TORSION SUBGROUPS OF RATIONAL ELLIPTIC CURVES OVER THE COMPOSITUM OF ALL D_4 EXTENSIONS OF THE RATIONAL NUMBERS

HARRIS B. DANIELS

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve and let $\mathbb{Q}(D_4^\infty)$ be the compositum of all extensions of $\mathbb{Q}$ whose Galois closure has Galois group isomorphic to a quotient of a subdirect product of a finite number of transitive subgroups of D_4. In this article we first show that $\mathbb{Q}(D_4^\infty)$ is in fact the compositum of all D_4 extensions of $\mathbb{Q}$ and then we prove that the torsion subgroup of $E(\mathbb{Q}(D_4^\infty))$ is finite and determine the 24 possibilities for its structure. We also give a complete classification of the elliptic curves that have each possible torsion structure in terms of their j-invariants.

1. INTRODUCTION

A fundamental theorem in arithmetic geometry known as the Mordell–Weil theorem says that the rational points on an elliptic curve defined over a number field can be given the algebraic structure of a finitely generated abelian group. More specifically, if K is a number field and E/K is an elliptic curve then the set of K-rational points $E(K)$ is isomorphic to a group of the form $\mathbb{Z}^r \oplus E(K)_{\text{tors}}$ where r is a nonnegative integer and $E(K)_{\text{tors}}$ is a finite abelian group called the *torsion subgroup of E over K*. In fact, as long as the base field K is a number field, the torsion subgroup of an elliptic curve is always isomorphic to a group of the form $\mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/ab\mathbb{Z}$ for some positive integers a and b. Merel, in [29] proved the existence of a uniform bound on the size of $E(K)_{\text{tors}}$ that depends only on the degree of the extension $K/\mathbb{Q}$. In light of this result it is natural to ask the following question.

Question 1.1. For a fixed $d \geq 1$, what groups (up to isomorphism) arise as the torsion subgroup of an elliptic curve over a number field of degree d?

The following theorems give a complete answer to Question 1.1 when $d = 1$ and 2.

Theorem 1.2 (Mazur [27])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & 1 \leq M \leq 10 \text{ or } M = 12, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & 1 \leq M \leq 4. \end{cases}$$

Theorem 1.3 (Kenku, Momose [20], Kamienny [14])**.** *Let E/F be an elliptic curve over a quadratic number field F. Then*

$$E(F)_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 16 \text{ or } M = 18, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 6, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \text{with } M = 1 \text{ or } 2, \text{ only if } F = \mathbb{Q}(\sqrt{-3}), \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \text{only if } F = \mathbb{Q}(\sqrt{-1}). \end{cases}$$

2010 *Mathematics Subject Classification.* Primary: 11G05, Secondary: 11R21, 12F10, 14H52.
Key words and phrases. Elliptic Curve, Torsion Points, Galois Theory.

Recently, Etropolski, Morrow, and Zureick-Brown, (and independently Derickx) announced that they have found a complete classification of the torsion structures that occur for elliptic curves over cubic fields, giving an answer to Question 1.1 in the case when $d = 3$. This answer comes after the work of Jeon, Kim, Lee, and Schweizer [12, 13] classifing all of the torsion structures of elliptic curves defined over cubic fields that occur infinitely often.

One way to simplify Question 1.1 is to restrict to the torsion subgroups of elliptic curves defined over $\mathbb{Q}$ that have been base-extended to degree d number fields. There are many results related to this question and below we present a few of them.

Theorem 1.4. [25, Thm. 2] *Let $E/\mathbb{Q}$ be an elliptic curve and let F be a quadratic number field. Then*

$$E(F)_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \text{ or } M = 12, 15, 16, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 6, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \text{with } 1 \leq M \leq 2 \text{ and } F = \mathbb{Q}(\sqrt{-3}), \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \text{with } F = \mathbb{Q}(\sqrt{-1}). \end{cases}$$

Theorem 1.5. [25, Thm. 1] *Let $E/\mathbb{Q}$ be an elliptic curve and let F be a cubic number field. Then*

$$E(F)_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \text{ or } M = 12, 13, 14, 18, 21, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 4 \text{ or } M = 7. \end{cases}$$

Moreover, the elliptic curve $162B1$ over $\mathbb{Q}(\zeta_9)^+$ is the unique rational elliptic curve over a cubic field with torsion subgroup isomorphic to $\mathbb{Z}/21\mathbb{Z}$. For all other groups T listed above there are infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$ for which $E(F) \simeq T$ for some cubic field F.

Another variant of this question would be to consider what torsion structures occur when base-extending an elliptic curve $E/\mathbb{Q}$ to some fixed *infinite* extension. Of course, since infinite extensions are not number fields the Mordell–Weil theorem does not immediately give us that the torsion subgroup an elliptic curve base-extended to an infinite extension is finite. Because of this we will need to carefully choose our infinite extensions so this question still has some content.

Definition 1.6. *For each fixed integer $d \geq 1$, let $\mathbb{Q}(d^\infty)$ denote the compositum of all field extensions $F/\mathbb{Q}$ of degree d. More precisely, let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$, and define*

$$\mathbb{Q}(d^\infty) := \mathbb{Q}\left(\{\beta \in \overline{\mathbb{Q}} : [\mathbb{Q}(\beta) : \mathbb{Q}] = d\}\right).$$

The fields defined in Definition 1.6 have been studied on their own by Gal and Grizzard [10], and the torsion structures of the rational elliptic curves base-extended to $\mathbb{Q}(2^\infty)$ and $\mathbb{Q}(3^\infty)$ are fully classified.

Theorem 1.7 (Laska, Lorenz [21], Fujita [8, 9])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. The torsion subgroup $E(\mathbb{Q}(2^\infty))_{\text{tors}}$ is finite, and*

$$E(\mathbb{Q}(2^\infty))_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } M \in 1, 3, 5, 7, 9, 15, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 6 \text{ or } M = 8, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \text{or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4M\mathbb{Z} & \text{with } 1 \leq M \leq 4, \text{ or} \\ \mathbb{Z}/2M\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 3 \leq M \leq 4. \end{cases}$$

Theorem 1.8 (D., Lozano-Robledo, Najman, Sutherland [7])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. The torsion subgroup $E(\mathbb{Q}(3^\infty))_{\text{tors}}$ is finite, and*

$$E(\mathbb{Q}(3^\infty))_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } M = 1, 2, 4, 5, 7, 8, 13, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4M\mathbb{Z} & \text{with } M = 1, 2, 4, 7, \text{ or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6M\mathbb{Z} & \text{with } M = 1, 2, 3, 5, 7, \text{ or} \\ \mathbb{Z}/2M\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } M = 4, 6, 7, 9. \end{cases}$$

All but 4 of the torsion subgroups T listed above occur for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$; for $T = \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/28\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/42\mathbb{Z}$, and $\mathbb{Z}/14\mathbb{Z}\times\mathbb{Z}/14\mathbb{Z}$ there are only 2, 2, 4, and 1 (respectively) $\overline{\mathbb{Q}}$-isomorphism classes of $E/\mathbb{Q}$ for which $E(\mathbb{Q}(3^\infty))_{\text{tors}} \simeq T$.

In their article [10], Gal and Grizzard prove a more general version of the following proposition.

Proposition 1.9. [10, Theorem 9] *Let $K/\mathbb{Q}$ be a finite extension. Then $K \subseteq \mathbb{Q}(d^\infty)$ if and only if the following two conditions are met.*

1. *There exists a group H which is a subdirect product of transitive subgroups of degree d with some normal subgroup N such that*
$$1 \to N \to H \to \text{Gal}(K/\mathbb{Q}) \to 1$$
is a short exact sequence.
2. *We can solve the corresponding Galois embedding problem, i.e. we can find a field $L \supseteq K$ such that $\text{Gal}(L/\mathbb{Q}) \simeq H$.*

This proposition gives a concrete way to check is a given finite extension is contained inside of $\mathbb{Q}(d^\infty)$ explicitly. Motivated by part (1) of this proposition we give the following definition which allows us to define some related fields.

Definition 1.10. *Let G be a transitive subgroup of S_d for some $d \geq 2$. We say that a finite group H is of **generalized G-type** if it is isomorphic to a quotient of a subdirect product of transitive subgroups of G. Given a number field $K/\mathbb{Q}$ and its Galois closure $\widehat{K}$, we say that $K/\mathbb{Q}$ is of **generalized G-type** if $\text{Gal}(\widehat{K}/\mathbb{Q})$ is a group of generalized G-type. Let $\mathbb{Q}(G^\infty)$ be the compositum of all fields that are of generalized G-type.*

While in general it is not necessarily true that $\mathbb{Q}(S_d^\infty) = \mathbb{Q}(d^\infty)$ since the relevant Galois embedding problems are not always solvable, it is always true that $\mathbb{Q}(d^\infty) \subseteq \mathbb{Q}(S_d^\infty)$. In the case that $d = 3$, [7] shows that in fact $\mathbb{Q}(3^\infty) = \mathbb{Q}(S_3^\infty)$. Further, if $G \subseteq S_d$ is transitive and nilpotent, then by a celebrated result of Shafarevich, the relevant Galois embedding problems are alway solvable and $\mathbb{Q}(G^\infty) \subseteq \mathbb{Q}(d^\infty)$ since the kernel of the embedding problem would also have to be nilpotent. In fact, G needn't be nilpotent itself as long as all the normal proper subgroups of G are nilpotent. For more information about what is known regarding Galois embedding problems, including a complete statement and proof of Shafarevich's theorem on the solvability of Galois embedding problems the reader is encouraged to see either [11], [19], or [32].

Theorem 1.11. *If $F/\mathbb{Q}$ is the compositum of all D_4-extensions of $\mathbb{Q}$, then $F = \mathbb{Q}(D_4^\infty)$.*

Proof. From Definition 1.10 and Shafarevich's theorem on the solvability of Galois embeddings with nilpotent kernels we see that the field $\mathbb{Q}(D_4^\infty)$ is the compositum of all D_4, $\mathbb{Z}/4\mathbb{Z}$, and V_4 extensions

of $\mathbb{Q}$. Here V_4 is the Klein Four-group. From this we immediately get that $F \subseteq \mathbb{Q}(D_4^\infty)$ and to show the reverse inclusion we simply need to show that any $\mathbb{Z}/4\mathbb{Z}$ or V_4 extension of $\mathbb{Q}$ is in F.

Suppose that $K/\mathbb{Q}$ is a finite extension such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ and consider the group $D_4 \times D_4$ together with t_i and s_i generators of the ith copy of D_4 with order 4 and 2 respectively. Next let $G = \langle t_1 s_2, t_2 s_1 \rangle \subseteq D_4 \times D_4$. The group G has the property that $G/[G,G] \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Clearly, there exists a $K'/\mathbb{Q}$ such that $\mathrm{Gal}(K'/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ since we can just pick $K' = K(\sqrt{p})$ for some prime p unramified in $K/\mathbb{Q}$. This give us a short exact sequence

$$1 \longrightarrow [G,G] \longrightarrow G \longrightarrow \mathrm{Gal}(K'/\mathbb{Q}) \longrightarrow 1$$

From the celebrated result of Shafarevich mentioned above together with the fact that $[G,G]$ is nilpotent we know that there is a field $L \subseteq K' \subseteq K$ such that $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$. Studying the group G, we see that there are two normal subgroups $N_1 = \langle t_1^2 \rangle$ and $N_2 = \langle t_1^2 \rangle$ such that $G/N_1 \simeq G/N_2 \simeq D_4$ which means that there are two subfields of L, call them L_1 and L_2 such that

$$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \mathrm{Gal}(L_2/\mathbb{Q}) \simeq D_4.$$

Further, since $|N_1| = |N_2| = 2$ and $N_1 \neq N_2$, we know that $[L : L_1] = [L : L_2] = 2$ and $L_1 \neq L_2$. Therefore $L = L_1 L_2 \subseteq F$ and $K \subseteq K' \subseteq L = L_1 L_2 \subseteq F$.

To see that every V_4 extension of $\mathbb{Q}$ is contained in F it is enough to note that by the same result of Shafarevich, every quadratic extension $F/\mathbb{Q}$ can be embedded in an $\mathbb{Z}/4\mathbb{Z}$ extension of $\mathbb{Q}$ and we just saw that every such extension is in F.

□

Remark 1.12. In light of Theorem 1.11, for the rest of the paper, we will use $\mathbb{Q}(D_4^\infty)$ to denote both the compositum of D_4 extensions of $\mathbb{Q}$ and well as the compositum of all generalized D_4 extensions of $\mathbb{Q}$.

The main goal of this article is to classify (up to isomorphism) the groups that occur as the torsion subgroup of an elliptic curve defined over $\mathbb{Q}$ and then base-extended to $\mathbb{Q}(D_4^\infty)$. The reason we chose to work with the group D_4 is that it is the simplest nonabelain transitive subgroup of S_4 that has yet to be dealt with. We chose to work with a nonabelain group since the torsion structures of rational elliptic curves base-extended to the maximal abelian extension of $\mathbb{Q}$ have been completely classified in [3].

Theorem 1.13. *Let $E/\mathbb{Q}$ be an elliptic curve. The torsion subgroup $E(\mathbb{Q}(D_4^\infty))_{\mathrm{tors}}$ is finite and*

$$E(\mathbb{Q}(D_4^\infty))_{\mathrm{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } M = 1,3,5,7,9,13,15, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \text{with } M = 1,5 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4M\mathbb{Z} & \text{with } 1 \leq M \leq 6 \text{ or } M = 8, \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} & \text{or} \\ \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8M\mathbb{Z} & \text{with } 1 \leq M \leq 4 \text{ or} \\ \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/12M\mathbb{Z} & \text{with } 1 \leq M \leq 2 \text{ or} \\ \mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}. & \end{cases}$$

All but 3 of the 24 torsion structures listed above occur for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$. The torsion structures that occur finitely often are $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z}$, and $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$ which occur for 4, 2, and 1 $\overline{\mathbb{Q}}$-isomorphism classes respectively.

In Table 1, for each torsion structure T that occurs in Theorem 1.13 we give the Cremona label of the elliptic curve $E/\mathbb{Q}$ with the smallest conductor such that $E(\mathbb{Q}(D_4^\infty))_{\text{tors}} \simeq T$. Throughout the paper, we will refer to elliptic curves by their Cremona label [4] and provide a hyperlink to their entry on the L-functions and Modular Forms Database [22].

$E/\mathbb{Q}$	$E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$	$E/\mathbb{Q}$	$E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$
26b2	$\{\mathcal{O}\}$	15a5	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$
19a2	$\mathbb{Z}/3\mathbb{Z}$	66c1	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$
11a2	$\mathbb{Z}/5\mathbb{Z}$	30a1	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$
26b1	$\mathbb{Z}/7\mathbb{Z}$	210e1	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$
54a2	$\mathbb{Z}/9\mathbb{Z}$	11a1	$\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$
2890d1	$\mathbb{Z}/13\mathbb{Z}$	17a1	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$
50a1	$\mathbb{Z}/15\mathbb{Z}$	15a2	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$
19a1	$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$	30a2	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$
338d1	$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z}$	210e2	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$
46a1	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	14a1	$\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$
17a3	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	256a1	$\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$
14a3	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$	15a1	$\mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$

TABLE 1. Examples of minimal conductor for each possible torsion structure over $\mathbb{Q}(D_4^\infty)$

All of the computations were done using Magma [1] and the procedures used to verify the examples in Table 1 and all the other computational results are available at [5]. These include the modular curves that were used to compute a complete set of rational functions that parametrize the elliptic curves over $\mathbb{Q}$ with a given torsion structure when base-extended to $\mathbb{Q}(D_4^\infty)$ in Table 4.

Many of the results in this article rely on recent advances on Galois representations associated to elliptic curves defined over $\mathbb{Q}$. In particular, we take advantage of the impressive results of Rouse and Zureick-Brown in [30], where all the possible 2-adic images of Galois representations attached to elliptic curves are classified. We also use the equally impressive classifications of mod p representations attached to rational elliptic curves given in [35] and the classification of modular curves of primes-power level with infinitely many points given in [34].

The organization of the paper is as follows. In Section 2, we briefly review results about Galois representations attached to elliptic curves which will be useful for the rest of the paper. In Section 3, we find necessary and sufficient conditions for a finite group to be of generalized D_4-type and classify some important subfields of $\mathbb{Q}(D_4^\infty)$. In Section 4, we give some general results about the field of definition of isogenies and how torsion groups grow under base-extension. Section 5 classifies all of the possible nontrivial p-primary components of torsion subgroups of an elliptic curve $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. In Section 6, we prove that the 24 groups in Theorem 1.13 are the only groups up to isomorphism that occur. Finally, in Section 7, we precisely characterize the elliptic curves that realize each of the subgroups listed in Theorem 1.13.

1.1. **Acknowledgements.** The author would like to thank Álvaro Lozano-Robledo for many useful conversations during the preparation of this paper. We would also like to thank Maarten Derickx, Jeffrey Hatley, Filip Najman, Andrew Sutherland, and the anonymous referee for useful comments and conversations about earlier versions of this article.

2. Galois representations associated to elliptic curves

Before talking about Galois representations associated to elliptic curves we need to establish some notation. We will follow the notational conventions laid out in [7, Section 2], but repeat some of them here for the ease of the reader.

For the rest of the paper we fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ that contains all of the algebraic extensions of $\mathbb{Q}$ that we are going to consider. For an elliptic curve E defined over a field K, we let

$$E[n] = \{P \in E(\overline{K}) : nP = \mathcal{O}\}$$

where $\overline{K}$ is a fixed algebraic closure of K. A classical result in the study of rational elliptic curves is that $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ as long as the characteristic of K is relatively prime to n. If L/K is a field extension, we write $E(L)[n]$ for the n-torsion subgroup of $E(L)$ and $E(L)(p)$ for the p-primary component of $E(L)$. Given a point $P \in E(L)$, we write $K(P)$ for the extension of K generated by adjoining the coordinates of P and $K(x(P))$ for the extension of K generated by adjoining the x-coordinate of P. We point out here that while $x(P)$ itself depends on the choice of model for E, the field $K(x(P))$ is in fact independent of this choice.

Given an elliptic curve E/K, an *n-isogeny* is a cyclic isogeny $\varphi\colon E \to E'$ of degree n; this means $\ker\varphi$ is a cyclic subgroup of $E[n]$, and as all the isogenies we consider are separable, this cyclic group has order n. The isogenies φ that we consider are also *rational*, meaning that φ is defined over K, equivalently, that $\ker\varphi$ is *Galois-stable*: the action of $\mathrm{Gal}(\overline{K}/K)$ on $E[n]$ given by its action on the coordinates of the points $P \in E[n]$ permutes $\ker\varphi$. We consider two (separable) isogenies to be distinct or nonisomorphic only when their kernels are distinct.

If $E/\mathbb{Q}$ is an elliptic curve and n is a positive integer, then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$ component-wise and this action induces a continuous homomorphism

$$\bar{\rho}_{E,n}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

whose image we will view as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ up to conjugacy. The reason it is only defined up to conjugacy is that the isomorphism between $\mathrm{Aut}(E[n])$ and $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and depends on a choice of basis for $E[n]$. The homomorphism $\bar{\rho}_{E,n}$ is called the *mod n Galois representation attached to E*. The extension $\mathbb{Q}(E[n])/\mathbb{Q}$ is Galois and the restriction of $\bar{\rho}_{E,n}$ to $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is injective and so $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$; namely, $\mathrm{Im}\,\bar{\rho}_{E,n}$. The determinant map $\det\colon \mathrm{Im}\,\bar{\rho}_{E,n} \to (\mathbb{Z}/n\mathbb{Z})^\times$ must be surjective and there must be an element in $\mathrm{Im}\,\bar{\rho}_{E,n}$ (corresponding to complex conjugation) with trace 0 and determinant -1. For more information about Galois representations attached to elliptic curves the reader should consult [31].

Given that the Galois groups that we are interested in studying are isomorphic to subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, it will be worthwhile to distinguish some subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ up to conjugation. In particular, two groups are worth highlighting:

(1) the *Borel group* of upper triangular matrices,
(2) the *split Cartan* subgroup of diagonal matrices.

We mention these two groups because if $E/\mathbb{Q}$ is an elliptic curve, then E has a rational n-isogeny if and only if $\mathrm{Im}\,\bar{\rho}_{E,n}$ is conjugate to a subgroup of the Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Similarly, E admits two independent n-isogenies if and only if $\mathrm{Im}\,\bar{\rho}_{E,n}$ is conjugate to a subgroup of the split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

3. Groups and Fields of Generalized D_4-type

In this section we study groups and fields of generalized D_4-type. Recall that a group is said to be of *generalized D_4-type* if it is isomorphic to a quotient of a subdirect product of transitive subgroups of D_4.

Example 3.1. Clearly the groups $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ are all of generalized D_4-type. More interestingly, the quaternion group Q_8 is generalized D_4-type since $Q_8 \simeq G/H$ with

$$G = \langle (2,4)(5,6,7,8), (1,2,3,4) \rangle, \quad H = \langle (1,3)(2,4)(5,7)(6,8) \rangle.$$

Going forward it will be useful to have necessary and sufficient conditions for a finite group G to be of generalized D_4-type.

Lemma 3.2. *A finite group G is of generalized D_4-type if and only if it has exponent dividing 4 and nilpotency class at most 2.*

Proof. The necessity of these two conditions follows from the fact that D_4 has both of these properties and they are preserved under taking subgroups, direct products and quotients.

What is left to prove is that these two conditions are sufficient to conclude that G is of generalized D_4-type. We prove this by showing that the free group of nilpotency class 2 and exponent 4 on k generators is isomorphic to a subgroup of D_4^n for some n. We will denote the free group of nilpotency class 2 and exponent 4 on k generators by G_k. Proving this is enough since any finite group that has nilpotency class at most 2 and exponent 4 is a quotient of one of these groups. We will proceed by induction on the number of generators.

Base case: The group G_2 has the following presentation:

$$G_2 = \langle x_1, x_2 \mid x_1^4 = x_2^4 = [x_1, x_2]^2 = e, [x_1, [x_1, x_2]] = [x_2, [x_1, x_2]] = e \rangle$$

and is SmallGroup(32,2) in Magma. Let $H = D_4^3$ and let τ_i and σ_i be the elements of order 4 and 2 respectively that generate the i-th copy of D_4. It is an easy check to show that $G_2 \simeq \langle \tau_1\tau_2, \sigma_1\tau_3 \rangle$.

Inductive Assumption: Suppose that G_k is isomorphic to a subgroup of D_4^n for some n. Let $x_1, \dots x_{k+1}$ be the generators of G_{k+1} and let H_ℓ be the smallest subgroup of G_{k+1} containing all the generators except x_ℓ. Notice that since G_{k+1} is nilpotent of degree 2, the commutator subgroup of G_{k+1} is contained in its center. Combining this with the fact that G_{k+1} is exponent 4, we get that every element in G_{k+1} can be written uniquely in the form

$$x_1^{a_1} \cdots x_{k+1}^{a_{k+1}} [x_1, x_2]^{b_1} [x_1, x_3]^{b_2} \cdots [x_k, x_{k+1}]^{b_m},$$

where $[x_i, x_j]$ is the commutator of x_i and x_j, $a_i \in \{0, 1, 2, 3\}$, and $b_j \in \{0, 1\}$.

Since all the relations defining these groups are symmetric, for each $1 \leq \ell \leq k+1$, $H_\ell \simeq G_k$ and so by assumption H_ℓ is isomorphic to a subgroup of D_4^n. Let $\varphi_\ell \colon H_\ell \to D_4^n$ be an injective homomorphism, so that $H_\ell \simeq \mathrm{Im}(\varphi_\ell) \subseteq D_4^n$. We extend each φ_ℓ to a homomorphism on all of G_{k+1} by declaring $\varphi_\ell(x_\ell)$ to be trivial.

Using these we define a map $\psi \colon G_{k+1} \to (D_4^n)^{k+1}$ by $\psi(x) = \big(\varphi_1(x), \varphi_2(x), \dots, \varphi_{k+1}(x)\big)$. Clearly this is a homomorphism since each φ_ℓ is a homomorphism. The map ψ is injective since $\ker(\varphi_\ell) = \langle x_\ell, [x_\ell, x_1], \dots, [x_\ell, x_{k+1}] \rangle$ and so the only element in G_{k+1} that gets sent to the identity by every φ_ℓ is the identity element. $\square$

Example 3.3. The proof of Lemma 3.2 is constructive and so we can compute explicitly the isomorphisms in each case. As pointed out in the proof $G_2 \simeq \langle \tau_1\tau_2, \sigma_1\tau_3\rangle$ and let G_3 be generated by x_1, x_2, and x_3, then

$$\begin{aligned} H_1 &= \langle x_2, x_3\rangle \simeq \langle \tau_1\tau_2, \sigma_1\tau_3\rangle, \\ H_2 &= \langle x_3, x_1\rangle \simeq \langle \tau_4\tau_5, \sigma_4\tau_6\rangle, \\ H_3 &= \langle x_1, x_2\rangle \simeq \langle \tau_7\tau_8, \sigma_7\tau_9\rangle. \end{aligned}$$

Again, it is a simple check in Magma to show that

$$G_3 \simeq \left\langle \sigma_4\tau_6\tau_7\tau_8, \tau_1\tau_2\sigma_7\tau_9, \sigma_1\tau_3\tau_4\tau_5 \right\rangle.$$

Remark 3.4. The embedding of G_3 into D_4^9 is far from optimal. In fact, G_3 is a subgroup of a much smaller power of D_4. The smallest possible power it embeds into is 6 with

$$G_3 \simeq \left\langle \tau_1\tau_2\tau_3, \sigma_2\sigma_3\tau_4\tau_5, \sigma_2\sigma_4\tau_5\tau_6 \right\rangle.$$

Example 3.5. Clearly, $\mathbb{Z}/8\mathbb{Z}$ is not of generalized D_4-type since its exponent is 8. On the other hand SmallGroup(32,6), the faithful semidirect product of $(\mathbb{Z}/2\mathbb{Z})^3$ and $\mathbb{Z}/4\mathbb{Z}$, has exponent 4 but nilpotency class 3 and so is not of generalized D_4-type.

Let $K/\mathbb{Q}$ be a number field. We will denote the Galois closure of K by $\widehat{K}$.

Remark 3.6. It is clear from basic Galois theory that the compositum of any two fields of generalized D_4-type, is also of generalized D_4-type and any subfield of a field of generalized D_4-type will also be of generalized D_4-type. Since every finite extension $K \subseteq \mathbb{Q}(D_4^\infty)$ over $\mathbb{Q}$ is contained in a finite Galois extension $\widehat{K}/\mathbb{Q}$ of generalized D_4-type, we can view $\mathbb{Q}(D_4^\infty)$ as the compositum of Galois extensions and thus the infinite extension $\mathbb{Q}(D_4^\infty)/\mathbb{Q}$ is also Galois.

Lemma 3.7. *Given any square-free $d \in \mathbb{Z}$, $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(D_4^\infty)$.*

Proof. For any such d, $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ which is of generalized D_4-type. □

Going forward it will also be important to know which roots of unity are contained in $\mathbb{Q}(D_4^\infty)$. Fortunately, using Lemma 3.2 classifying these subfields is fairly simple.

Lemma 3.8. *Let n be a natural number. Then, $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(D_4^\infty)$ if and only if n divides 240.*

Proof. Let $\lambda(n)$ be the exponent of $\mathrm{Gal}(\zeta_n/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. It is a classical result that $\lambda(2^e) = 2^{e-2}$ and $\lambda(p^e) = (p-1)p^{e-1}$ for primes $p > 2$. It follows that if ℓ is prime then $\lambda(\ell^j)$ divides 4 if and only $\ell^j \in \{2, 3, 4, 5, 8, 16\}$. In these cases $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ which has nilpotency class 1 and so Lemma 3.2 shows that $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(D_4^\infty)$. □

4. Growth of the torsion subgroups of elliptic curves by base extension

In this section, we present results about the fields of definition of torsion subgroups of elliptic curves that will be useful throughout the rest of the paper.

Proposition 4.1. [33, Ch. III, Cor. 8.1.1] *Let E/L be an elliptic curve with $L \subseteq \overline{\mathbb{Q}}$. For each integer $n \geq 1$, if $E[n] \subseteq E(L)$ then the nth cyclotomic field $\mathbb{Q}(\zeta_n)$ is a subfield of L.*

Theorem 4.2. [7, Theorem 4.1] *Let $E/\mathbb{Q}$ be an elliptic curve and let F be a (possibly infinite) Galois extension of $\mathbb{Q}$ that only contains finitely many roots of unity. Then $E(F)_{\text{tors}}$ is finite. Moreover, there is a uniform bound B, depending only on F, such that $\#E(F)_{\text{tors}} \leq B$ for every elliptic curve $E/\mathbb{Q}$.*

Theorem 4.2 together with Lemma 3.8 shows that if $E/\mathbb{Q}$ is an elliptic curve, then $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ must be finite and immediately limits the possible n's such that $E[n] \subseteq E(\mathbb{Q}(D_4^\infty))$. Below we present the main reults used to prove Theorem 4.2 as they will be useful in the next few sections.

Lemma 4.3. [7, Lemma 4.6] *Let E and F be as in Theorem 4.2, let p be a prime, and let k be the largest integer for which $E[p^k] \subseteq E(F)$. If $E(F)_{\text{tors}}$ contains a subgroup isomorphic to $\mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^j\mathbb{Z}$ with $j \geq k$, then E admits a rational p^{j-k}-isogeny.*

Theorem 4.4 ([28],[15],[16],[17],[18])**.** *Let $E/\mathbb{Q}$ be an elliptic curve with a rational n-isogeny. Then*

$$n \leq 19 \text{ or } n \in \{21, 25, 27, 37, 43, 67, 163\}.$$

With these results, it is clear that it will be helpful to better understand the field of definition of the kernel a given isogeny.

Lemma 4.5. [7, Lemma 4.8] *Let $E/\mathbb{Q}$ be an elliptic curve that admits a rational n-isogeny φ, and let $R \in E[n]$ be a point of order n in the kernel of φ. The field extension $\mathbb{Q}(R)/\mathbb{Q}$ is Galois and $\text{Gal}(\mathbb{Q}(R)/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. In particular, if n is prime, then $\text{Gal}(\mathbb{Q}(R)/\mathbb{Q})$ is cyclic and its order divides $n-1$.*

Proposition 4.6. [23, Theorem 2.1] *Let $E/\mathbb{Q}$ be an elliptic curve and let $p \geq 11$ be a prime, other than 13. Let $R \in E[p]$ be a torsion point of exact order p and let $\mathbb{Q}(R) = \mathbb{Q}(x(R), y(R))$ be the field of definition of R. Then*

$$[\mathbb{Q}(R) : \mathbb{Q}] \geq \frac{p-1}{2}$$

unless $j(E) = -7 \cdot 11^3$ and $p = 37$, in which case $[\mathbb{Q}(R) : \mathbb{Q}] \geq (p-1)/3 = 12$.

5. The maximal p-primary components of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$

We are now ready to start to classifying the groups $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ up to isomorphism as E ranges over all elliptic curves defined over $\mathbb{Q}$. The first step is to compute a bound on $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ by obtaining bounds on the p-primary components of $E(\mathbb{Q}(D_4^\infty))$ for elliptic curves E defined over $\mathbb{Q}$ *without* complex multiplication.

Theorem 5.1. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to a subgroup of*

$$T_{\max} = (\mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}) \oplus (\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}) \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z},$$

and $T_{\max}$ is the smallest group with this property.

To prove Theorem 5.1 we first notice that there are only finitely many primes such that the p-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ could be nontrivial.

Proposition 5.2. *Let $E/\mathbb{Q}$ be an elliptic curve, and let p be a prime dividing the cardinality of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. Then $p \in \{2, 3, 5, 7, 13\}$.*

Proof. From Proposition 4.1 and Lemma 4.3 the p-primary component of $E(\mathbb{Q}(D_4^\infty))$ maybe non-trivial if and only if $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(D_4^\infty)$ or E has a rational p-isogeny. With this, Lemma 3.8, and Theorem 4.4 the only primes that can divide the cardinality of $E(\mathbb{Q}(D_4^\infty))$ are exactly the ones in $S = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$. From Lemma 4.5 if $E(\mathbb{Q}(D_4^\infty))[p] = \langle R \rangle \simeq \mathbb{Z}/p\mathbb{Z}$, then $\mathbb{Q}(R)/\mathbb{Q}$ is a cyclic extension and of generalized D_4-type. Therefore the extension is at most degree 4. Combining this with Proposition 4.6 completes the proof. □

Remark 5.3. Proposition 5.2 does not require that $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. This observation will be useful when we are dealing with the case of elliptic curves with complex multiplication in Section 5.6.

Recall that the $\overline{\mathbb{Q}}$-isomorphism class of an elliptic curve $E/\mathbb{Q}$ may be identified with its j-invariant $j(E)$.

Proposition 5.4. *Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) \neq 0$. The isomorphism type of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ depends only on the $\overline{\mathbb{Q}}$-isomorphism class of E, equivalently, only on $j(E)$.*

Proof. Recall that for $j(E) \neq 0, 1728$, if $j(E') = j(E)$ for some $E'/\mathbb{Q}$ then E', is a quadratic twist of E, hence isomorphic to E over an extension of degree at most 2. If $j(E) = 1728 = j(E')$, then $E'/\mathbb{Q}$ is isomorphic to E over a field of the form $\mathbb{Q}(\sqrt[4]{n})$ for some $n \in \mathbb{Z}$ [33, §X.5]. The Galois closure of such a field is isomorphic to a subgroup of D_4 and so for $j(E) = j(E') \neq 0$, the elliptic curves E and E' are isomorphic over a field of generalized D_4-type, hence their base changes to $\mathbb{Q}(D_4^\infty)$ are isomorphic and $E(\mathbb{Q}(D_4^\infty))_{\text{tors}} \simeq E'(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. □

Lemma 5.5. *There are three possible torsion structures over $\mathbb{Q}(D_4^\infty)$ given an elliptic curve $E/\mathbb{Q}$ with $j(E) = 0$. They are realized by the curves* `27a1`, `36a1`, *and* `108a1`.

Proof. Every elliptic curve $E/\mathbb{Q}$ with $j(E) = 0$ is isomorphic over $\mathbb{Q}$ to a curve of the form

$$E_s : y^2 = x^3 + s$$

for some $s \in \mathbb{Z} \setminus \{0\}$ that is 6th power free. The three division polynomial of E_s is given by $f_3(x) = 3x(x^3 + 4s)$ and so we can see that generically these curve will have a point of order 3 defined over a quadratic field and hence $\mathbb{Q}(D_3^\infty)$. Further inspection shows that if $4s = t^3$ for some $t \in \mathbb{Q}$ then $E[3] \subseteq E(\mathbb{Q}(D_4^\infty))$ since this would mean that E would have it's full 3-torsion defined over a 2-elementary extension of $\mathbb{Q}$. In this case $\operatorname{Im} \bar{\rho}_{s,3}$ is contained in a group conjugate to a subgroup of the split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. In fact, if $4s$ is a cube, the factorization of the 9-division polynomial of E_s shows shows that E_s has a 3-isogeny and a 9-isogeny that are independent of each other. Notice also that if $t, r \in \mathbb{Z} \setminus \{0\}$, then the curves E_{2t^3} and E_{2r^3} are isomorphic over $\mathbb{Q}(\sqrt{rt}) \subseteq \mathbb{Q}(D_4^\infty)$. Therefore, all over these curves have the same torsion subgroup over $\mathbb{Q}(D_4^\infty)$ as $E_2(\mathbb{Q}(D_4^\infty))_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

From [23, Table 3 & 4], the only other possible isogeny type that E_s can have is a 2-isogeny. This occurs exactly when $s = t^3$ for some $t \in \mathbb{Z}$ and thus has a point of order 2 defined of $\mathbb{Q}$ and in fact $E[4] \subseteq E(\mathbb{Q}(D_4^\infty))$. Again, if $t, r \in \mathbb{Z} \setminus \{0\}$, then E_{t^3} is isomorphic to E_{r^3} over $\mathbb{Q}(\sqrt{rt}) \subseteq \mathbb{Q}(D_4^\infty)$ and so $E_{t^3}(\mathbb{Q}(D_4))_{\text{tors}} \simeq E_{r^3}(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. Thus for every $r \in \mathbb{Z} \setminus \{0\}$, $E_{r^3}(D_4^\infty)_{\text{tors}} \simeq E_1(\mathbb{Q}(D_4^\infty))_{\text{tors}} \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$.[1]

[1]The curve E_{t^3} has its full 8-torsion defined over $\mathbb{Q}(D_4^\infty)$ because it has discriminant $-432t^6$ and its 2-isogenous curve has discriminant $6912t^6$ and so $-432t^6 \equiv (-1)(6912t^6) \bmod (\mathbb{Q}^\times)^2$. This is enough to show that $\operatorname{Im} \bar{\rho}_{E_{t^3},8}$ is of generalized D_4-type.

The analysis in the sections following this lemma we show that for every other prime p, the p-primary componenet of $E_s(\mathbb{Q}(D_4^\infty))$ must be trivial. Bringing this all together we have that

$$E_s(\mathbb{Q}(D_4^\infty))_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \text{if 4s is a cube,} \\ \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z} & \text{if s is a cube,} \\ \mathbb{Z}/3\mathbb{Z} & \text{otherwise.} \end{cases}$$

Each of these three cases are realized by the three curves listed in the statement of the Lemma. □

5.1. The case when $p = 13$.

Proposition 5.6. *Suppose that $E/\mathbb{Q}$ is an elliptic curve such that 13 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. Then, $E(\mathbb{Q}(D_4^\infty))(13) \simeq \mathbb{Z}/13\mathbb{Z}$ and there exists $t \in \mathbb{Q}$ such that*

$$j(E) = \frac{(t^2 - t + 1)^3 P(t)^3}{(t-1)^{13} t^{13} (t^3 - 4t^2 + t + 1)}$$

where $P(t) = t^{12} - 9t^{11} + 29t^{10} - 40t^9 + 22t^8 - 16t^7 + 40t^6 - 22t^5 - 23t^4 + 25t^3 - 4t^2 - 3t + 1$.

Proof. Since $\mathbb{Q}(\zeta_{13}) \not\subseteq \mathbb{Q}(D_4^\infty)$ it must be that $E(\mathbb{Q}(D_4^\infty))[13] \simeq \mathbb{Z}/13\mathbb{Z}$. Suppose that R is a point that generates $E(\mathbb{Q}(D_4^\infty))[13]$. By Lemma 4.3 and Proposition 4.6, $\mathbb{Q}(R)/\mathbb{Q}$ must be a cyclic extension of degree dividing 12. Further, since this point is defined over $\mathbb{Q}(D_4^\infty)$ from Lemma 3.2 the degree $\mathbb{Q}(R)/\mathbb{Q}$ must divide 4 and $\operatorname{Im} \bar{\rho}_{E,13}$ is conjugate to a subgroup contained inside of the matrices of the form $\begin{pmatrix} a^3 & * \\ 0 & * \end{pmatrix}$.

The elliptic curves defined over $\mathbb{Q}$ with this property have been completely classified in [35], and they correspond to the curves with j-invariant of the form in the statement of the proposition. Further, since there are no elliptic curves defined over $\mathbb{Q}$ with a cyclic 169-isogeny, it is not possible for $E(\mathbb{Q}(D_4^\infty))(13)$ to be any larger. □

5.2. The case when $p = 7$.

Proposition 5.7. *Suppose that $E/\mathbb{Q}$ is an elliptic curve such that 7 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. Then, $E(\mathbb{Q}(D_4^\infty))(7) \simeq \mathbb{Z}/7\mathbb{Z}$ and there exists $t \in \mathbb{Q}$ such that*

$$j(E) = \frac{(t^2 - t + 1)^3 (t^6 - 11t^5 + 30t^4 - 15t^3 - 10t^2 + 5t + 1)^3}{(t-1)^7 t^7 (t^3 - 8t^2 + 5t + 1)}.$$

Proof. Again, since $\mathbb{Q}(\zeta_7) \not\subseteq \mathbb{Q}(D_4^\infty)$ and there are no elliptic curves defined over $\mathbb{Q}$ with a 49-isogeny it must be that $E(\mathbb{Q}(D_4^\infty))(7) \simeq \mathbb{Z}/7\mathbb{Z}$. Suppose that R is a point that generates $E(\mathbb{Q}(D_4^\infty))(7)$. This time, the extension $\mathbb{Q}(R)/\mathbb{Q}$ is cyclic of degree dividing 6. Therefore, if $\mathbb{Q}(R) \subseteq \mathbb{Q}(D_4^\infty)$ it must be degree 2 or 1. If $[\mathbb{Q}(R) : \mathbb{Q}]$ is in fact degree 2, this means that E has a point of order 7 defined over a quadratic extension of $\mathbb{Q}$. In fact, if E has a point of order 7 defined over a quadratic field, then there is a quadratic twist of E that has a order of order 7 defined over $\mathbb{Q}$. These curves are parameterized by a genus 0 modular curve and the j-map can again be found in [35]. □

5.3. The case when $p = 5$.

Proposition 5.8. *Suppose that $E/\mathbb{Q}$ is an elliptic curve such that 5 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. Then it must be that $E(\mathbb{Q}(D_4^\infty))(5) \simeq \mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$. Further, $E(\mathbb{Q}(D_4^\infty))(5)$ has a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z}$ exactly when there exists a $t \in \mathbb{Q}$ such that*

$$j(E) = \frac{5^2(t^2+10t+5)^3}{t^5},$$

while $E(\mathbb{Q}(D_4^\infty))(5) \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ exactly when there exists a $t \in \mathbb{Q}$ such that

$$j(E) = \frac{(t^2+5t+5)^3(t^4+5t^2+25)^3(t^4+5t^3+20t^2+25t+25)^3}{t^5(t^4+5t^3+15t^2+25t+25)^5}.$$

Proof. If $E(\mathbb{Q}(D_4^\infty))(5) \simeq \mathbb{Z}/5\mathbb{Z}$, the single point of order 5 must be defined over a cyclic extension of order dividing 4 by Lemma 4.5. All of these extensions are of generalized D_4-type, which is to say that having a 5-isogeny is necessary and sufficient for E to have a point of order 5 defined over $\mathbb{Q}(D_4^\infty)$. Elliptic curves defined over $\mathbb{Q}$ with a rational 5-isogeny are parametrized by the genus 0 modular curve $X_0(5)$ and the j-map can again be found in [35] and is listed above.

If $E(\mathbb{Q}(D_4^\infty))(5) \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ then $\text{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}) \simeq \text{Im}\,\bar{\rho}_{E,5} \subseteq \text{GL}_2(\mathbb{Z}/5\mathbb{Z})$ must be of generalized D_4-type. Searching for subgroups of $\text{GL}_2(\mathbb{Z}/5\mathbb{Z})$ up to conjugation that are of generalized D_4-type, have surjective determinant, and have an element of trace 0 and determinant -1, we find that up to conjugation they are all contained in a single maximal group. More precisely, if $\text{Im}\,\bar{\rho}_{E,5}$ is of generalized D_4-type, then it is conjugate to a subgroup of the split-Cartan subgroup of $\text{GL}_2(\mathbb{Z}/5\mathbb{Z})$. Elliptic curves with this property are again parametrized by a genus 0 modular curve whose j-map is given in [35].

To complete the proof, all that is left to do is prove that $E(\mathbb{Q}(D_4^\infty))(5)$ cannot contain a point of order 25. Suppose towards a contradiction that $E(\mathbb{Q}(D_4^\infty))$ contains a point of order 25. There are two ways that this could happen: either $E(\mathbb{Q}(D_4^\infty))(5) \simeq \mathbb{Z}/25\mathbb{Z}$ or it contains a group isomorphic to $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}$.

In the first case, from Lemmas 4.3 and 4.5 together with our classification of groups of generalized D_4-type, the first case can only occur if E has a point of order 25-defined over a cyclic quartic extension of $\mathbb{Q}$, but from [2, Theorem 1.2] this can't happen.

Next, suppose that $E(\mathbb{Q}(D_4^\infty)$ contains a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}$. This would mean that $G = \text{Im}(\bar{\rho}_{E,25}) \subseteq \text{GL}_2(\mathbb{Z}/25\mathbb{Z})$ has the following two properties:

(1) G has a surjective determinant map and an element with trace 0 and determinant -1,
(2) G contains a normal subgroup N that acts trivially on a $\mathbb{Z}/25\mathbb{Z}$-submodule of $\mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}$ isomorphic to $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}$ for which G/N is of generalized D_4-type.

The first property is comes from the discussion in Section 2, while the second property reflects the requirement that $\mathbb{Q}(E[25])$ contains the Galois extension $\mathbb{Q}(E(\mathbb{Q}(D_4^\infty))[25])/\mathbb{Q}$ whose Galois group is isomorphic to G/N and for which the Galois group $\text{Gal}(\mathbb{Q}(E[27])/\mathbb{Q}(E(\mathbb{Q}(D_4^\infty))[25])) \simeq N$ acts trivially on a subgroup of $E[25]$ which is isomorphic to $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}$.

Enumerating such groups in Magma, we find that there are 3 maximal groups with properties (1) and (2) and each of them is conjugate to a subgroup of

$$H = \left\langle \begin{pmatrix} 7 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Inspecting this group, we see that $\operatorname{Im}\bar{\rho}_{E,25}$ can only be conjugate to a subgroup H if E has a point of order 25 defined over a cyclic quartic field and again this is impossible from [2]. □

Corollary 5.9. *Suppose that $E/\mathbb{Q}$ is an elliptic curve without complex multiplication such that 5 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. Then E admits a rational 5-isogeny. In particular if $E(\mathbb{Q}(D_4^\infty))(5) \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, then E admits two independent 5-isogenies.*

5.4. **The case when $p = 3$.**

Proposition 5.10. *Suppose that $E/\mathbb{Q}$ is an elliptic curve without complex multiplication such that 3 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. Then it must be that $E(\mathbb{Q}(D_4^\infty))(3) \simeq \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$, or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Further, $E(\mathbb{Q}(D_4^\infty))(3)$ has a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$ exactly when there exists a $t \in \mathbb{Q}$ such that*

$$j(E) = 27\frac{(t+1)(t+9)^3}{t^3},$$

$E(\mathbb{Q}(D_4^\infty))(3)$ has a subgroup isomorphic to $\mathbb{Z}/9\mathbb{Z}$ exactly when there exists a $t \in \mathbb{Q}$ such that

$$j(E) = \frac{(t^3-3t^2+1)^3(t^9-9t^8+27t^7-48t^6+54t^5-45t^4+27t^3-9t^2+1)^3}{(t-1)^9t^9(t^2-t+1)^2(t^3-6t^2+3t+1)},$$

$E(\mathbb{Q}(D_4^\infty))(3)$ has a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ exactly when there exists a $t \in \mathbb{Q}$ such that

$$j(E) = 27\frac{(t+1)^3(t-3)^3}{t^3}.$$

Proof. Suppose that $E(\mathbb{Q}(D_4^\infty))(3) \simeq \mathbb{Z}/3^k\mathbb{Z}$. In this case, in order for these points to be defined over $\mathbb{Q}(D_4^\infty)$ it must be that they are defined over a quadratic field since $(\mathbb{Z}/3^k\mathbb{Z})^\times$ is cyclic of order $2 \cdot 3^{k-1}$. Thus E must have a quadratic twist with a rational point point of order 3^k and from Theorem 1.2 this is only possible when $k = 1$ or 2. The curves with this property are again parameterized by genus 0 modular curves $X_1(3)$ and $X_1(9)$ and their j-maps can be found in many places including [34].

Next assume that $\mathbb{Q}(E[3]) \subseteq \mathbb{Q}(D_4^\infty)$. Searching for subgroups of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ up to conjugation that are of generalized D_4-type, have surjective determinant, and have an element of trace 0 and determinant -1, we find that all of these groups are contained inside the normalizer of the split-Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. These curves are parameterized by a genus zero modular curve and the j-map can be found in [35].

The last case we need to consider is if it is possible for $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ to contain a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$. Just as we did in the proof of Proposition 5.8, suppose towards a contradiction that E is such a curve and let $G = \operatorname{Im}\bar{\rho}_{E,9} \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. Using Magma we search for subgroups G of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ up to conjugation such that

(1) G has a surjective determinant map and an element with trace 0 and determinant -1,
(2) G contains a normal subgroup N that acts trivially on a $\mathbb{Z}/9\mathbb{Z}$-submodule of $\mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ for which G/N is of generalized D_4-type.

Again, there is exactly one maximal group H with this property,

$$H = \left\langle \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 8 & 0 \\ 0 & 8 \end{pmatrix} \right\rangle.$$

Inspecting H we see that in order for $\operatorname{Im}\bar{\rho}_{E,9} \subseteq H$, E would have to have a quadratic twist with a point of order 9 and another independent 3-isogeny. Since there is only one $\overline{\mathbb{Q}}$-isomorphism class of

elliptic curves with a 27-isogeny (see for example [23, Table 4]), there is only one elliptic curve up to $\overline{\mathbb{Q}}$-isomorphism with independent 3- and 9-isogenies. This is the class of CM elliptic curves with j-invariant equal to 0. □

Remark 5.11. Unlike the case when $p = 5$, there are elliptic curves $E/\mathbb{Q}$ such that 3 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$, but E does not admit a rational 3-isogeny.

Example 5.12. Let $E/\mathbb{Q}$ be the elliptic curve with Cremona label `338e1`. Then $\operatorname{Im}\bar{\rho}_{E,3}$ is exactly the normalizer of the split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. This curve has the property that $E(\mathbb{Q}(D_4^\infty))(3) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, but E does not admit a rational 3-isogeny.

5.5. **The case when $p = 2$.**

Proposition 5.13. *Given an elliptic curve $E/\mathbb{Q}$, either $E(\mathbb{Q}(D_4^\infty))[2]$ is trivial or $E[4] \subseteq E(\mathbb{Q}(D_4^\infty))$.*

Proof. Notice that generically one expects that $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$ which is not of generalized D_4-type. Further, in order for $E(\mathbb{Q}(D_4^\infty))[2]$ to be nontrivial it must be that $\mathbb{Q}(E[2])/\mathbb{Q}$ is either trivial or a quadratic extension. This is equivalent to $\operatorname{Im}\bar{\rho}_{E,2}$ being trivial or conjugate to $G = \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$. A simple check shows that the preimage of these groups under the standard componentwise reduction map $\pi\colon \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is of generalized D_4-type. Thus, $E(\mathbb{Q}(D_4^\infty))[2]$ is nontrivial exactly when E has at least one point of order 2 defined over $\mathbb{Q}$ and in this case it must be that case $E[4] \subseteq E(\mathbb{Q}(D_4^\infty))$. □

There are many additional issues when dealing with the case of $p = 2$ that do not arise in the previous cases. In particular, since there are rational elliptic curves with 16-isogenies and $\mathbb{Q}(\zeta_{16}) \subseteq \mathbb{Q}(D_4^\infty)$ the potential size of $E(\mathbb{Q}(D_4^\infty))(2)$ is much greater than the previous primes. While this does make things more difficult, we are fortunate that all the possible images of the 2-adic representations associated to rational elliptic curves have all been completely classified by Rouse and Zureick-Brown in [30]. Rather than ignoring these results and trudging through the many cases, we search the data available at their website using Magma and classify all the possible 2-torsion structures that can occur over $\mathbb{Q}(D_4^\infty)$. Doing this yields the following proposition.

Proposition 5.14. *Suppose that $E/\mathbb{Q}$ is an elliptic curve without complex multiplication such that 2 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. Then it must be that $E(\mathbb{Q}(D_4^\infty))(2)$ is isomorphic to one of the following group:*

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z},$$

$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z},\ \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z},\ \textit{or}\ \mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}.$$

Further, $E(\mathbb{Q}(D_4^\infty))(2)$ contains a subgroup isomorphic to each these options if and only if they come from a rational points on the genus 0 curves given in Table 2.

For the sake of brevity, we leave the j-maps for each of these genus 0 curve out of the statement of this Proposition 5.14 and this section. Instead, in Table 2 we list each possible nontrivial 2-primary component and the corresponding modular curves (in the notation of [30]) that parametrize the curves with these $\mathbb{Q}$. We also include Figure 1, that shows how these curves are related to each other. There is a line between two curves if the top one is covered by the bottom.

Together Propositions 5.6, 5.7, 5.8, 5.10, and 5.14 complete the proof of Theorem 5.1.

$E(\mathbb{Q}(D_4^\infty))(2)$	RZB Curve	$E(\mathbb{Q}(D_4^\infty))(2)$	RZB Curve
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	X_6	$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	X_8, X_{11}
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	X_{12}, X_{13}	$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$	X_{25}, X_{92}
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$	X_{36}	$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z}$	X_{193}
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z}$	X_{235}	$\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$	X_{58}

TABLE 2. Parameterization of the possible nontrivial 2-primary components

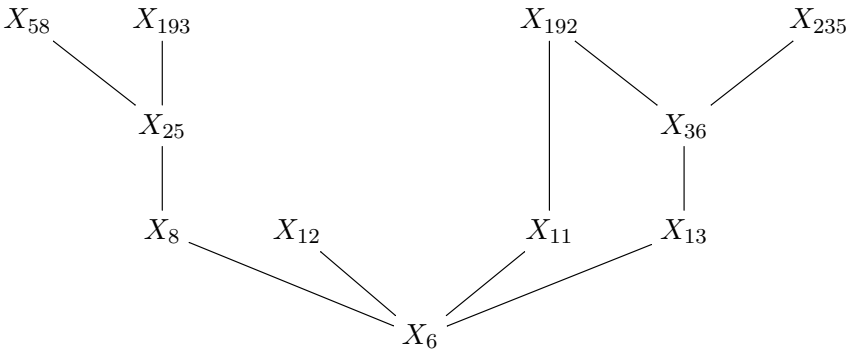


FIGURE 1. Covering relationships between the curves in Table 2

$E/\mathbb{Q}$	$E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$	$E/\mathbb{Q}$	$E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$
27a1	$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$	108a2	$\mathbb{Z}/3\mathbb{Z}$
27a4	$\mathbb{Z}/3\mathbb{Z}$	121b1	$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$
32a1	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	256d1	$\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$
32a4	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	361a1	$\{\mathcal{O}\}$
36a1	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$	1849a1	$\{\mathcal{O}\}$
36a2	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$	4489a1	$\{\mathcal{O}\}$
49a1	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	26569a1	$\{\mathcal{O}\}$
49a2	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$		

TABLE 3. Torsion structures of CM Elliptic curves

5.6. **The case when E has complex multiplication.** As mentioned in Proposition 5.4 and Lemma 5.5, if $E/\mathbb{Q}$ is an elliptic curve, as long as $j(E) \neq 0$, the isomorphism class of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ does not change under twisting and if $j(E)$ is 0, then it is sufficient to compute the torsion structure for the curves 27a1, 36a1, and 108a1. Using Proposition 5.2 to limit the computations, we compute $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ for each of the necessary representatives. The results of these computations can be found in Table 3.

6. Determining the possible torsion structures

The last task is to completely determine the finite abelian groups T that arise as the torsion subgroup of an elliptic curve defined over $\mathbb{Q}$ base-extended to $\mathbb{Q}(D_4^\infty)$ by determining which combinations of the possible p-primary components can occur. Throughout this section we will assume that E is an elliptic curve without complex multiplication, since we have already fully determined the torsion structures for curves with complex multiplication in Table 3.

Before we embark on this task, we look back on the previous section and make a useful observation.

Corollary 6.1. *If $E/\mathbb{Q}$ is an elliptic curve without CM and p is a prime such that $E(\mathbb{Q}(D_4^\infty))(p)$ is nontrivial, then either E has a p-isogeny, or $p = 3$ and $E(\mathbb{Q}(D_4^\infty)(3) = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.*

6.1. The cases when 13 or 7 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$.

We group the case of 13 and 7 diving $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ together because their classifications are similar in spirit.

Proposition 6.2. *Let $E/\mathbb{Q}$ be an elliptic curve such that 13 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. Then it follows that $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/13\mathbb{Z}$.*

Proof. From Lemma 4.3 and Proposition 5.6, the only way that 13 can divide $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is if E has a 13-isogeny. This combined with Corollary 6.1 and Theorem 4.4 shows that the only other possible nontrivial p-primary component is $p = 3$. Thus, the last case that needs to be ruled out is the case that E also has full 3-torsion defined over $\mathbb{Q}(D_4^\infty)$.

In order to rule out this last possibility we construct the modular curve that would parametrize elliptic curves with full 3-torsion and a point of order 13 defined over $\mathbb{Q}(D_4^\infty)$. We can construct this modular curve by taking the fiber product of the j-maps defined in Propositions 5.10 and 5.6. For shorthand we will denote the relevant j-maps by $j_3(t)$ and $j_{13}(t)$ respectively. The resulting modular curve X, is genus 13 with 4 singular points. In order to show that there are no elliptic curves defined over $\mathbb{Q}$ with full 3-torsion and a point of order 13 defined over $\mathbb{Q}(D_4^\infty)$ we need to show that there are no nonsingular and noncuspidal rational points on X. We can restrict to the nonsingular points here and else where in the paper since the singular points can only correspond to $j = 0$ or $j = 1728$ and those isomorphism classes have been dealt with in Section 5.6.

Inspecting j_3 and j_{13} we see that they are each invariant under a different fractional linear transformation. In particular,

$$j_{13}\left(\frac{1}{1-t}\right) = j_{13}(t) \text{ and } j_3\left(\frac{-3}{t}\right) = j_3(t).$$

Using these symmetries, we can construct two distinct automorphisms of the curve X and compute the quotient curve of X by the group $G \subseteq \text{Aut}(X)$, that they generate. Let $\pi\colon X \to X/G = H$ be the quotient map. Then π is a surjective map whose image, H is a nonsingular genus 2 hyperelliptic curve. The curve H has a simplified model given by

$$H\colon y^2 = x^6 + 10x^3 - 27.$$

Letting J be the jacobian of H, we can use Magma to compute that $J(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$. Thus, in order to find all of the points on H we can use the pullback of the natual embedding of $H(\mathbb{Q})$ into $J(\mathbb{Q})$. Using Magma we can see that the only points on H that are defined over $\mathbb{Q}$ are the two points at infinity (there are *two* points at infinity since H has the form $y^2 = f(x)$ with $\deg(f)$ even). Computing the pullback of these two points at infinity under π, we see that the only points on $X(\mathbb{Q})$ are the 4 singular points. □

Proposition 6.3. *Let $E/\mathbb{Q}$ be an elliptic curve such that 7 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$. Then it follows that $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/7\mathbb{Z}$.*

Proof. Again, from Lemma 4.3 and Proposition 5.7, the only way that 7 can divide $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is if E has a 7-isogeny. The difference this time is that according to Theorem 4.4 there are elliptic curves with 7-isogenies and 2- or 3-isogenies as well. Thus our isogeny argument still leaves open the possibility that E has a point of order 14 or 21 defined over $\mathbb{Q}(D_4^\infty)$. But, looking at the proof of Proposition 5.7 we see that the only way that 7 can divide $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is if E has a 7-isogeny defined over a quadratic field. From [23, Table 4] we can see that up to $\overline{\mathbb{Q}}$-isomorphism there are exactly 2 elliptic curves with 14-isogenies and 4 elliptic curves with 21-isogenies. Checking these curves by hand we see that none of them have a point of order 7 defined over a quadratic field and thus in these cases 7 doesn't divide $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$.

From Corollary 6.1, the only other possibility is that E has its full 3-torsion defined over $\mathbb{Q}(D_4^\infty)$. Let $j_7(t)$ and $j_3(t)$ be the relevant j-maps and construct the curve given by the affine equation defined by the numerator of $j_3(x) - j_7(y)$. The curve X that is defined by this equation is a singular genus 7 curve, but again we can construct two automorphisms from the fact that

$$j_7\left(\frac{1}{1-t}\right) = j_7(t) \text{ and } j_3\left(\frac{-3}{t}\right) = j_3(t).$$

Taking the quotient of X by the subgroup generated by these two automorphisms leaves a hyperelliptic curve H with genus 2. The curve H is given by the simplified equation

$$H\colon y^2 = x^6 + 26x^3 - 27.$$

Letting J be the jacobian of H we use Magma to compute that $J(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and again using the pullback of the natural embedding of $H(\mathbb{Q})$ into $J(\mathbb{Q})$ we get that

$$H(\mathbb{Q}) = \{(-3,0), (1,0), \infty_+, \infty_-\}.$$

Computing the pullback of these points through the surjective quotient map, we get that the only points in $X(\mathbb{Q})$ are the singular ones. Therefore, there are no elliptic curves with a point of order 7 and full 3-torsion defined over $\mathbb{Q}(D_4^\infty)$. □

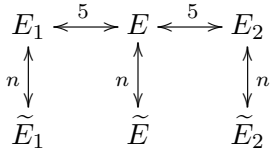
Remark 6.4. Some of these computations could have been avoided by using the modular interpretation of the quotient curves in Propositions 6.2 and 6.3. In those Propositions, the points on the curve H correspond to elliptic curves whose mod 13 (and respectively mod 7) Galois representations are Borel and the image of the mod 3 representation is contained inside of the 2-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. Since there are no such curves, there are no rational points on each H.

6.2. The case when 5 divides $\#E(\mathbb{Q}(D_4^\infty)_{\text{tors}}$.

Proposition 6.5. *Suppose that $E/\mathbb{Q}$ is an elliptic curve such that $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ contains a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$. Then $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.*

Proof. We start by remarking that Corollary 5.9 says that $E/\mathbb{Q}$ has its full 5-torsion defined over $\mathbb{Q}(D_4^\infty)$ if and only if E has two independent 5-isogenies. So first suppose towards a contradiction that E has an n-isogeny independent of its two 5-isogenies for some $n > 1$.

If this were the case, the isogeny graph of E would have to contain a subgraph of the form



where the number associated to each arrow is the degree of the isogeny. This would imply that there is a $25n$-isogeny between $\widetilde{E}_1$ and E_2, but looking at Theorem 4.4 we see that this would force n to be 1, giving us our contradiction. Thus, if E has its full 5-torsion defined over $\mathbb{Q}(D_4^\infty)$ it can't have any isogenies other than its two independent 5-isogenies.

From Corollary 6.1 the last case to rule out is that $E/\mathbb{Q}$ has its full 15-torsion defined over $\mathbb{Q}(D_4^\infty)$. To do this let j_5 and j_3 be the j-maps associated with having full 3- and 5-torsion defined over $\mathbb{Q}(D_4^\infty)$ given in Propositions 5.8 and 5.10. Next, define X to be the curve given by the affine equation $j_3(x) = j_5(y)$. This time the corresponding curve X is singular with genus 9 and while we are able to compute two separate automorphisms as before, Magma can only easily quotient by one of them at a time. After quotienting out by the first automorphism, we are left with a curve C of genus 4. In this case Magma is able to compute $\mathrm{Aut}(C)$ in a reasonable amount of time, and we get that $\mathrm{Aut}(C) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. If we quotient out by the full automorphism group of C we are left with a genus 0 curve and this is not useful. Instead, we pick a subgroup of $\mathrm{Aut}(C)$ of order 2 to quotient out by and we are left with a genus 1 elliptic curve $F/\mathbb{Q}$. The curve that Magma gives back has large coefficients (the smallest one has over 1000 digits) so it is cumbersome to work with, but with some work we are able to show that F is isomorphic to the curve with Cremona label `15a8` over $\mathbb{Q}$. The Mordel–Weil group over $\mathbb{Q}$ of `15a8` is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, and so we find a point of order 4 on F defined over $\mathbb{Q}$ and pull its multiples back through the reduction maps to see that $X(\mathbb{Q})$ only contains singular points. □

Proposition 6.6. *Suppose that $E/\mathbb{Q}$ is an elliptic curve such that the 5-primary component of $E(\mathbb{Q}(D_4^\infty))_{\mathrm{tors}}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Then the 3-primary component of $E(\mathbb{Q}(D_4^\infty))_{\mathrm{tors}}$ is either trivial or isomorphic to $\mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.*

Proof. Let E be an elliptic curve such that the 5-primary component of $E(\mathbb{Q}(D_4^\infty))_{\mathrm{tors}}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. This means that E has a rational 5-isogeny and while we expect that generically this is the only isogeny E has, it is possible that E does in fact also have a 3-isogeny. In this case, $E(\mathbb{Q}(D_4^\infty))_{\mathrm{tors}}$ will automatically contain a point of order 15. Since there are no elliptic curves with 45-isogenies, the last possibility for the 3-primary component of $E(\mathbb{Q}(D_4^\infty))_{\mathrm{tors}}$ is that it is isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Again, we start by constructing the associated modular curve using the relevant j-maps, this time getting a singular curve X that is genus 1. Finding a nonsingular model for this curve, shows that it is isomorphic over $\mathbb{Q}$ to the elliptic curve F with Cremona reference `15a3`. From [22] we see that $F(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and pulling these points back to X we get that the nonsingular points of $X(\mathbb{Q})$ are exactly

$$\{(9/2, -5/8), (9/32, -8/25), (-32/3, -8/25), (-2/3, -5/8)\}.$$

Plugging the appropriate coordinates into the corresponding j-maps, we see that there are exactly 2 elliptic curves up to $\overline{\mathbb{Q}}$-isomorphism such that $E(\mathbb{Q}(D_4^\infty))_{\mathrm{tors}}$ contains a subgroup isomorphic to

$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z}$ and they have

$$j(E) = -\frac{1680914269}{32768} \text{ or } j(E) = \frac{1331}{8}.$$

□

Proposition 6.7. *Suppose that $E/\mathbb{Q}$ is an elliptic curve such that the 5-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Then the 2-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is either trivial or isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.*

Proof. Let E be an elliptic curve such that the 5-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. This means that E has a rational 5-isogeny and if this is the only isogeny that E has, then the 2-primary component of $E(\mathbb{Q}(D_4^\infty))$ must be trivial. Inspecting Theorem 4.4, we see that it is possible that E could also have a 2-isogeny, in which case the full 4-torsion of E would be defined over $\mathbb{Q}(D_4^\infty)$. All that is left to show is that there are no curves that have a 5-isogeny and two primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ containing a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

According to Table 2, Figure 1, and [30] there are four ways that $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ can contain a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. These 4 possibilities break in to pairs. The first pair is that E comes from a points on either X_{12} or X_{13} which can be interpreted as the following two conditions:

(1) the curve E has a point of order 2 defined over $\mathbb{Q}$ and $\Delta(E) \equiv \Delta(E_2) \bmod (\mathbb{Q}^\times)^2$ where E_2 is the elliptic curve that is 2-isogenous to E, or
(2) the curve E has a 4-isogeny.

Since we are already assuming that E has a 5-isogeny, (2) cannot happen by Theorem 4.4 since there are no elliptic curves over $\mathbb{Q}$ with a 20-isogeny. Further, if E has a 5-isogeny and satisfies condition (1) then E is isomorphic to

$$E_t \colon y^2 + xy = x^3 - \frac{36(t-4)(t+1)^2t^5}{(t^2-2t-4)^2(t^2-2t+2)^2(t^2+4)(t^4-2t^3-6t^2-8t-4)}x - \frac{(t-4)(t+1)^2t^5}{(t^2-2t-4)^2(t^2-2t+2)^2+(t^2+1)(t^4-2t^3-6t^2-8t-4)}.$$

over $\mathbb{Q}(D_4^\infty)$ for some $t \in \mathbb{Q}$. This curve has discriminant

$$\Delta(E_t) = \frac{(t-4)t^5(t+1)^2(t^6-4t^5+16t+16)^6}{(t^2-2t-4)^6(t^2-2t+2)^6(t^2+4)^3(t^4-2t^3-6t^2-8t-4)^6}$$

and its 2-isogenous curve has discriminant

$$\Delta(E_{t,2}) = \frac{(t-4)^2t^{10}(t+1)(t^6-4t^5+16t+16)^6}{(t^2-2t-4)^6(t^2-2t+2)^6(t^2+4)^3(t^4-2t^3-6t^2-8t-4)^6}.$$

These two curves have discriminants in the same square class exactly when $(t+1)/(t^6-4t^5)$ is a square. Considering the curve

$$C \colon s^2 = (t+1)/(t^6-4t^5)$$

in Magma we show that C has genus 1 and exactly 1 rational point that is singular, $P = (-1, 0)$. Since the curve E_0 is singular here we have that there are no elliptic curves with a 10-isogeny whose 2-isogenous curve has the same discriminant mod squares, i.e. there are no curves with a point of order 5 over $\mathbb{Q}(D_4^\infty)$ that satisfy condition (1).

Lastly from Table 2, Figure 1, and [30] there are two ways that $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ could also correspond to a rational point on X_8 or X_{11}. These two possibilities correspond to the following two conditions:

(1) The curve E has a point of order 2 defined over $\mathbb{Q}$ and $\Delta(E) \equiv -\Delta(E_2) \bmod (\mathbb{Q}^\times)^2$ where E_2 is the elliptic curve that is 2-isogenous to E.
(2) The curve E its full 2-torsion defined over $\mathbb{Q}$.

If E has a 5-isogeny, then E cannot have its full 2-torsion defined over $\mathbb{Q}$ as this would imply the existence of an elliptic curve with a 20-isogeny. So we can rule out condition (2). To show that there are no elliptic curves with a 5-isogeny that satisfy condition (1), we proceed the same way as before, but this time we consider the curve

$$C' : \ -s^2 = (t+1)/(t^6 - 4t^5).$$

The curve C' is also genus 1 and singular and it has only one rationla points in the given affine patch which corresponds to a singluar curve. Thus condition (2) cannot occur for an elliptic curve with a 5-isogeny, completing the proof of the proposition.

□

Proposition 6.8. *Suppose that $E/\mathbb{Q}$ is an elliptic curve such that the 5-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Then $E(\mathbb{Q}(D_4^\infty))_{\text{tors}} \simeq \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z}$, or $\mathbb{Z}/4 \oplus \mathbb{Z}/20\mathbb{Z}$.*

Proof. In order to prove this proposition we simply need to show that if the 5-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is $\mathbb{Z}/5\mathbb{Z}$ and the 3-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is nontrivial, then the 2-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is trivial.

First, suppose that the 3-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is nontrivial but $E[3] \not\subseteq E(\mathbb{Q}(D_4^\infty))$. Then it must be that E has a 15-isogeny and by Theorem 4.4 this means that E cannot also have a 2-isogeny and the 2-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is trivial.

Lastly, suppose that the 3-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. From Proposition 6.6, either $j(E) = -\frac{1680914269}{32768}$ or $j(E) = \frac{1331}{8}$. Using Proposition 5.4 it is enough to check one curve with each j-invariant. Doing so in both cases shows that both curves have torsion subgroup $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z}$ over $\mathbb{Q}(D_4^\infty)$. □

6.3. **The cases when 3 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$.** The last thing that we need to determine is what are the possible 2-primary components of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ give that the 3-primary component is nontrivial. This breaks into 3 different cases that correspond to the 3 possible nontrivial 3-primary components listed in Proposition 5.10.

Proposition 6.9. *Suppose that $E/\mathbb{Q}$ is an elliptic curve such that the 3-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Then the 2-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is either trivial or isomorphic to either $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, or $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.*

Proof. From Lemma 4.3 that E must have a 3-isogeny and since we have examples of the three torsion structures listed above, all that is left to do is rule out the case where the 2-primary component of $E(\mathbb{Q}(D_4^\infty))$ contains a point of order 16. Looking at Table 2 and the data in [30] we see that in order for E to have a point of order 16 defined over $\mathbb{Q}(D_4^\infty)$ it must be that either E has an 8-isogeny or it must have a 4-isogeny and an independent 2-isogeny. In both of these cases, since E also has a 3-isogeny there would have to exist an elliptic curve (either E itself or another elliptic

curve in its isogeny class) that has a 24-isogeny. Once again thanks to Theorem 4.4 we have that this can't happen, and thus if the 3-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, then E cannot have a point of order 16 defined over $\mathbb{Q}(D_4^\infty)$. □

Proposition 6.10. *Suppose that $E/\mathbb{Q}$ is an elliptic curve such that the 3-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/9\mathbb{Z}$. Then the 2-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is trivial.*

Proof. Recall from Proposition 5.10 that E has a point of order 9-defined over $\mathbb{Q}(D_4^\infty)$ if and only if E has a quadratic twist with a point of order 9 defined over $\mathbb{Q}$. Since every quadratic extension of $\mathbb{Q}$ is contained inside of $\mathbb{Q}(D_4^\infty)$, we can assume that we are working with a model of $E/\mathbb{Q}$ such that E has a point of order 9 defined over $\mathbb{Q}$ itself. The only way that the 2-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is nontrivial is for E to have a rational point of order 2. Thus, in order for $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ to have a point of order 9 *and* nontrivial 2-primary component, it would have to be that E has a rational point of order 18, but by Theorem 1.2 this cannot happen. □

Proposition 6.11. *Suppose that $E/\mathbb{Q}$ is an elliptic curve such that the 3-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Then the 2-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is either trivial or isomorphic to either $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.*

Proof. It is sufficient to show that if E has its full 3-torsion defined over $\mathbb{Q}(D_4^\infty)$ then it can't have its full 8-torsion or a point of order 16 defined over $\mathbb{Q}(D_4^\infty)$.

Assume that E is an elliptic curve such that E has its full 3- and full 8-torsion defined over $\mathbb{Q}(D_4^\infty)$. From Proposition 5.10 and Table 2 there are two ways in which this can happen. These two possibilities correspond to two different modular curves that can be again constructed setting the two relevant j-maps equal to each other. These curves both end up begin singular curves with genus 1 and we can use Magma to show that they both only contain singular points which can only correspond to the curve with $j = 0$ or $j = 1728$. Thus giving us a contradiction.

Next, assume that E is an elliptic curve with its full 3-torsion and a point of order 16 defined over $\mathbb{Q}(D_4^\infty)$. Since we have shown that E cannot have its full 8-torsion defined over $\mathbb{Q}(D_4^\infty)$ the 2-primary component of $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ must be either $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$. Again, using the data from [30] we see that in order for this to be the case E must have an 8-isogeny. Constructing the modular curve X parametrizing elliptic curves with an 8-isogeny and full 3-torsion over $\mathbb{Q}(D_4^\infty)$, we get a genus 3 singular curve. It turns out that X is a hyperelliptic curve whose jacobian has rank 0, but since much of Magma's functionality is only implemented for genus 2 hyperelliptic curves, we take the extra step to quotient out by a subgroup of $\text{Aut}(X)$ generated by a single automorphism of order 2. The resulting quotient curve H is hyperelliptic, genus 2 and given by the equation $H\colon y^2 = x^6 + 1$. The jacobian of H again has rank 0 over $\mathbb{Q}$ and finding all the points on H in Magma and pulling them back to X, we se that $X(\mathbb{Q})$ only contains singular points and points where both j-maps are undefined. □

6.4. **When only 2 divides $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$.** When $\#E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is a nontrivial power of 2, we know from Table 2 that

$$E(\mathbb{Q}(D_4^\infty)_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2^j\mathbb{Z} & j = 2, 3, 4, 5, \text{ or} \\ \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2^j\mathbb{Z} & j = 3, 4, 5, \text{ or} \\ \mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}. \end{cases}$$

Further, the examples listed in Table 1 show that each of these possibilities does occur.

7. Parameterizations for each possible torsion structure.

Since the torsion structure of $E/\mathbb{Q}$ base-extended to $\mathbb{Q}(D_4^\infty)$ only depends on the j-invariant of E (unless $j(E)=0$) to completely parametrize when each torsion structure occurs, it is sufficient to give explicit descriptions of the sets

$$S_T = \{j(E) : E(\mathbb{Q}(D_4^\infty))_{\text{tors}} \simeq T\},$$

where T ranges over the 24 possible torsion structures determined in Section 6 and listed in Table 1. From Proposition 5.4 if $j(E)\neq 0$, then $j(E)$ is in exactly one set S_T. Further, Lemma 5.5 shows $j(E)=0$ is in 3 different sets S_T depending which rational model is chosen; namely it is in the sets S_T for $T=\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$, and $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/24\mathbb{Z}$.

We will describe each set S_T by providing sets F_T of (possibly constant) rational functions $j(t)$ which parameterize the j-invariants $j(E)$ of elliptic curves $E/\mathbb{Q}$ for which $E(\mathbb{Q}(D_4^\infty))$ contains a subgroup isomorphic to T. In order to ease notation, we will let $\mathcal{T}$ be the set of the 24 possible torsion structures for $E(\mathbb{Q}(D_4^\infty))$ and we will put a partial order on $\mathcal{T}$ given by $T_1\leq T_2$ exactly when T_2 has a subgroup isomorphic to T_1. Further, for a fixed elliptic curve $E/\mathbb{Q}$ with $j(E)\neq 0$ we let $\mathcal{T}(E)\subseteq\mathcal{T}$ be the set of groups T for which $j(E)$ is in the image of some function in F_T.

Theorem 7.1. *Let $E/\mathbb{Q}$ be an elliptic curve with $j(E)\neq 0$. Then, the set $\mathcal{T}(E)$ has a unique maximal element $T(E)$ with respect to the partial order on $\mathcal{T}$, and $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $T(E)$.*

Remark 7.2. The set $\mathcal{T}(E)$ need not contain every $T\leq T(E)$. For example, the curve `338e1` has $T(E)=\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$, but $j(E)$ is not in the image of the unique function $j(t)$ for $\mathbb{Z}/3\mathbb{Z}$ since it does not have a rational 3-isogeny.

The proof of Theorem 7.1 follows from the exact same argument that is presented in the proof of [7, Theorem 7.1] changing a few minor details. For the sake of brevity, we omit its proof here and instead finish by justifying the j-maps that appear in Table 4.

- Justification for any of the functions for a torsion structure T of the form $\mathbb{Z}/p^k\mathbb{Z}\oplus\mathbb{Z}/p^j\mathbb{Z}$, can be found in Section 5.
- $\mathbb{Z}/15\mathbb{Z}$: In section 5, we saw that in order for $E/\mathbb{Q}$ to have a point of order 3 nd not full level 3 structure or 5 defined over $\mathbb{Q}(D_4^\infty)$ it is necessary and sufficient for E to have a rational 3- or 5-isogeny respectively. Thus, $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$ is isomorphic to $\mathbb{Z}/15\mathbb{Z}$ exactly when E has a 15-isogeny and there are exatly 4 $\overline{\mathbb{Q}}$-isomorphism classes such curves. See [23, Table 4].
- $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/15\mathbb{Z}$: In Section 5 that $E/\mathbb{Q}$ has its full 3-torsion defined over $\mathbb{Q}(D_4^\infty)$ exactly when the mod 3 Galois representation associated to E has its image contained in the normalizer of a nonsplit Cartan subgroup. Thus, $\mathcal{T}(E)=\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/15\mathbb{Z}$ if and only if $\operatorname{Im}\rho_{E,3}$ is conjugate to a subgroup of the normalizer of the split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and E has a 5-isogeny. We can construct the curve X that parameterizes such elliptic curve as the fiber product of the modular curves $X_s^+(3)$ and $X_0(5)$. The resulting curve is a genus 1 singular curve whose desingularization is the elliptic curve `15a3`. The curve `15a3` has rank zero and torsion group $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ over $\mathbb{Q}$. Computing the pullback of these 8 points back to X in Magma and then applying the j-maps from X to $\mathbb{P}^1$ we see that there are only 2 possible j-invariant which are listed in Table 4.
- $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$: In Section 5 we showed that for each of these p-primary components to occur it is necessary and sufficient for E to have a rational point of order 2 and a rational

T	$j(t)$
$\{\mathcal{O}\}$	t
$\mathbb{Z}/3\mathbb{Z}$	$\frac{27(t+1)(t+9)^3}{t^3}$
$\mathbb{Z}/5\mathbb{Z}$	$\frac{5^2(t^2+10t+5)^3}{t^5}$
$\mathbb{Z}/7\mathbb{Z}$	$\frac{(t^2-t+1)^3(t^3-8t^2+5t+1)(t^6-11t^5+30t^4-15t^3-10t^2+5t+1)^3}{(t-1)^7t^6}$
$\mathbb{Z}/9\mathbb{Z}$	$\frac{(t^3-3t^2+1)^3(t^9-9t^8+27t^7-48t^6+54t^5-45t^4+27t^3-9t^2+1)^3}{(t-1)^9t^9(t^2-t+1)^2(t^3-6t^2+3t+1)}$
$\mathbb{Z}/13\mathbb{Z}$	$\frac{(t^2-t+1)^3(t^{12}-9t^{11}+29t^{10}-40t^9+22t^8-16t^7+40t^6-22t^5-23t^4+25t^3-4t^2-3t+1)^3}{(t-1)^{13}t^{13}(t^3-4t^2+t+1)}$
$\mathbb{Z}/15\mathbb{Z}$	$\{-\frac{25}{2}, -\frac{349938025}{8}, -\frac{121945}{32}, \frac{46969655}{32768}\}$
$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$	$\frac{27(t+1)^3(t-3)^3}{t^3}$
$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/15\mathbb{Z}$	$\{-\frac{1680914269}{32768}, \frac{1331}{8}\}$
$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	$\frac{t^3}{t+16}$
$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$	$\frac{(t^2+16)^3}{t^2}, \frac{(t^2-48)^3}{(t-8)(t+8)}$
$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$	$\frac{(t+6)^3(t^3+18t^2+84t+23)^2}{t(t+8)^3(t+9)^2}$
$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z}$	$\frac{(t^4-16t^2+16)^3}{(t-4)t^2(t+4)}$
$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/20\mathbb{Z}$	$\frac{(t^6-4t^5+16t+16)^3}{(t+1)^2(t-4)t^5}$
$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/24\mathbb{Z}$	$\frac{(t^2-3)^3(t^6-9t^4+3t^2-3)^3}{t^4(t^2-9)(t^2-1)^3}$
$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/32\mathbb{Z}$	$\frac{(t^{16}-8t^{14}+12t^{12}+8t^{10}-10t^8+8t^6+12t^4-8t^2+1)^3}{(t-1)^4t^{16}(t+1)^4(t^2-2t-1)(t^2+1)^2(t^2+2t-1)}$
$\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}$	$\frac{(t^2+5t+5)^3(t^4+5t^2+25)^3(t^4+5t^3+20t^2+25t+25)^3}{t^5(t^4+5t^3+15t^2+25t+25)^5}$
$\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$	$\frac{(t^2+3)^3}{(t-1)^2(t+1)^2}, \frac{(t-4)^3(t+4)^3}{t^2}$
$\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z}$	$\frac{(t^4-8t^3+2t^2+8t+1)^3(t^4+8t^3+2t^2-8t+1)^3}{(t-1)^2t^2(t+1)^2(t^2+1)^8}$
$\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/24\mathbb{Z}$	$\frac{(t^2-6t+21)^3(t^6-18t^5+75t^4+180t^3-825t^2-2178t+6861)^3}{(t-9)^2(t-5)^6(t-3)^2(t-1)^6(t+3)^2}$
$\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/32\mathbb{Z}$	$\frac{(65536t^{16}-131072t^{14}+49152t^{12}+8192t^{10}+58880t^8+512t^6+192t^4-32t^2+1)^3}{256t^8(2t-1)^8(2t+1)^8(4t^2-4t-1)^2(4t^2+1)^4(4t^2+4t-1)^2}$
$\mathbb{Z}/12\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$	$\frac{(t^3-15t^2-33t+955)^3(t^3-15t^2+75t-233)^3}{729(t-11)^3(t-8)^6(t+1)^3}$
$\mathbb{Z}/12\mathbb{Z}\oplus\mathbb{Z}/24\mathbb{Z}$	$\{8000\}$
$\mathbb{Z}/16\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z}$	$\frac{(t^4-2t^3+2t^2+2t+1)^3(t^4+2t^3+2t^2-2t+1)^3}{(t-1)^4t^4(t+1)^4(t^2+1)^4}$

TABLE 4. Parameterizations $j(t)$ of the $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$ according to isomorphism type of $E(\mathbb{Q}(D_4^\infty))_{\mathrm{tors}}$.

3-isogeny. This is the same as saying that E has a rational 6-isogeny since having a point of order 2 is equivalent to have a 2-isogeny. These curves are parameterized by the genus zero curve $X_0(6)$ whose j-map has been taken from [23, Table 3].

- $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/20\mathbb{Z}$: As in the previous case, Section 5 shows that these two p-primary components occur exactly when E has a rational point of order 2 and a 5-isogeny. Again, this is equivalent to $E/\mathbb{Q}$ having a 10-isogeny and such curves are parameterized by $X_0(10)$ whose j-map is taken from [23, Table 3].
- $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$: This time there are 2 possible ways for this torsion structure to occur and both of them require that E has a 3-isogeny. The two possibilities correspond to the two distinct ways for E to have 2-primary component $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ (see Table 2).
  - The first possibility is that E has a 2-isogeny and that the discriminant of E is equivalent to the discriminant of the 2-isogenous curve modulo squares. Starting with a generic elliptic curve with a 6-isogeny in Magma and computing the 2-isogenous curve we see that there are no elliptic curves over $\mathbb{Q}$ with a 6-isogeny such that its discriminant is equivalent to that of its two isogenous curve modulo squares.
  - The second possibility is that E has a 4-isogeny. Combining this with a 3-isogeny, E has torsion structure $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$ if and only if E has a 12-isogeny. Again these curves are parameterized by the genus 0 modular curve $X_0(12)$ whose j-map is taken from [23, Table 3].
- $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$: Again, there are two distinct ways that E can have its full 8-torsion defined over $\mathbb{Q}(D_4^\infty)$ (see Table 2) so this breaks into two distinct cases.
  - The first possibility is that E has a 2-isogeny and the discriminant of E is equivalent to the *negative* of the discriminant of its two isogenous curve. Just as before, we start with a generic elliptic curve with a 6-isogeny and see that it is impossible for such an elliptic curve to be defined over $\mathbb{Q}$.
  - The second possibility is that E has its full 2-torsion defined over $\mathbb{Q}$. In this case, any twist of E also will have its full 2-torsion defined over $\mathbb{Q}$ and since any elliptic curve with a 3-isogeny has a quadratic twist with a rational point of order 3, we see that in this case E must have a quadratic twist with torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. These curves have been completely parametrized and the j-map has been taken from [24, Figure 2].
- $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$: This can only occur if E has a point of order 2 defined over $\mathbb{Q}$ and E is nonsplit at 3. Constructing the modular curve X that parameterizes such elliptic curves by considering the fiber product of the genus 0 modular curves $X_1(2)$ and $X_s^+(3)$ we see that the resulting curve has genus 0. The j-map of this curve is computed using Magma.
- $\mathbb{Z}/12\mathbb{Z}\oplus\mathbb{Z}/24\mathbb{Z}$: Once again there are two cases to consider corresponding to the two distinct ways that E can have 2-primary component $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Constructing the fiber product of the two corresponding curves with $X_{ns}^+(3)$ we get two different genus 1 modular curves. In total, these two curves only contain 1 nonsingular and noncuspidal point defined over $\mathbb{Q}$. This point corresponds to the elliptic curve with $j = 8000$.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symolic Comput., **24** (1997), 235–265. 1

[2] M. Chou, *Torsion of rational elliptic curves over quartic Galois number fields*, J. Number Theory **160** (2016), 603-628. 5.3, 5.3

[3] M. Chou, *Torsion of rational elliptic curves over the maximal abelian extension of Q*, preprint, available at https://arxiv.org/abs/1711.00412. 1

[4] J. E. Cremona, *Elliptic curve data*, database available at http://homepages.warwick.ac.uk/~masgaj/ftp/data/. 1

[5] H. B. Daniels, Magma scripts related to *Torsion subgroups of rational elliptic curves over the compositum of all D_4 extensions of the rational numbers*, available at http://hdaniels.people.amherst.edu 1

[6] H. Daniels, Á. Lozano-Robledo, J. Morrow, F. Najman, and A.V. Sutherland, Magma scripts related to *Torsion subgroups of rational elliptic curves over the compositum of all cubic fields*, available at http://math.mit.edu/~drew.

[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), pp. 425-458. 1.8, 1, 2, 4.2, 4.3, 4.5, 7

[8] Y. Fujita, *Torsion subgroups of elliptic curves with non-cyclic torsion over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$,* Acta Arith. **115** (2004), 29–45. 1.7

[9] Y. Fujita, *Torsion subgroups of elliptic curves in elementary abelian 2-extensions of $\mathbb{Q}$*, J. Number Theory **114** (2005), 124-134. 1.7

[10] I. Gal, R. Grizzard, *On the compositum of all degree d extensions of a number field*, J. Théor. Nombres Bordeaux. **26** (2014), 655–672. 1, 1, 1.9

[11] V. V. Ishkhanov, B.B. Lure, D.K. Faddeev, *The embedding problem in Galois theory*, Translations of Mathematical Monographs, 165. American Mathematical Society, Providence, RI, 1997. 1

[12] D. Jeon, C. H. Kim, Y. Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), 579–591. 1

[13] D. Jeon, C. H. Kim, A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), 291–301. 1

[14] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229. 1.3

[15] M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), 21–23. 4.4

[16] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20. 4.4

[17] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), 239–244. 4.4

[18] M. A. Kenku, *The modular curve $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) **23** (1981), 415–427. 4.4

[19] G. Malle, B. H. Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999. 1

[20] M. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. 1.3

[21] M. Laska and M. Lorenz, *Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$*, J. Reine Angew. Math. **355** (1985), 163–172. 1.7

[22] LMFDB Collaboration, *The L-functions and modular forms database*, available at http://www.lmfdb.org. 1, 6.2

[23] Á. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), 279–305. 4.6, 5, 5.4, 6.1, 7

[24] Á. Lozano-Robledo, *Elliptic curves, modular forms, and their L-functions*, American Mathematical Society, Providence, Rhode Island, 2010. 7

[25] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Letters, 23 (2016) 245-272. 1.4, 1.5

[26] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, Explicit methods in number theory 99117 Panor. Synthèses 36 Soc. Math. France, Paris 2012.

[27] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186. 1.2

[28] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162. 4.4

[29] L. Merel, *Bornes pour la torsions des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449. 1

[30] J. Rouse, D. Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Research in Number Theory **1** (2015), 34 pages. 1, 5.5, 5.5, 6.2, 6.2, 6.3, 6.3

[31] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331. 2

[32] J.-P. Serre, *Topics in Galois theory*, Second edition, Research Notes in Mathematics, 1. A K Peters, Ltd., Wellesley, MA, 2008. 1

[33] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 2nd Edition, New York, 2009. 4.1, 5

[34] A. V. Sutherland and D. Zywina, *Modular curves of prime power level with infinitely many rational points*, Algebra and Number Theory 11 (2017), 1199-1229. 1, 5.4

[35] D. Zywina, *On the possible images of mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, preprint, available at http://arxiv.org/abs/1508.07660. 1, 5.1, 5.2, 5.3, 5.4

Department of Mathematics and Statistics, Amherst College, Amherst, MA 01002, USA
E-mail address: hdaniels@amherst.edu
URL: http://hdaniels.people.amherst.edu