin{aligned}
G = (9) \quad &: \quad c = t^2(t-1), \\
&\quad\ \ b = c(t^2 - t + 1), &&t \neq 0, 1, \\
G = (12) \quad &: \quad c = (3t^2 - 3t + 1)(t - 2t^2)/(t-1)^3, \\
&\quad\ \ b = c(2t - 2t^2 - 1)/(t-1), &&t \neq 0, 1, 1/2.
\end{aligned}$$

Thanks to the classification of $\Phi(1)$ we have that for those values of $t \in \mathbb{Q}$ we have $\mathcal{T}_t^G(\mathbb{Q})_{\text{tors}} = G$. Moreover, $\mathcal{T}_t^G$ does not have CM since $G \notin \Phi^{\text{CM}}(1)$. Since $\mathcal{T}_t^G$ has a rational point of order 3, Table 2 tells us that the image of the mod 3 Galois representation attached to $\mathcal{T}_t^G$ is labeled 3Cs.1.1 or 3B.1.1. The former case cannot happen since in that case $[\mathbb{Q}(\mathcal{T}_t^G[3]) : \mathbb{Q}] = 2$, but $(3,9), (3,12)$ are not subgroups of some group in $\Phi_{\mathbb{Q}}(2)$. For the case 3B.1.1 we have $[\mathbb{Q}(\mathcal{T}_t^G[3]) : \mathbb{Q}] = 6$. Therefore $K = \mathbb{Q}(\mathcal{T}_t^G[3])$ is a sextic field satisfying $(3,9)$ if $G = (9)$ (resp., $(3,12)$ if $G = (12)$) is a subgroup of $\mathcal{T}_t^G(K)$. But this happens for infinitely many values of t and since $(3,9)$ (resp., $(3,12)$) is a maximal subgroup in $\Phi^\infty(6)$ we have that, in fact, $\mathcal{T}_t^G(K)_{\text{tors}} = (3,9)$ (resp., $= (3,12)$).

Now, let $G = (9)$ and $K = \mathbb{Q}(\mathcal{T}_t^G[2])$. Then $(2,18)$ is a subgroup of $\mathcal{T}_t^G(K)$. We have that $[K : \mathbb{Q}] = 6$, since otherwise $(2,18)$ is a subgroup of some group in $\Phi_{\mathbb{Q}}(d)$ for d dividing 6. That is impossible. Analogous to the cases above, we have that in this case $\mathcal{T}_t^G(K)_{\text{tors}} = (2,18)$.

Finally the case $(6,6)$. Let the one-parameter family[3] be given by

$$\mathcal{A}_t : \ y^2 = x^3 - 3(a-1)^3(a-9)x - 2(a-1)^4(a^2 + 18a - 27), \qquad a = (t^3 - 1)^2, \ t \neq 0, 1.$$

This elliptic curve satisfies $\mathbb{Q}(\mathcal{A}_t[2]) = \mathbb{Q}(\mathcal{A}_t[3])$. In particular, the field $K = \mathbb{Q}(\mathcal{A}_t[6])$ is of degree 6. Then $(6,6)$ is a subgroup of $\mathcal{A}_t(K)$. An analogous argument to the above proves that $\mathcal{A}_t(K)_{\text{tors}} = (6,6)$.

Since the j-invariant of $\mathcal{T}_t^G$ and $\mathcal{A}_t$ is not constant, this proves that there are infinitely many non-$\overline{\mathbb{Q}}$-isomorphic elliptic curves over $\mathbb{Q}$ with torsion structures $H = (2,18), (3,9), (3,12),$ or $(6,6)$ over sextic fields. $\qquad\square$

---

[3]This family was computed by the first author and Álvaro Lozano-Robledo while working on the question of when can $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$. The family $\mathcal{A}_t$ is the 1-parameter family of elliptic curves with the property that $\mathbb{Q}(\mathcal{A}_t[2]) = \mathbb{Q}(\mathcal{A}_t[3])$ and both are sextic extensions of $\mathbb{Q}$.

4. Proof of Theorems 1 and 2

The results in Section 3 are exactly the results necessary to proof the main theorems of the paper.

Proof of Theorem 1. For $d = 2, 3$ we have that $\Phi_\mathbb{Q}(d) \subseteq \Phi_\mathbb{Q}(6)$ and $\Phi_\mathbb{Q}(d) \subseteq \Phi^\infty(6)$. Therefore $\Phi_\mathbb{Q}(2) \cup \Phi_\mathbb{Q}(3) \subseteq \Phi_\mathbb{Q}^\star(6)$. For $H \in \{(30), (2, 18), (3, 9), (3, 12), (6, 6)\}$ we have examples in Table 7 of an elliptic curve $E/\mathbb{Q}$, a sextic number field K such that $E(K)_{\mathrm{tors}} = H$. Now, by definition, $\Phi_\mathbb{Q}^\star(6) \subseteq \Phi^\infty(6)$, so our task to complete the description of $\Phi_\mathbb{Q}^\star(6)$ is to prove that the following torsion structures do not appear for elliptic curves over $\mathbb{Q}$ base change to any sextic number field:

$$(11), (17), (19), (20), (22), (24), (26), (27), (28), (2, 16), (2, 20), (4, 8).$$

Indeed,

- $H \neq (11), (17), (19), (22)$ by Proposition 6(a) and by Proposition 7(A).
- $H \neq (20)$ by Proposition 6(k).
- $H \neq (24)$ by Proposition 6(b), (d), (g), and (p).
- $H \neq (26)$ by Proposition 6(q) and by Proposition 7(A).
- $H \neq (27)$ by Proposition 6(r).
- $H \neq (28)$ by Proposition 6(s).
- $H \neq (2, 16), (4, 8)$ by Proposition 6(b).
- $H \neq (2, 20)$ by Proposition 6(b), (e), and (c).

This concludes the first part of Theorem 1, that is, the determination of $\Phi_\mathbb{Q}^\star(6)$. In particular we have obtained

$$(2) \qquad \Phi_\mathbb{Q}^\star(6) = \Phi_\mathbb{Q}(2) \cup \Phi_\mathbb{Q}(3) \cup \{(30), (2, 18), (3, 9), (3, 12), (6, 6)\}.$$

Now part (i) comes from Theorem 8 and (ii), (iii) from Theorem 9. It remains to determine $\Phi_\mathbb{Q}^\infty(6)$. Najman [34] has proved that $\Phi_\mathbb{Q}^\infty(2) = \Phi_\mathbb{Q}(2) \setminus \{(15)\}$ and $\Phi_\mathbb{Q}^\infty(3) = \Phi_\mathbb{Q}(3) \setminus \{(21)\}$. Then by (2) and (i)–(iii) we only need to prove that there are infinitely many non-$\overline{\mathbb{Q}}$-isomorphic classes of elliptic curves over $\mathbb{Q}$ such that, base change to sextic number field, the torsion grows to one of the groups in $\{(2, 18), (3, 9), (3, 12), (6, 6)\}$. This has been done in Theorem 10. $\square$

Proof of Theorem 2. The groups $H \in \Phi_\mathbb{Q}^\star(6)$ that do not appear in some $\Phi_\mathbb{Q}^\star(6, G)$ for any $G \in \Phi(1)$, with $G \subseteq H$, can be ruled out using Propositions 6 and 7. In Table 6, for each group G at the top of a column, we indicate what groups H (in each row) may appear, and indicate

- with (a)–(t), which part of Proposition 6 is used to prove that the pair (G, H) cannot appear in the non-CM case,
- with (A)–(E), which part of Proposition 7 is used to prove that the pair (G, H) cannot appear in the CM case,
- with $-$, if the case is ruled out because $G \nsubseteq H$,
- with a $\checkmark$, if the case is possible and, in fact, it occurs. There are a few types of check marks in Table 6:
    - $\checkmark$ (without a subindex) means[4] that $G = H$.

---

[4]Note that for any positive integer d, and any elliptic curve $E/\mathbb{Q}$ with $E(\mathbb{Q})_{\mathrm{tors}} = G$, there is always an extension $K/\mathbb{Q}$ of degree d such that $E(K)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$ (and, in fact, this is the case for almost all degree d extensions).

TABLE 6. The table displays either if the case happens for $G = H$ ($\checkmark$), if it already occurs over a quadratic field ($\checkmark_2$) or over a cubic field ($\checkmark_3$), if it occurs over a sextic but not a quadratic or cubic field ($\checkmark_6$), if it is impossible because $G \not\subseteq H$ ($-$) or if it is ruled out by Proposition 6 ((a)-(t)) and Proposition 7 ((A)-(E)).

H \ G	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(12)	(2,2)	(2,4)	(2,6)	(2,8)
(1)	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(2)	$\checkmark_3$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(3)	$\checkmark_{2,3}$	$-$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(4)	$\checkmark_3$	$\checkmark_2$	$-$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(5)	$\checkmark_2$	$-$	$-$	$-$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(6)	$\checkmark_3$	$\checkmark_{2,3}$	$\checkmark_3$	$-$	$-$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(7)	$\checkmark_{2,3}$	$-$	$-$	$-$	$-$	$-$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(8)	(b)	$\checkmark_2$	$-$	$\checkmark_2$	$-$	$-$	$-$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(9)	$\checkmark_2$	$-$	$\checkmark_3$	$-$	$-$	$-$	$-$	$-$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$
(10)	$\checkmark_6$	$\checkmark_2$	$-$	$-$	$\checkmark_3$	$-$	$-$	$-$	$-$	$\checkmark$	$-$	$-$	$-$	$-$	$-$
(11)	(a)	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(12)	$\checkmark_6$	$\checkmark_2$	$\checkmark_3$	$\checkmark_{2,3}$	$-$	$\checkmark_2$	$-$	$-$	$-$	$-$	$\checkmark$	$-$	$-$	$-$	$-$
(13)	$\checkmark_3$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(14)	$\checkmark_6$	$\checkmark_3$	$-$	$-$	$-$	$-$	$\checkmark_3$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(15)	$\checkmark_6$	$-$	$\checkmark_2$	$-$	$\checkmark_2$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(16)	(b)	$\checkmark_2$	$-$	(b)	$-$	$-$	$-$	$\checkmark_2$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(17)	(a)	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(18)	$\checkmark_6$	$\checkmark_6$	(l),(E)	$-$	$-$	$\checkmark_3$	$-$	$-$	$\checkmark_3$	$-$	$-$	$-$	$-$	$-$	$-$
(19)	(a)(A)	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(20)	(k)	(k)	$-$	(k)	(k)	$-$	$-$	$-$	$-$	(k)	$-$	$-$	$-$	$-$	$-$
(21)	$\checkmark_6$	$-$	$\checkmark_3$	$-$	$-$	$-$	(o)	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(22)	(a)	(a)	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(24)	(b)	(p)	(b)	(p)	$-$	(p)	$-$	(d)	$-$	$-$	(g)	$-$	$-$	$-$	$-$
(26)	(q),(A)	(q),(A)	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(27)	(r)	$-$	(r)	$-$	$-$	$-$	$-$	$-$	(r)	$-$	$-$	$-$	$-$	$-$	$-$
(28)	(s)	(s)	$-$	(s)	$-$	$-$	(s)	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(30)	(t)	(t)	$\checkmark_6$	$-$	$\checkmark_6$	(t)	$-$	$-$	$-$	(t)	$-$	$-$	$-$	$-$	$-$
(2,2)	$\checkmark_3$	$\checkmark_2$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$\checkmark$	$-$	$-$	$-$
(2,4)	(b),(B)	(b),(B)	$-$	$\checkmark_2$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$\checkmark_2$	$\checkmark$	$-$	$-$
(2,6)	$\checkmark_6$	$\checkmark_2$	$\checkmark_3$	$-$	$-$	$\checkmark_2$	$-$	$-$	$-$	$-$	$-$	$\checkmark_{2,3}$	$-$	$\checkmark$	$-$
(2,8)	(b)	(b)	$-$	$\checkmark_2$	$-$	$-$	$-$	$\checkmark_2$	$-$	$-$	$-$	$\checkmark_2$	$\checkmark_2$	$-$	$\checkmark$
(2,10)	$\checkmark_6$	$\checkmark_2$	$-$	$-$	$\checkmark_6$	$-$	$-$	$-$	$-$	$\checkmark_2$	$-$	(e)	$-$	$-$	$-$
(2,12)	(b)	(b)	(b)	$\checkmark_2$	$-$	(b)	$-$	$-$	$-$	$-$	$\checkmark_2$	$\checkmark_2$	(f)	$\checkmark_2$	$-$
(2,14)	$\checkmark_3$	$\checkmark_6$	$-$	$-$	$-$	$-$	$\checkmark_6$	$-$	$-$	$-$	$-$	(h),(C)	$-$	$-$	$-$
(2,16)	(b)	(b)	$-$	(b)	$-$	$-$	$-$	(b)	$-$	$-$	$-$	(b)	(b)	$-$	(b)
(2,18)	$\checkmark_6$	$\checkmark_6$	(n)	$-$	$-$	$\checkmark_6$	$-$	$-$	$\checkmark_6$	$-$	$-$	(m)	$-$	(m)	$-$
(2,20)	(b)	(b)	$-$	(c)	(b)	$-$	$-$	$-$	$-$	(b)	$-$	(e)	(c)	$-$	$-$
(3,3)	$\checkmark_6$	$-$	$\checkmark_2$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(3,6)	(i),(D)	$\checkmark_6$	$\checkmark_6$	$-$	$-$	$\checkmark_2$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
(3,9)	$\checkmark_6$	$-$	$\checkmark_6$	$-$	$-$	$-$	$-$	$-$	$\checkmark_6$	$-$	$-$	$-$	$-$	$-$	$-$
(3,12)	(i)	$\checkmark_6$	(j)	$\checkmark_6$	$-$	$\checkmark_6$	$-$	$-$	$-$	$-$	$\checkmark_6$	$-$	$-$	$-$	$-$
(4,4)	$\checkmark_6$	(b)	$-$	$\checkmark_2$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	(b)	$\checkmark_2$	$-$	$-$
(4,8)	(b)	(b)	$-$	(b)	$-$	$-$	$-$	(b)	$-$	$-$	$-$	(b)	(b)	$-$	(b)
(6,6)	$\checkmark_6$	$\checkmark_6$	$\checkmark_6$	$-$	$-$	$\checkmark_6$	$-$	$-$	$-$	$-$	$-$	$\checkmark_6$	$-$	$\checkmark_6$	$-$

　　　$-$　$\checkmark_d$ for $d = 2$ or 3 means that the structure H occurs already over a quadratic[5] or cubic[6] field, respectively. $\checkmark_{2,3}$ means that both cases appear (not necessarily for a single elliptic curve).

[5]Examples can be found in Table 2 of [16].
[6]Examples can be found in Table 1 of [15].

– $\sqrt{6}$ means that H can be achieved over a sextic field but not over an intermediate quadratic or cubic field, and we have collected examples of curves and sextic fields in Table 7. □

5. Sporadic torsion over sextic fields

Let d be a positive integer and H a finite abelian group. We say that H is a sporadic torsion group for degree d if there is a number field K of degree d and an elliptic curve E/K such that $H = E(K)_{\text{tors}}$ satisfying $H \notin \Phi^{\infty}(d)$. Notice that these elliptic curves are in bijection to its j-invariants in $J(d)$. To our knowledge only a few examples of sporadic torsion groups are known. Excluding Najman's elliptic curve mentioned in the introduction with $H = (21)$ and $d = 3$, the known examples have been found by van Hoeij [18]:

- $d = 5$: $H = (28), (30)$,
- $d = 6$: $H = (25), (37)$.

Interestingly, all of these cases correspond to cyclic groups. In this paper we have dealt with the problem of characterizing $\Phi^{\star}_{\mathbb{Q}}(6) = \Phi_{\mathbb{Q}}(6) \cap \Phi^{\infty}(6)$ and it is easy to check that the two examples that van Hoeij found for $d = 6$, namely (25) and (37), are not subgroups of any group in $\Phi_{\mathbb{Q}}(6)$; the former case because by Table 2 in order to gain a point P_5 of order 5 in a sextic field we have $[\mathbb{Q}(P_5) : \mathbb{Q}] = 1, 2$. Now if P_{25} is a point of order 25 such that $5P_{25} = P_5$, then by [13, Proposition 4.6] we have $[\mathbb{Q}(P_{25}) : \mathbb{Q}(P_5)]$ divides 25 or 20. Looking at $\Phi_{\mathbb{Q}}(d)$ for $d = 2$ and 3 we show that the case (25) is not possible. The last case can be eliminated by simply noticing that $37 \notin R_{\mathbb{Q}}(6)$.

On the other hand, in [14] the second author and Najman give two examples of elliptic curves over $\mathbb{Q}$ and a number field K of degree 6 over $\mathbb{Q}$ such that $E(K)_{\text{tors}} = (4, 12)$ and thus showing that $(4, 12) \in \Phi_{\mathbb{Q}}(6)$. In particular this is the first known example of a sporadic non-cyclic torsion group (over degree 6). See Remark 1 for more information about this sporadic torsion.

6. Computations

Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a number field. We say that the torsion of E grows from $\mathbb{Q}$ to K if $E(\mathbb{Q})_{\text{tors}} \subsetneq E(K)_{\text{tors}}$. Note that if the torsion of E grows from $\mathbb{Q}$ to K, then of course the torsion of E also grows from $\mathbb{Q}$ to any extension of K. We say that the torsion growth from $\mathbb{Q}$ to K is primitive if $E(K')_{\text{tors}} \subsetneq E(K)_{\text{tors}}$ for any subfield $K' \subsetneq K$. With this definition it is possible to give a more detailed description of how the torsion grows in extensions of $\mathbb{Q}$. Given an elliptic curve $E/\mathbb{Q}$ and a positive integer d, we denote by $\mathcal{H}_{\mathbb{Q}}(d, E)$ the set of pairs (H, K) (up to isomorphisms) where $K/\mathbb{Q}$ is an extension of degree dividing d, $H = E(K)_{\text{tors}} \neq E(\mathbb{Q})_{\text{tors}}$, and the torsion growth in K is primitive. Note that we are allowing the possibility of two (or more) of the torsion subgroups H being isomorphic if the corresponding number fields K are not isomorphic. We call the set $\mathcal{H}_{\mathbb{Q}}(d, E)$ the set of torsion configurations of the elliptic curve $E/\mathbb{Q}$. We let $\mathcal{H}_{\mathbb{Q}}(d)$ denote the set of $\mathcal{H}_{\mathbb{Q}}(d, E)$ as $E/\mathbb{Q}$ runs over all elliptic curves. Finally, for any $G \in \Phi(1)$ we define $\mathcal{H}_{\mathbb{Q}}(d, G)$ as the set of sets $\mathcal{H}_{\mathbb{Q}}(d, E)$ where $E/\mathbb{Q}$ runs over all the elliptic curves such that $E(\mathbb{Q})_{\text{tors}} = G$.

Note that if we denote the maximum of the cardinality of the sets S when $S \in \mathcal{H}_{\mathbb{Q}}(d)$ by $h_{\mathbb{Q}}(d)$, then $h_{\mathbb{Q}}(d)$ gives the maximum number of primitive degree d extensions that can appear.

The sets $\mathcal{H}_{\mathbb{Q}}(d)$ and $\mathcal{H}_{\mathbb{Q}}(d, G)$ for any $G \in \Phi(1)$ have been completely determined for $d = 2$ in [17], for $d = 3$ in [15], for $d = 5$ in [10], for $d = 7$, and for any d not divisible by a prime less than 11 in [13]. For the case $d = 4$, in order to conjecture what $\mathcal{H}_{\mathbb{Q}}(4)$ may be, $\mathcal{H}_{\mathbb{Q}}(4, E)$ has been computed for all elliptic curves over $\mathbb{Q}$ with conductor less than 350000. In fact,[7] this computation has been enlarged to include elliptic curves with conductor up to 400000.

In the same vein as the quartic computations we have carried out similar computations for the case when $d = 6$. Table 8 gives all[8] the torsion configurations over sextic fields that we have found. We found 137 torsion configurations in total and note all of the found configurations occur for an elliptic curve with conductor less than or equal to 10816, far from 400000.

The following table shows what is known about $h_{\mathbb{Q}}(d)$:

d	2	3	4	5	6	7	$2, 3, 5, 7 \nmid d$
$h_{\mathbb{Q}}(d)$	4	3	≥ 9	1	≥ 9	1	0

APPENDIX: IMAGES OF MOD p GALOIS REPRESENTATIONS ASSOCIATED TO ELLIPTIC CURVES OVER $\mathbb{Q}$

For each possible subgroup $G_E(p) \subseteq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for $p \in R_{\mathbb{Q}}(6) = \{2, 3, 5, 7, 13\}$, Table 2 lists in the first and second column the corresponding labels in Sutherland and Zywina notation, and the following data:

d_0: the index of the largest subgroup of $G_E(p)$ that fixes a $\mathbb{Z}/p\mathbb{Z}$-submodule of rank 1 of $E[p]$; equivalently, the degree of the minimal extension $L/\mathbb{Q}$ over which E admits a p-isogeny defined over L.

d_v: the index of the stabilizers of $v \in (\mathbb{Z}/p\mathbb{Z})^2$, $v \neq (0, 0)$, by the action of $G_E(p)$ on $(\mathbb{Z}/p\mathbb{Z})^2$; equivalently, the degrees of the extension $L/\mathbb{Q}$ over which E has a L-rational point of order p.

d: the order of $G_E(p)$; equivalently, the degree of the minimal extension $L/\mathbb{Q}$ for which $E[p] \subseteq E(L)$.

Note that Table 2 is partially extracted from Table 3 of [39]. The difference is that [39, Table 3] only lists the minimum of d_v, which is denoted by d_1 therein.

---

[7]Filip Najman and the second author have developed [14] a (fast) algorithm that takes as input an elliptic curve defined over $\mathbb{Q}$ and an integer d and returns the torsion configurations of degree d for E, that is, $\mathcal{H}_{\mathbb{Q}}(d, E)$. At this moment the algorithm has been run on all elliptic curves in Cremona's database and the torsion growth appears in the LMFDB webpage [29] until degree 7.

[8]Including the elliptic curves 162d1 and 1296h1 that give sporadic torsion $(4, 12)$ over sextic fields (see Section 5).

TABLE 7. Examples of elliptic curves such that $G \in \Phi(1)$ and $H \in \Phi_{\mathbb{Q}}(6, G)$ but $H \notin \Phi_{\mathbb{Q}}(d, G)$, $d = 2, 3$.

G	H	Sextic K	Label of $E/\mathbb{Q}$
(1)	(10)	$x^6 + 2x^5 + 2x - 1$	50a4
	(12)	$x^6 - 3x^4 + 2x^3 + 9x^2 - 12x + 4$	162a2
	(14)	$x^6 + 2x^5 + 8x^4 + 8x^3 + 14x^2 + 4x + 4$	208d1
	(15)	$x^6 - 5$	50a4
	(18)	$x^6 - 3x^5 + 3x^3 + 6x^2 - 9x + 3$	54a2
	(21)	$x^6 + x^3 + 1$	162b2
	(2, 6)	$x^6 - 3x^5 + 5x^3 - 3x + 1$	27a2
	(2, 10)	$x^6 - x^5 + 2x^4 - 3x^3 + 2x^2 - x + 1$	121d1
	(2, 18)	$x^6 - 3x^2 + 6$	1728e3
	(3, 3)	$x^6 + 3x^5 + 4x^4 + 3x^3 - 5x^2 - 6x + 12$	19a2
	(3, 9)	$x^6 + 3$	54a2
	(4, 4)	$x^6 - 2x^3 + 9x^2 + 6x + 2$	162d2
	(4, 12)	$x^6 + 2x^3 + 9x^2 - 6x + 2$	1296h1
	(6, 6)	$x^6 + 3x^5 - 5x^3 + 3x + 1$	108a2
(2)	(18)	$x^6 + 4x^3 + 7$	14a3
	(2, 14)	$x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$	49a1
	(2, 18)	$x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$	98a1
	(3, 6)	$x^6 + 3x^5 - 3x^4 - 4x^3 + 69x^2 + 201x + 181$	14a3
	(3, 12)	$x^6 + 3$	30a3
	(6, 6)	$x^6 + 3x^5 - 5x^3 + 3x + 1$	36a3
(3)	(30)	$x^6 - 2x^5 - 2x - 1$	50a3
	(3, 6)	$x^6 + x^5 + 8x^4 + 5x^3 + 10x^2 + 3x + 3$	19a1
	(3, 9)	$x^6 - x^3 + 1$	27a1
	(4, 12)	$x^6 + 9x^4 - 12x^2 + 4$	162d1
	(6, 6)	$x^6 - 3x^5 + 6x^4 - 9x^3 + 12x^2 - 9x + 3$	27a1
(4)	(3, 12)	$x^6 - 3x^5 + 4x^4 - 3x^3 - 2x^2 + 3x + 3$	90c1
(5)	(30)	$x^6 - 2x^5 - 2x - 1$	50b1
	(2, 10)	$x^6 + x^5 + 2x^4 + 3x^3 + 2x^2 + x + 1$	11a1
(6)	(2, 18)	$x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$	14a4
	(3, 12)	$x^6 - 3x^5 + 4x^4 - 3x^3 - 2x^2 + 3x + 3$	30a1
	(6, 6)	$x^6 - 3x^5 + 6x^4 - 9x^3 + 12x^2 - 9x + 3$	36a1
(7)	(2, 14)	$x^6 - 2x^5 + 5x^4 + 4x^3 + 22x^2 + 16x + 16$	26b1
(9)	(2, 18)	$x^6 - 3x^2 + 6$	54b3
	(3, 9)	$x^6 + 3$	54b3
(12)	(3, 12)	$x^6 + 3$	90c3
(2, 2)	(6, 6)	$x^6 + 3$	30a6
(2, 6)	(6, 6)	$x^6 + 3x^5 + 4x^4 + 3x^3 - 2x^2 - 3x + 3$	30a2

TABLE 8. Torsion configurations over sextic fields.

G	$\mathcal{H}_{\mathbb{Q}}(6, E)$	Label
	$(2, 2)$	392b1
	$(2, 14)$	1922c1
	$(2), (2, 2)$	11a2
	$(2, 2), (2, 14)$	1922e1
	$(4), (4, 4)$	648a1
	$(7), (2, 2)$	1922c2
	$(2), (5), (2, 10)$	121d1
	$(2), (7), (2, 2)$	26b2
	$(2), (7), (2, 14)$	10816bk1
	$(2), (13), (2, 2)$	147c1
	$(3), (6), (6, 6)$	108a2
	$(4), (7), (4, 4)$	338b1
	$(2), (3)^2, (2, 6)$	484a1
	$(2), (3), (9), (2, 18)$	1728e3
	$(2), (4)^2, (2, 2)$	648c1
	$(2), (5), (10), (2, 2)$	75a2
	$(2), (7), (14), (2, 2)$	208d1
	$(3)^2, (2, 2), (2, 6)$	196a1
	$(3)^2, (4), (4, 12)$	1296h1
	$(2), (3)^2, (2, 6), (3, 3)$	225b2
	$(2), (3)^2, (6), (2, 2)$	50b3
	$(2), (3)^2, (6), (2, 6)$	361b2
	$(2), (3)^2, (7), (2, 6)$	5184bd1
	$(2), (3)^2, (9), (2, 6)$	361b1
	$(2), (3)^2, (21), (2, 6)$	5184u1
	$(2), (3), (6)^2, (2, 2)$	300a1
(1)	$(2), (3), (9), (18), (2, 2)$	432e3
	$(2), (4)^2, (7), (2, 2)$	338a1
	$(3)^2, (2, 2), (2, 6), (3, 3)$	196b2
	$(3)^2, (4), (12), (4, 4)$	1296h2
	$(2), (3)^2, (4)^2, (2, 6)$	1296j1
	$(2), (3)^2, (4), (12), (2, 2)$	1296j2
	$(2), (3)^2, (5), (6), (2, 10)$	1600q1
	$(2), (3)^2, (5), (10), (2, 6)$	1600v3
	$(2), (3)^2, (6), (2, 2), (3, 3)$	44a2
	$(2), (3)^2, (6), (2, 2), (3, 9)$	486c2
	$(2), (3)^2, (6)^2, (2, 2)$	175b2
	$(2), (3)^2, (6), (7), (2, 2)$	1296e2
	$(2), (3)^2, (6), (9), (2, 2)$	175b1
	$(2), (3)^2, (6), (9), (2, 6)$	1728e2
	$(2), (3)^2, (6), (21), (2, 2)$	1296e1
	$(2), (3), (9), (18), (2, 2), (3, 9)$	54a2
	$(3)^2, (4), (12), (3, 3), (4, 4)$	162d2
	$(2), (3)^2, (4)^2, (6), (2, 2)$	4050g2
	$(2), (3)^2, (4), (12), (2, 2), (3, 3)$	162a2
	$(2), (3)^2, (5), (6), (10), (2, 2)$	400b1
	$(2), (3)^2, (6)^2, (9), (2, 2)$	432a1
	$(2), (3)^2, (6), (7), (2, 2), (3, 3)$	162b4
	$(2), (3)^2, (6), (7), (21), (2, 2)$	7938u3
	$(2), (3)^2, (6), (21), (2, 2), (3, 3)$	162c2
	$(2), (3)^2, (9)^2, (2, 6), (3, 3)$	27a2
	$(2), (3)^2, (6), (7), (21), (2, 2), (3, 3)$	162b2
	$(2), (3)^2, (6), (9)^2, (2, 2), (3, 3)$	19a2
	$(2), (3)^2, (5), (6), (10), (15), (2, 2), (3, 3)$	50a4

G	$\mathcal{H}_{\mathbb{Q}}(6, E)$	Label
(2)	$(2, 2)$	46a1
	$(2, 10)$	450a3
	$(2, 2), (2, 14)$	49a1
	$(6), (2, 6)$	80b1
	$(10), (2, 2)$	150b3
	$(14), (2, 2)$	49a2
	$(4)^2, (2, 2)$	15a5
	$(4), (8), (2, 2)$	24a6
	$(4), (16), (2, 2)$	3150bk1
	$(6), (2, 2), (2, 6)$	80b3
	$(6), (2, 6), (2, 18)$	98a1
	$(6), (2, 6), (6, 6)$	36a3
	$(6)^2, (2, 2)$	80b2
	$(8)^2, (2, 2)$	2880bd6
	$(14), (2, 2), (2, 14)$	49a3
	$(4)^2, (6), (2, 6)$	960o7
	$(4)^2, (12), (2, 6)$	450g1
	$(4), (6), (12), (2, 2)$	240b3
	$(4), (12), (2, 2), (2, 6)$	450g3
	$(6)^2, (18), (2, 2)$	98a2
	$(6), (18), (2, 2), (2, 6)$	98a5
	$(4)^2, (6), (2, 2), (2, 6)$	960o4
	$(4)^2, (6)^2, (2, 2)$	150c4
	$(4)^2, (6), (12), (2, 2)$	240b1
	$(6)^2, (2, 2), (2, 6), (3, 6)$	20a3
	$(4), (6), (12)^2, (2, 2), (2, 6), (3, 12)$	30a3
	$(6)^2, (18)^2, (2, 2), (2, 6), (3, 6)$	14a3
	$(4)^2, (6)^2, (12)^2, (2, 2), (2, 6), (3, 6)$	30a7
(3)	$(2, 6), (3, 3)$	196b1
	$(6), (6, 6)$	108a1
	$(6), (2, 6), (3, 3)$	44a1
	$(12), (3, 3), (4, 12)$	162d1
	$(6), (2, 6), (3, 3), (3, 6)$	19a1
	$(6), (3, 3), (3, 9), (6, 6)$	27a1
	$(6), (9), (2, 6), (3, 9)$	486f1
	$(6), (21), (2, 6), (3, 3)$	162b1
	$(6), (2, 6), (3, 3), (3, 6), (3, 9)$	54a1
	$(6), (9), (3, 3), (3, 9), (6, 6)$	27a3
	$(6), (9)^2, (2, 6), (3, 3)$	19a3
	$(6), (12)^2, (2, 6), (3, 3)$	162a1
	$(6), (15), (30), (2, 6), (3, 3)$	50a3
	$(6), (9), (2, 6), (3, 3), (3, 6), (3, 9)$	54b1

G	$\mathcal{H}_{\mathbb{Q}}(6, E)$	Label
(4)	$(2, 4)$	17a1
	$(2, 8)$	192c6
	$(4, 4)$	40a4
	$(12), (2, 12)$	150c3
	$(8)^2, (2, 4)$	15a7
	$(8)^2, (2, 8)$	240d6
	$(12), (2, 4), (2, 12)$	150c1
	$(12)^2, (2, 4)$	720j5
	$(12)^2, (2, 4), (2, 12), (3, 12)$	90c1
(5)	$(10), (2, 10)$	11a1
	$(10), (15)^2, (30), (2, 10)$	50b1
(6)	$(2, 6), (3, 6)$	14a1
	$(2, 6), (6, 6)$	36a1
	$(12)^2, (2, 6), (3, 6)$	30a4
	$(12)^2, (2, 6), (3, 12)$	30a1
	$(18)^2, (2, 6), (2, 18), (3, 6)$	14a4
(7)	$(14), (2, 14)$	26b1
(8)	$(2, 8)$	15a4
	$(16)^2, (2, 8)$	210e1
(9)	$(18), (2, 18), (3, 9)$	54b3
(10)	$(2, 10)$	66c1
(12)	$(2, 12), (3, 12)$	90c3
(2, 2)	$(2, 4)$	33a1
	$(2, 8)$	63a2
	$(2, 4)^2$	17a2
	$(2, 4), (2, 8)$	75b3
	$(2, 6)^2$	240b2
	$(2, 6), (2, 12)$	960o6
	$(2, 4)^3$	15a2
	$(2, 4)^2, (2, 8)$	510e5
	$(2, 4), (2, 6)^2$	150c2
	$(2, 4), (2, 6), (2, 12)$	960o2
	$(2, 6)^2, (6, 6)$	30a6
	$(2, 4), (2, 6)^2, (2, 12), (6, 6)$	90c2
(2, 4)	$(2, 8)$	15a3
	$(4, 4)$	195a3
	$(2, 8)^2$	1230f2
	$(2, 8), (4, 4)$	15a1
	$(2, 8)^2, (4, 4)$	210e3
(2, 6)	$(6, 6)$	30a2
	$(2, 12), (6, 6)$	90c6

References

[1] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, *Explicit Chabauty–Kim for the split Cartan modular curve of level 13*, arXiv:1711.05846, (2017). To appear in Ann. of Math.

[2] W. Bosma, J. Cannon, C. Fieker, and A. Steel (eds.), *Handbook of Magma functions, Edition 2.23*, http://magma.maths.usyd.edu.au/magma, 2018.

[3] M. Chou, *Torsion of rational elliptic curves over quartic Galois number fields*, J. Number Theory **160** (2016), 603–628, DOI 10.1016/j.jnt.2015.09.013. MR3425225

[4] P. L. Clark, P. Corn, A. Rice, and J. Stankewicz, *Computation on elliptic curves with complex multiplication*, LMS J. Comput. Math. **17** (2014), no. 1, 509–535, DOI 10.1112/S1461157014000072. MR3356044

[5] J. E. Cremona, *ecdata: 2016-10-17 (Elliptic curve data for conductors up to 400.000)*, available on http://johncremona.github.io/ecdata/.

[6] H. B. Daniels and E. González-Jiménez, Magma scripts related to *On the torsion of rational elliptic curves over sextic fields*, available at http://matematicas.uam.es/~enrique.gonzalez.jimenez/.

[7] 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** (2018), no. 309, 425–458, DOI 10.1090/mcom/3213. MR3716201

[8] M. Derickx and A. V. Sutherland, *Torsion subgroups of elliptic curves over quintic and sextic number fields*, Proc. Amer. Math. Soc. **145** (2017), no. 10, 4233–4245, DOI 10.1090/proc/13605. MR3690609

[9] G. W. Fung, H. Ströher, H. C. Williams, and H. G. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over pure cubic fields*, J. Number Theory **36** (1990), no. 1, 12–45, DOI 10.1016/0022-314X(90)90003-A. MR1068671

[10] E. González-Jiménez, *Complete classification of the torsion structures of rational elliptic curves over quintic number fields*, J. Algebra **478** (2017), 484–505, DOI 10.1016/j.jalgebra.2017.01.012. MR3621686

[11] E. González-Jiménez and Á. Lozano-Robledo, *On the minimal degree of definition of p-primary torsion subgroups of elliptic curves*, Math. Res. Lett. **24** (2017), no. 4, 1067–1096, DOI 10.4310/MRL.2017.v24.n4.a7. MR3723804

[12] E. González-Jiménez and Á. Lozano-Robledo, *On the torsion of rational elliptic curves over quartic fields*, Math. Comp. **87** (2018), no. 311, 1457–1478, DOI 10.1090/mcom/3235. MR3766394

[13] E. González-Jiménez and F. Najman, *Growth of torsion groups of elliptic curves upon base change*, arXiv:1609.02515, (2016).

[14] E. González-Jiménez and F. Najman, *An algorithm for determining torsion growth of elliptic curves*, arXiv:1904.07071, (2019).

[15] E. González-Jiménez, F. Najman, and J. M. Tornero, *Torsion of rational elliptic curves over cubic fields*, Rocky Mountain J. Math. **46** (2016), no. 6, 1899–1917, DOI 10.1216/RMJ-2016-46-6-1899. MR3591265

[16] E. González-Jiménez and J. M. Tornero, *Torsion of rational elliptic curves over quadratic fields*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM **108** (2014), no. 2, 923–934, DOI 10.1007/s13398-013-0152-4. MR3249985

[17] E. González-Jiménez and J. M. Tornero, *Torsion of rational elliptic curves over quadratic fields II*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM **110** (2016), no. 1, 121–143, DOI 10.1007/s13398-015-0223-9. MR3462078

[18] M. van Hoeij, *Low degree places on the modular curve $X_1(N)$*, arXiv:1202.4355 (data file available at https://www.math.fsu.edu/~hoeij/files/X1N/LowDegreePlaces).

[19] D. Jeon, C. H. Kim, and Y. Lee, *Infinite families of elliptic curves over dihedral quartic number fields*, J. Number Theory **133** (2013), no. 1, 115–122, DOI 10.1016/j.jnt.2012.06.014. MR2981403

[20] D. Jeon, C. H. Kim, and A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), no. 3, 291–301, DOI 10.4064/aa113-3-6. MR2069117

[21] D. Jeon, C. H. Kim, and E. Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), no. 1, 1–12, DOI 10.1112/S0024610706022940. MR2254548

[22] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229, DOI 10.1007/BF01232025. MR1172689

[23] M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), no. 1, 21–23, DOI 10.1017/S0305004100055444. MR510395

[24] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), no. 1, 15–20, DOI 10.1017/S0305004100056462. MR549292

[25] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), no. 2, 239–244, DOI 10.1112/jlms/s2-22.2.239. MR588271

[26] M. A. Kenku, *On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) **23** (1981), no. 3, 415–427, DOI 10.1112/jlms/s2-23.3.415. MR616546

[27] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149, DOI 10.1017/S0027763000002816. MR931956

[28] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237, DOI 10.1112/plms/s3-33.2.193. MR0434947

[29] LMFDB Collaboration, *The L-functions and modular forms database*, available at `http://www.lmfdb.org`.

[30] Á. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), no. 1, 279–305, DOI 10.1007/s00208-013-0906-5. MR3084348

[31] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162, DOI 10.1007/BF01390348. MR482230

[32] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres* (French), Invent. Math. **124** (1996), no. 1-3, 437–449, DOI 10.1007/s002220050059. MR1369424

[33] H. H. Müller, H. Ströher, and H. G. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over quadratic fields*, J. Reine Angew. Math. **397** (1989), 100–161. MR993219

[34] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Lett. **23** (2016), no. 1, 245–272, DOI 10.4310/MRL.2016.v23.n1.a12. MR3512885

[35] L. D. Olson, *Points of finite order on elliptic curves with complex multiplication*, Manuscripta Math. **14** (1974), 195–205, DOI 10.1007/BF01171442. MR0352104

[36] A. Pethö, T. Weis, and H. G. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over general cubic number fields*, Internat. J. Algebra Comput. **7** (1997), no. 3, 353–413, DOI 10.1142/S0218196797000174. MR1448331

[37] J. Rouse and D. Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Res. Number Theory **1** (2015), Art. 12, 34, DOI 10.1007/s40993-015-0013-7. MR3500996

[38] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368

[39] A. V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), e4, 79, DOI 10.1017/fms.2015.33. MR3482279

[40] D. Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, arXiv:1508.07660, (2015).

DEPARTMENT OF MATHEMATICS AND STATISTICS, AMHERST COLLEGE, MASSACHUSETTS 01002
Email address: `hdaniels@amherst.edu`

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD AUTÓNOMA DE MADRID, MADRID, SPAIN
Email address: `enrique.gonzalez.jimenez@uam.es`