2-ADIC GALOIS IMAGES OF ISOGENY-TORSION GRAPHS OVER $\mathbb{Q}$ WITH CM

GAREN CHILOYAN

Abstract. Let $\mathcal{E}$ be a $\mathbb{Q}$-isogeny class of elliptic curves defined over $\mathbb{Q}$. The isogeny graph associated to $\mathcal{E}$ is a graph which has a vertex for each elliptic curve over $\mathbb{Q}$ of $\mathcal{E}$ and an edge for each $\mathbb{Q}$-isogeny of prime degree that maps one elliptic curve in $\mathcal{E}$ to another elliptic curve in $\mathcal{E}$, with the degree of the isogeny recorded as a label of the edge. The isogeny-torsion graph associated to $\mathcal{E}$ is the isogeny graph associated to $\mathcal{E}$ where, in addition, we label each vertex with the abstract group structure of the torsion subgroup over $\mathbb{Q}$ of the corresponding elliptic curve. The main result of the article is a classification of the 2-adic Galois image at each vertex of the isogeny-torsion graphs whose associated $\mathbb{Q}$-isogeny class consists of elliptic curves over $\mathbb{Q}$ with complex multiplication.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. It is well known that $E$ has the structure of an abelian group with group identity which we will denote $O$. By the Mordell–Weil theorem, the set of points on $E$ defined over $\mathbb{Q}$, denoted $E(\mathbb{Q})$ has the structure of a finitely generated abelian group. Thus, the set of points on $E$ defined over $\mathbb{Q}$ of finite order, denoted $E(\mathbb{Q})_{\text{tors}}$ is a finite, abelian group. By Mazur’s theorem, $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of fifteen groups (see Theorem 2.4). Moreover, these fifteen groups occur infinitely often. Let $E'/\mathbb{Q}$ be an elliptic curve. An isogeny mapping $E$ to $E'$ is a rational morphism $\phi: E \to E'$ such that $\phi$ maps the identity of $E$ to the identity of $E'$. If there is a non-constant isogeny defined over $\mathbb{Q}$, mapping $E$ to $E'$, we say that $E$ is $\mathbb{Q}$-isogenous to $E'$. This relation is an equivalence relation and the set of elliptic curves defined over $\mathbb{Q}$ that are $\mathbb{Q}$-isogenous to $E$ is called the $\mathbb{Q}$-isogeny class of $E$.

An isogeny is a group homomorphism and the kernel of a non-constant isogeny is finite. We are particularly interested in non-constant isogenies with cyclic kernels. The isogeny graph associated to the $\mathbb{Q}$-isogeny class of $E$ is a visual description of the $\mathbb{Q}$-isogeny class of $E$. Denote the $\mathbb{Q}$-isogeny class of $E$ by $\mathcal{E}$. The isogeny graph associated to $\mathcal{E}$ is a graph which has a vertex for each elliptic curve in $\mathcal{E}$ and an edge for each $\mathbb{Q}$-isogeny of prime degree that maps one elliptic curve in $\mathcal{E}$ to another elliptic curve in $\mathcal{E}$, with the degree recorded as a label of the edge. The isogeny-torsion graph associated to $\mathcal{E}$ is the isogeny graph associated to $\mathcal{E}$ where, in addition, we label each vertex with the abstract group structure of the torsion subgroup over $\mathbb{Q}$ of the corresponding elliptic curve.

Example 1.1. There are four elliptic curves in the $\mathbb{Q}$-isogeny class with LMFDB label 27.a which we will denote $E_1$, $E_2$, $E_3$, and $E_4$. The isogeny graph associated to 27.a is above and the isogeny-torsion graph associated to 27.a is below.

\[
\begin{align*}
E_1 & \xrightarrow{3} E_2 \xrightarrow{3} E_3 \xrightarrow{3} E_4 \\
\mathbb{Z}/3\mathbb{Z} & \xrightarrow{3} \mathbb{Z}/3\mathbb{Z} \xrightarrow{3} \mathbb{Z}/3\mathbb{Z} \xrightarrow{3} O
\end{align*}
\]

A proof classifying the isogeny graphs associated to $\mathbb{Q}$-isogeny classes of elliptic curves over $\mathbb{Q}$ appears in Section 6 of [3].

Theorem 1.2. There are 26 isomorphism types of isogeny graphs that are associated to $\mathbb{Q}$-isogeny classes of elliptic curves defined over $\mathbb{Q}$. More precisely, there are 16 types of (linear) $L_k$ graphs of $k = 1$–4 vertices.
3 types of (nonlinear two-primary torsion) $T_k$ graphs of $k = 4, 6, \text{ or } 8$ vertices, 6 types of (rectangular) $R_k$ graphs of $k = 4$ or 6 vertices, and 1 (special) $S$ graph (see Tables 1-4 in [3]).

The isogeny class degree of $E$ is the least common multiple of the degrees of all cyclic, $\mathbb{Q}$-rational isogenies mapping elliptic curves over $\mathbb{Q}$ in $E$ to elliptic curves over $\mathbb{Q}$ in $E$. In other words, the isogeny class degree of $E$ is equal to the greatest degree of a cyclic, $\mathbb{Q}$-rational isogeny that maps an elliptic curve in $E$ to an elliptic curve in $E$. For example, if $E$ is of $L_4$ type, the isogeny class of $E$ is equal to 27.

In the case of an isogeny graph of $L_2$, $L_3$, or $R_4$ type, the isogeny class degree of the $\mathbb{Q}$-isogeny class is written in parentheses to distinguish it from other isogeny-torsion graphs of the same size and shape, but with different isogeny class degree. For example, there are $L_2(2)$ graphs; graphs of $L_2$ type generated by an isogeny of degree 2 and there are $L_2(3)$ graphs; isogeny graphs of $L_2$ type generated by an isogeny of degree 3. Relying only on the size and shape of isogeny graphs of $L_2$ type is not enough to distinguish isogeny graphs of $L_2(2)$ type from isogeny graphs of $L_2(3)$ type. On the other hand, the isogeny-torsion graph of $L_4$ type is the only linear isogeny-torsion graph with four vertices and it is not necessary to designate the isogeny class degree in parentheses to distinguish it from other isogeny-torsion graphs. The main theorem in [3] was the classification of isogeny-torsion graphs associated to $\mathbb{Q}$-isogeny classes of elliptic curves over $\mathbb{Q}$.

**Theorem 1.3** (Chiloyan, Lozano-Robledo, [3]). There are 52 isomorphism types of isogeny-torsion graphs that are associated to $\mathbb{Q}$-isogeny classes of elliptic curves defined over $\mathbb{Q}$. In particular, there are 23 isogeny-torsion graphs of $L_k$ type, 13 isogeny-torsion graphs of $T_k$ type, 12 isogeny-torsion graphs of $R_k$ type, and 4 isogeny-torsion graphs of $S$ type.

We denote the cyclic group of order $a$ as $[a]$ and for $b = 1-4$, we denote the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2 \cdot b\mathbb{Z}$ as $[2,b]$. We organize torsion configuration of isogeny-torsion graphs in “vector-group” formation corresponding to the enumeration of the elliptic curves in the isogeny-torsion graph. For example, reconsider the $\mathbb{Q}$-isogeny class with LMFDB label 27.a and its associated isogeny graph and isogeny-torsion graph, $\mathcal{G}$.

$$
\begin{array}{cccc}
E_1 & 3 & E_2 & 3 \\
\mathbb{Z}/3\mathbb{Z} & & \mathbb{Z}/3\mathbb{Z} & 3 \\
E_3 & 3 & E_4 & 3 \\
\mathcal{O} & & & \\
\end{array}
$$

Then we will denote the torsion configuration of $\mathcal{G}$ as $([3],[3],[3],[1])$. For another case, consider the $\mathbb{Q}$-isogeny class $E$ with LMFDB label 17.a. Then the isogeny graph of $E$ is below on the left and the isogeny-torsion graph of $E$ is below on the right.

$$
\begin{array}{cccc}
E_1 & 2 & E_2 & Z/4\mathbb{Z} \\
\mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z} & 2 & \mathbb{Z}/2\mathbb{Z} \\
E_3 & 2 & E_4 & 2 \\
\mathbb{Z}/2\mathbb{Z} & & & \\
\end{array}
$$

We denote the torsion classification of $\mathcal{G}$ to be $([2,2],[4],[4],[2])$.

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication (CM) and denote the $\mathbb{Q}$-isogeny class of $E$ by $\mathcal{E}$ and the isogeny-torsion graph associated to $\mathcal{E}$ by $\mathcal{G}$. Then all elliptic curves over $\mathbb{Q}$ in $\mathcal{E}$ have CM. Thus, it is natural to say that $\mathcal{E}$ and $\mathcal{G}$ are defined over $\mathbb{Q}$ and have CM. Moreover, it is natural to say that the classification of the 2-adic Galois image of each of the vertices of $\mathcal{G}$ would classify the 2-adic Galois image of $\mathcal{G}$. The isogeny-torsion graph, $\mathcal{G}$ is of $L_2(p)$, $L_4$, $T_4$, $R_4(6)$, or $R_4(14)$ type, where $p \in \{2,3,11,19,43,67,163\}$. Table 1 classifies the isogeny-torsion graphs with CM. This same table appears as Table 5 in Section 4 of [3].
| $d_K$ | $j$ | Type | Torsion config. | LMFDB |
|------|-----|------|----------------|-------|
| 0    | $y^2 = x^3 + t^3, t = -3, 1$ | $R_4(6)$ | ([6], [6], [2], [2]) | 36.a4 |
|      | $y^2 = x^3 + t^3, t \neq -3, 1$ | $R_4(6)$ | ([2], [2], [2], [2]) | 144.a3 |
|      | $y^2 = x^3 + 16t^3, t = -3, 1$ | $L_4$ | ([3], [3], [3], [1]) | 27.a3 |
|      | $y^2 = x^3 + 16t^3, t \neq -3, 1$ | $L_4$ | ([1], [1], [1], [1]) | 432.e3 |
|      | $y^2 = x^3 + s^2, s^2 \neq t^3, 16t^3$ | $L_2(3)$ | ([3], [1]) | 108.a2 |
|      | $y^2 = x^3 + s, s \neq t^3, 16t^3$ | $L_2(3)$ | ([1], [1]) | 225.e1 |
| 54000 | $y^2 = x^3 - 15t^2x + 22t^3, t = 1, 3$ | $R_4(6)$ | ([6], [6], [2], [2]) | 36.a1 |
|      | $y^2 = x^3 - 15t^2x + 22t^3, t \neq 1, 3$ | $R_4(6)$ | ([2], [2], [2], [2]) | 144.a1 |
| −12288000 | $E^t, t = -3, 1$ | $L_4$ | ([3], [3], [3], [1]) | 27.a2 |
|      | $E^t, t \neq -3, 1$ | $L_4$ | ([1], [1], [1], [1]) | 432.e1 |
| 1728  | $y^2 = x^3 + tx, t = -1, 4$ | $T_4$ | ([2], [4], [4], [2]) | 32.a3 |
|      | $y^2 = x^3 + tx, t = -4, 1$ | $T_4$ | ([2], [4], [2], [2]) | 64.a3 |
|      | $y^2 = x^3 \pm t^2x, t \neq 1, 2$ | $T_4$ | ([2], [2], [2], [2]) | 288.d3 |
|      | $y^2 = x^3 \pm sx, s \neq \pm t^2$ | $L_2(2)$ | ([2], [2]) | 256.b1 |
| 287496 | $y^2 = x^3 - 11t^2x + 14t^3, t = \pm 1$ | $T_4$ | ([2], [4], [4], [2]) | 32.a2 |
|      | $y^2 = x^3 - 11t^2x + 14t^3, t = \pm 2$ | $T_4$ | ([2], [4], [2], [2]) | 64.a1 |
|      | $y^2 = x^3 - 11t^2x + 14t^3, t \neq \pm 1, \pm 2$ | $T_4$ | ([2], [2], [2], [2]) | 288.d1 |
| −7    | $-3375$ | $R_4(14)$ | ([2], [2], [2], [2]) | 49.a2 |
|      | 16581375 | | ([2], [2], [2], [2]) | 49.a1 |
| −8    | 8000 | $L_2(2)$ | ([2], [2]) | 256.a1 |
| −11   | −32768 | $L_2(11)$ | ([1], [1]) | 121.b1 |
| −19   | −884736 | $L_2(19)$ | ([1], [1]) | 361.a1 |
| −43   | −884736000 | $L_2(43)$ | ([1], [1]) | 1849.b1 |
| −67   | −147197952000 | $L_2(67)$ | ([1], [1]) | 4489.b1 |
| −163  | −262537412640768000 | $L_2(163)$ | ([1], [1]) | 26569.a1 |

Table 1. The list of rational $j$-invariants with CM and the possible isogeny-torsion graphs that occur, where $E^t$ denotes the curve $y^2 = x^3 - 38880t^2x + 2950992t^3$. 
Example 1.4. Let $E/\mathbb{Q}$ be an elliptic curve such that the isogeny graph associated to the $\mathbb{Q}$-isogeny class of $E$ is of $L_4$ type. Then $E$ is represented by one of the elliptic curves $E_1$, $E_2$, $E_3$, or $E_4$ in the isogeny graph below.

$$
E_1 \xrightarrow{3} E_2 \xrightarrow{3} E_3 \xrightarrow{3} E_4
$$

No matter the torsion configuration of the isogeny-torsion graph, $\rho_{E,2\infty}(G_{\mathbb{Q}})$ is conjugate to the group

$$
\left\langle \begin{bmatrix} -\text{Id} & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 7 & 4 & 3 \\ 4 & 7 & 3 \\ 3 & 3 & 7 \end{bmatrix}, \begin{bmatrix} 3 & 6 & 6 \\ 6 & 3 & 6 \\ 6 & 6 & 3 \end{bmatrix} \right\rangle \subseteq \text{GL}(2,\mathbb{Z}_2).
$$

The reason why the $2$-adic Galois image of all elliptic curves in an $L_4$ graph are conjugate comes from the fact that $3$ is odd (see Corollary 2.21). The situation will not always be as seamless as this. When there are non-trivial, cyclic isogenies of $2$-power degree in the isogeny graph, it is likely the $2$-adic Galois image of the vertices are different.

Let $\delta$, $\phi$, and $N$ be integers such that $N \geq 0$. Denote the subgroup of $\text{GL}(2,\mathbb{Z}/2^N\mathbb{Z})$ of matrices of the form

$$
\begin{bmatrix}
  a + b \cdot \phi & b \\
  \delta \cdot b & a
\end{bmatrix}
$$

by $C_{\delta,\phi}(2^N)$ and let $\mathcal{N}_{\delta,\phi}(2^N) = \left\langle C_{\delta,\phi}(2^N), \begin{bmatrix} -1 & 0 \\ \phi & 1 \end{bmatrix} \right\rangle$. Finally, let $\mathcal{N}_{\delta,\phi}(2^\infty) = \lim \left\langle C_{\delta,\phi}(N) \right\rangle$.

Example 1.5. Let $E/\mathbb{Q}$ be an elliptic curve such that the isogeny graph associated to the $\mathbb{Q}$-isogeny class of $E$ is of $R_4(14)$ type (see below).

$$
\begin{array}{c|c|c}
E_1 & E_2 \\
7 & 7
\end{array}
\begin{array}{c|c|c}
E_3 & E_4 \\
2 & 2
\end{array}
$$

If $E$ is represented by $E_1$ or $E_3$, then $\rho_{E,2\infty}(G_{\mathbb{Q}})$ is conjugate to $\mathcal{N}_{-7,0}(2^\infty)$ and if $E$ is represented by $E_2$ or $E_4$, then $\rho_{E,2\infty}(G_{\mathbb{Q}})$ is conjugate to $\mathcal{N}_{-7,1}(2^\infty)$.

Section 2 will be devoted to going over background and some lemmas, Section 3 will be devoted to going over work by Lozano-Robledo in classifying the $2$-adic Galois image of elliptic curves defined over $\mathbb{Q}$ with complex multiplication and Section 4 will have the proof of Proposition 1.6 and will fully classify the $2$-adic Galois image attached to isogeny-torsion graphs defined over $\mathbb{Q}$ with complex multiplication. The proof will be broken up into many steps, appealing to isogeny graphs and $j$-invariants.

Proposition 1.6. Let $\mathcal{G}$ be a CM isogeny-torsion graph defined over $\mathbb{Q}$. Then $\mathcal{G}$ fits into Table 2 or Table 3 with the given classification of the corresponding $2$-adic Galois image of its vertices. Examples of the possible CM isogeny-torsion graphs with the given $2$-adic Galois image classification are provided in the final column of each table.
Acknowledgements. The author would like to express his gratitude to Álvaro Lozano-Robledo for many helpful conversations about this topic and providing invaluable code to help with computations.
2. Background and Some Lemmas

2.1. Elliptic curves, isogeny graphs, and isogeny-torsion graphs. Let \( E/\mathbb{Q} \) be an elliptic curve. Then \( E \) has the structure of an abelian group. Let \( N \) be a positive integer. The set of points on \( E \) of order dividing \( N \) with coordinates in \( \overline{\mathbb{Q}} \) is a group, denoted \( E[N] \) and is isomorphic to \( \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \). An element of \( E[N] \) is called an \( N \)-torsion point. Let \( E/\mathbb{Q} \) and \( E'/\mathbb{Q} \) be elliptic curves. An isogeny mapping \( E \) to \( E' \) is a non-constant morphism \( \phi: E \to E' \) that maps the identity of \( E \) to the identity of \( E' \). An isogeny is a group homomorphism with a kernel of finite order. The degree of an isogeny agrees with the order of its kernel.

Let \( M \) be an integer and let \( [M]: E \to E \) be the map such that

\[
\begin{cases}
[M](P) = P + \ldots + P & M \geq 1 \\
[M](P) = -P + \ldots + -P & M \leq -1 \\
[M](P) = \mathcal{O} & M = 0
\end{cases}
\]

We call the map \([M]\) the multiplication-by-\( M \) map. The endomorphism ring of \( E \) is the set of all isogenies mapping \( E \) to \( E \), denoted, \( \text{End}(E) \). All of the multiplication-by-\( M \) maps are elements of \( \text{End}(E) \). If \( \text{End}(E) \) consists solely of the multiplication-by-\( M \) maps, then \( \text{End}(E) \) is ring-isomorphic to \( \mathbb{Z} \) and \( E \) is said to not have complex multiplication (CM). Otherwise, \( E \) has CM and \( \text{End}(E) \) is isomorphic as a ring to an order in a quadratic field.

Example 2.1. Let \( E \) be the elliptic curve with LMFDB label 11.a1. Then \( E \) does not have CM. In other words, \( \text{End}(E) \cong \mathbb{Z} \).

Example 2.2. Let \( E \) be the elliptic curve \( y^2 = x^3 - x \). Consider the isogeny \([i]: E \to E\) that maps \( \mathcal{O} \to \mathcal{O} \) and maps a point \((a, b)\) in \( E \) to the point \((-a, ib)\). Thus, \([i]\) maps non-zero points on \( E \) to non-zero points on \( E \) and hence, the degree of \([i]\) is equal to 1. As \([i]\) is not equal to the identity or inversion maps, \([i]\) is an endomorphism of \( E \) that is not a multiplication-by-\( M \) map. Hence, \( E \) has CM and \( \text{End}(E) = \mathbb{Z} + [i] \cdot \mathbb{Z} \cong \mathbb{Z}[i] \). Note that \( i \in \mathbb{Z} + [i] \cdot \mathbb{Z} \) designates the map \([i]\) and the \( i \) in \( \mathbb{Z}[i] \) designates a root of \( x^2 + 1 \).

Let \( E/\mathbb{Q} \) be a homogenized elliptic curve. The group \( G_\mathbb{Q} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) has a natural action on \( E[N] \) for all positive integers \( N \); for each \([a, b, c] \in E \) and each \( \sigma \in G_\mathbb{Q} \), we have

\[
\sigma : [a, b, c] = [\sigma(a), \sigma(b), \sigma(c)].
\]

From this action, we have the mod-\( N \) Galois representation attached to \( E \):

\[
\overline{\rho}_{E,N}: G_\mathbb{Q} \to \text{Aut}(E[N]).
\]

After identifying \( E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \) and fixing a set of (two) generators of \( E[N] \), we may consider the mod-\( N \) Galois representation attached to \( E \) as

\[
\overline{\rho}_{E,N}: G_\mathbb{Q} \to \text{GL}(2, \mathbb{Z}/N\mathbb{Z}).
\]

Let \( \ell \) be a prime and denote \( \rho_{E,\ell} \ast (G_\mathbb{Q}) = \lim \overline{\rho}_{E,\ell N}(G_\mathbb{Q}) \). In particular, the group \( \rho_{E,2} \ast (G_\mathbb{Q}) \) is the main focus of this paper. Let \( u \) be an element of \((\mathbb{Z}/N\mathbb{Z})^\times\). By the properties of the Weil pairing, there exists an element of \( \overline{\rho}_{E,N}(G_\mathbb{Q}) \) whose determinant is equal to \( u \). Moreover, \( \overline{\rho}_{E,N}(G_\mathbb{Q}) \) has an element that behaves like complex conjugation.

Definition 2.3. Let \( E/\mathbb{Q} \) be a (homogenized) elliptic curve. A point \( P \) on \( E \) is said to be defined over \( \mathbb{Q} \) if \( P = [a : b : c] \) for some \( a, b, c \in \mathbb{Q} \).

The set of all points on \( E \) defined over \( \mathbb{Q} \) is denoted \( E(\mathbb{Q}) \). By the Mordell–Weil theorem, \( E(\mathbb{Q}) \) has the structure of a finitely-generated abelian group. Let \( E(\mathbb{Q})_{\text{tors}} \) denote the set of points on \( E \) defined over \( \mathbb{Q} \) of finite order.
Theorem 2.4 (Mazur [6]). Let $E/\mathbb{Q}$ be an elliptic curve. Then

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

Moreover, each of the fifteen torsion subgroups occur for infinitely many $j$-invariants. We now move on to the possible isogenies with finite, cyclic kernel.

Definition 2.5. Let $E/\mathbb{Q}$ be an elliptic curve. A subgroup $H$ of $E$ of finite order is said to be $\mathbb{Q}$-rational if $\sigma(H) = H$ for all $\sigma \in G_\mathbb{Q}$.

Remark 2.6. Note that for an elliptic curve $E/\mathbb{Q}$, a group generated by a point $P$ on $E$ defined over $\mathbb{Q}$ of finite order is certainly a $\mathbb{Q}$-rational group but in general, the elements of a $\mathbb{Q}$-rational subgroup of $E$ need not be fixed by $G_\mathbb{Q}$. For example, $E[3]$ is a $\mathbb{Q}$-rational subgroup of $E$ of order 9 and $G_\mathbb{Q}$ fixes one or three of the nine elements of $E[3]$ by Theorem 2.4.

Lemma 2.7 ([III.4.12, [8]]). Let $E/\mathbb{Q}$ be an elliptic curve. Then for each finite, cyclic, $\mathbb{Q}$-rational subgroup $H$ of $E$, there is a unique elliptic curve defined over $\mathbb{Q}$ up to isomorphism denoted $E/H$, and an isogeny $\phi_H : E \to E/H$ with kernel $H$.

Remark 2.8. Note that it is only the elliptic curve $E/H$ that is unique (up to isomorphism) but the isogeny $\phi_H$ is not necessarily unique. For any isogeny $\phi$, the isogeny $-\phi$ has the same domain, codomain, and kernel as $\phi$. Moreover, for any positive integer $N$, $\phi$ and $[N]\circ\phi$ have the same domain and codomain. This is why the bijection in Lemma 2.7 is with cyclic, $\mathbb{Q}$-rational subgroups instead of with all $\mathbb{Q}$-rational subgroups.

The $\mathbb{Q}$-rational points on the modular curves $X_0(N)$ have been described completely in the literature, for all $N \geq 1$. One of the most important milestones in the classification was [6], where Mazur dealt with the case when $N$ is prime. The complete classification of $\mathbb{Q}$-rational points on $X_0(N)$, for any $N$, was completed due to work by Fricke, Kenku, Klein, Kubert, Ligozat, Mazur and Ogg, among others (see the summary tables in [5]).

Theorem 2.9. Let $N \geq 2$ be a number such that $X_0(N)$ has a non-cuspidal $\mathbb{Q}$-rational point. Then:

1. $N \leq 10$, or $N = 12, 13, 16, 18$ or 25. In this case $X_0(N)$ is a curve of genus 0 and its $\mathbb{Q}$-rational points form an infinite 1-parameter family, or
2. $N = 11, 14, 15, 17, 19, 21,$ or 27. In this case $X_0(N)$ is a curve of genus 1, i.e., $X_0(N)$ is an elliptic curve over $\mathbb{Q}$, but in all cases the Mordell-Weil group $X_0(N)(\mathbb{Q})$ is finite, or
3. $N = 37, 43, 67$ or 163. In this case $X_0(N)$ is a curve of genus $\geq 2$ and (by Faltings’ theorem) there are only finitely many $\mathbb{Q}$-rational points, which are known explicitly.

Definition 2.10. Let $E/\mathbb{Q}$ be an elliptic curve. We define $C(E)$ as the number of finite, cyclic, $\mathbb{Q}$-rational subgroups of $E$ (including the trivial subgroup), and we define $C_p(E)$ similarly to $C(E)$ but only counting cyclic, $\mathbb{Q}$-rational subgroups of order a power of $p$ (like in the definition of $C(E)$, this includes the trivial subgroup), for each prime $p$.

Notice that it follows from the definition that $C(E) = \prod_p C_p(E)$.

Theorem 2.11 (Kenku, [4]). There are at most eight $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class. More concretely, let $E/\mathbb{Q}$ be an elliptic curve, then $C(E) = \prod_p C_p(E) \leq 8$. Moreover, each factor $C_p(E)$ is bounded as follows:

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

Moreover:
The best way to visualize the elliptic curves defined over \( \mathbb{Q} \) is to use its associated isogeny graph.

**Theorem 2.12.** There are 26 isomorphism types of isogeny graphs that are associated to \( \mathbb{Q} \)-isogeny classes of elliptic curves defined over \( \mathbb{Q} \). More precisely, there are 16 types of (linear) \( L_k \) graphs, 3 types of (nonlinear two-primary torsion) \( T_k \) graphs, 6 types of (rectangular) \( R_k \) graphs, and 1 type of (special) \( S \) graph. Moreover, there are 11 isomorphism types of isogeny graphs that are associated to \( \mathbb{Q} \)-isogeny classes of elliptic curves over \( \mathbb{Q} \) with complex multiplication, namely the types \( L_2(p) \) for \( p = 2, 3, 11, 19, 43, 67, 163, L_4, R_4(6), \) and \( R_4(14) \). Finally, the isogeny graphs of type \( L_4 \), \( R_4(14) \), and \( L_2(p) \) for \( p \in \{19, 43, 67, 167\} \) occur exclusively for elliptic curves with CM.

The main theorem in [3] was the classification of isogeny-torsion graphs that occur over \( \mathbb{Q} \).

**Theorem 2.13.** There are 52 isomorphism types of isogeny-torsion graphs that are associated to \( \mathbb{Q} \)-isogeny classes of elliptic curves defined over \( \mathbb{Q} \). In particular, there are 23 types of \( L_k \) graphs, 13 types of \( T_k \) graphs, 12 types of \( R_k \) graphs, and 4 types of \( S \) graphs. Moreover, there are 16 isomorphism types of isogeny-torsion graphs that are associated to \( \mathbb{Q} \)-isogeny classes of elliptic curves over \( \mathbb{Q} \) with complex multiplication (and examples are given in Table 1).

The 16 isomorphism types of isogeny-torsion graphs that occur over \( \mathbb{Q} \) with CM are the two isogeny-torsion graphs of type \( L_4 \)

\[
\begin{array}{ccc}
\mathbb{Z}/M\mathbb{Z} & \frac{3}{\mathbb{Z}/M\mathbb{Z}} & \mathbb{Z}/M\mathbb{Z} \\
\end{array}
\]

where \( m = 1 \) or 3, the eight isogeny-torsion graphs of type \( L_2 \)

\[
\begin{array}{ccc}
\mathbb{Z}/2\mathbb{Z} & \frac{2}{\mathbb{Z}/2\mathbb{Z}} & \mathbb{Z}/M\mathbb{Z} & \frac{3}{\mathbb{Z}/M\mathbb{Z}} & \mathbb{O} \\\n\end{array}
\]

where \( M = 3 \) or 1, and \( p = 11, 19, 43, 67, \) or 163, the three isogeny-torsion graphs of \( R_4 \) type

\[
\begin{array}{cccc}
\mathbb{Z}/2\mathbb{Z} & \frac{2}{\mathbb{Z}/2\mathbb{Z}} & \mathbb{Z}/2\mathbb{Z} & \frac{2}{\mathbb{Z}/M\mathbb{Z}} \\
\mathbb{Z}/2\mathbb{Z} & \frac{2}{\mathbb{Z}/2\mathbb{Z}} & \mathbb{Z}/2\mathbb{Z} & \frac{2}{\mathbb{Z}/2\mathbb{Z}} \\
\end{array}
\]

where \( M = 2 \) or 6, and the three isogeny-torsion graphs of \( T_4 \) type.
We continue with some lemmas and more background that will be used to classify the 2-adic Galois images attached to isogeny-torsion graphs with CM.

2.2. Quadratic Twists.

Lemma 2.14. Let $N$ be a positive integer such that $\text{GL}(2, \mathbb{Z}/N\mathbb{Z})$ has a subgroup $H$ that does not contain $-\text{Id}$. Let $H' = \langle -\text{Id}, H \rangle$. Then $H' \cong \langle -\text{Id} \rangle \times H$.

Proof. Note that $H$ is a subgroup of $H'$ of index 2. Hence, the order of $H'$ and the order of $\langle -\text{Id}, H \rangle$ are the same. Define

$$
\psi: \langle -\text{Id} \rangle \times H \rightarrow H'
$$

by $\psi(x, h) = xh$. Then $\psi$ is a group homomorphism as $-\text{Id}$ is in the center of $\text{GL}(2, \mathbb{Z}/N\mathbb{Z})$. We are done if we prove that $\psi$ is injective. Let $(x, h) \in \langle -\text{Id} \rangle \times H$ such that $\psi(x, h) = xh = \text{Id}$. Then $h = x^{-1} = x$ as the order of $x$ is equal to 1 or 2. As $-\text{Id} \not\in H$, $h$ cannot be $-\text{Id}$. Hence, $h = x = \text{Id}$ and so, $\psi$ is injective. \[\square\]

Definition 2.15. Let $G$ and $H$ be subgroups of $\text{GL}(2, \mathbb{Z}/2\mathbb{Z})$. Then we will say that $G$ and $H$ are quadratic twists if $G$ is the same as $H$, up to multiplication of some elements of $H$ by $-\text{Id}$. Note that if $\langle G, -\text{Id} \rangle = \langle H, -\text{Id} \rangle$, then $H$ and $G$ are quadratic twists.

Lemma 2.16. Let $N$ be a positive integer, let $H$ be a subgroup of $\text{GL}(2, \mathbb{Z}/N\mathbb{Z})$, and let $H' = \langle H, -\text{Id} \rangle$. Let $\chi$ be a character of $H$ of degree two. Then $\chi(H) = H'$ or $\chi(H)$ is a subgroup of $H'$ of index 2.

Proof. The character $\chi$ multiplies some elements of $H$ by $-\text{Id}$. If $-\text{Id} \in \chi(H)$, then we can multiply all of the elements of $H$ that $\chi$ multiplied by $-\text{Id}$ by $-\text{Id}$ again, and recoup all of the elements of $H$. Thus, $\chi(H)$ is a subgroup of $H'$ that contains both $-\text{Id}$ and $H$ and so, $\chi(H) = H'$.

On the other hand, let us say that $-\text{Id} \notin \chi(H)$. Let $\chi(H)' = \langle \chi(H), -\text{Id} \rangle$. By the same argument from before, we can multiply all of the elements of $H$ that $\chi$ multiplied by $-\text{Id}$ by $-\text{Id}$ again, and recoup all of the elements of $H$ in $\chi(H)'$. In other words, $\chi(H)' = \langle -\text{Id}, \chi(H) \rangle = \langle -\text{Id}, H \rangle = H'$. By Lemma 2.14, $H' = \langle \chi(H), -\text{Id} \rangle \cong \langle -\text{Id} \rangle \times \chi(H)$ and $\chi(H)$ is a subgroup of $H'$ of index 2. \[\square\]

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve and let $d$ be a non-zero integer. Then the quadratic twist of $E$ by $d$ is the elliptic curve $E^{(d)} : y^2 = x^3 + d^2Ax + d^2B$. Equivalently, $E^{(d)}$ is isomorphic to the elliptic curve defined by $dy^2 = x^3 + Ax + B$. Moreover, $E$ is isomorphic to $E^{(d)}$ over $\mathbb{Q}(\sqrt{d})$ by the map $\phi: E \rightarrow E^{(d)}$ defined by fixing $\mathcal{O}$ and mapping any non-zero point $(a, b)$ on $E$ to $\left(a, \frac{b}{\sqrt{d}}\right)$.

Corollary 2.17. Let $N$ be a positive integer such that $\text{GL}(2, \mathbb{Z}/N\mathbb{Z})$ contains a subgroup $H$ such that all subgroups of $H$ of index 2 contain $-\text{Id}$. Suppose that there exists an elliptic curve $E/\mathbb{Q}$ such that $\overline{\rho}_{E, N}(G_{\mathbb{Q}})$ is conjugate to $H$. Let $E^x$ be a quadratic twist of $E$. Then $\overline{\rho}_{E^x, N}(G_{\mathbb{Q}})$ is conjugate to $H$. 

\[\square\]
Proof. The group $H$ contains $-\text{Id}$. By Lemma 2.16, $\overline{\tau}_{E,N}(G_Q)$ is conjugate to $H$ or is conjugate to a subgroup of $H$ of index 2. Moreover, $\overline{\tau}_{E,N}(G_Q)$ is the same as $\overline{\tau}_{E,N}(G_Q) = H$, up to multiplication of some elements of $H$ by $-\text{Id}$. As all subgroups of $H$ of index 2 contain $-\text{Id}$, we can just multiply the elements of $\overline{\tau}_{E,N}(G_Q)$ that $\chi$ multiplied by $-\text{Id}$ again by $-\text{Id}$ to recoup all elements of $H$. Hence, $\overline{\tau}_{E,N}(G_Q)$ is conjugate to $H$. $\Box$

Remark 2.18. Let $N$ be a positive integer such that $\text{GL}(2,\mathbb{Z}/N\mathbb{Z})$ contains a subgroup $H$ that does not contain $-\text{Id}$. Suppose there is an elliptic curve $E/\mathbb{Q}$ such that $\overline{\tau}_{E,N}(G_Q)$ is conjugate to $H' = (H, -\text{Id})$. Then there is a quadratic twist $\chi$ such that $\overline{\tau}_{E,N}(G_Q)$ is conjugate to $H$ (see Remark 1.1.3 and Section 10 in [7]). Conversely, if $\overline{\tau}_{E,N}(G_Q)$ is conjugate to $H$, then there is a non-zero integer $d$ and a quadratic twist $E(d')$ of $E$, such that $\overline{\tau}_{E(d'),N}(G_Q)$ is conjugate to $H'$. Note that $\mathbb{Q}(E[N])$ does not contain $\mathbb{Q}(\sqrt{d})$.

2.3. Galois representations.

Lemma 2.19. Let $E$ and $E'$ be elliptic curves defined over $\mathbb{Q}$ that are $\mathbb{Q}$-isogenous by an isogeny $\phi$ whose kernel is finite, cyclic, and $\mathbb{Q}$-rational. Let $\ell$ be a prime and let $r$ be the non-negative integer such that $\ell^r$ is the greatest power of $\ell$ that divides the order of $\text{Ker}(\phi)$. Let $m$ be a non-negative integer. Then there is a basis $\{P_{m+r}, Q_{m+r}\}$ of $E[\ell^{m+r}]$ such that

1. if $\sigma$ is a Galois automorphism of $\mathbb{Q}$, then, there are integers $A, B, C,$ and $D$, where $\overline{\tau}_{E,m+r}(\sigma) = \begin{bmatrix} A & C \\ B & D \end{bmatrix}$ and $\ell^r$ divides $C$,

2. $\{\phi(\ell^r P_{m+r}), \phi(Q_{m+r})\}$ is a basis of $E'[\ell^m]$,

3. $\overline{\tau}_{E',m}(\sigma) = \begin{bmatrix} A & C \\ \ell^r \cdot B & D \end{bmatrix}$.

Proof. We break up the proof into steps

1. Let $Q_{\ell^r}$ be an element of $\text{Ker}(\phi)$ of order $\ell^r$ and let $Q_{m+r}$ be a point on $E$ such that $\ell^m Q_{m+r} = Q_{\ell^r}$. Let $P_{m+r}$ be a point on $E$ such that $E[\ell^{m+r}] = \langle P_{m+r}, Q_{m+r} \rangle$. Let $\sigma$ be a Galois automorphism of $\mathbb{Q}$. Then there are integers $A$ and $B$ such that $\sigma(P_{m+r}) = [A] P_{m+r} + [B] Q_{m+r}$ and there are integers $C$ and $D$ such that $\sigma(Q_{m+r}) = [C] P_{m+r} + [D] Q_{m+r}$. Then

$\sigma(Q_{\ell^r}) = \sigma(\ell^m Q_{m+r}) = \ell^m [\sigma(Q_{m+r})] = \ell^m [C] P_{m+r} + [D] Q_{m+r}$.

As $Q_{\ell^r}$ generates a $\mathbb{Q}$-rational group, $\sigma(Q_{\ell^r}) = \ell^m [C] P_{m+r} + [D] Q_{m+r} \in \langle Q_{\ell^r} \rangle \subseteq \langle Q_{m+r} \rangle$. Thus, $\ell^m [C] P_{m+r} \in \langle Q_{m+r} \rangle$. As $\langle P_{m+r} \rangle \cap \langle Q_{m+r} \rangle = \{0\}$, we have that $\ell^m [C] P_{m+r} = 0$. Thus, $\ell^{m+r}$ divides $\ell^m C$ and hence, $\ell^r$ divides $C$.

2. We claim that $E'[\ell^m] = \langle \phi(\ell^r P_{m+r}), \phi(Q_{m+r}) \rangle$. We claim that the order of $\phi(\ell^r P_{m+r})$ and the order of $\phi(Q_{m+r})$ are both equal to $\ell^m$. Note that $\ell^m \phi(\ell^r P_{m+r}) = \phi(\ell^{m+r} P_{m+r}) = 0$. Next, $\ell^m \phi(Q_{m+r}) = \phi(\ell^m Q_{m+r}) = 0(\ell^r)$. If $m = 0$, then we can move on. If $m$ is positive, then $m - 1$ is a non-negative integer and

$\ell^{m-1} \cdot \phi(\ell^r P_{m+r}) = \phi(\ell^{m+r-1} P_{m+r})$.

If we claim that $\phi(\ell^{m+r-1} P_{m+r}) = 0$, then $\ell^{m+r-1} P_{m+r} \in \langle Q_{\ell^r} \rangle \subseteq \langle Q_{m+r} \rangle$. The point $\ell^{m+r-1} P_{m+r}$ generates the subgroup of $\langle Q_{m+r} \rangle$ of order $\ell$ and so cannot be contained in $\langle Q_{m+r} \rangle$ and so we arrive at a contradiction. Next,

$\ell^{m-1} \cdot \phi(Q_{m+r}) = \phi(\ell^{m-1} Q_{m+r})$.

If we claim that $\phi(\ell^{m-1} Q_{m+r}) = 0$, then $\ell^{m-1} Q_{m+r} \in \langle Q_{\ell^r} \rangle$ but this is a contradiction as the order of $\ell^{m-1} Q_{m+r}$ is equal to $r + 1$ and the order of $Q_{\ell^r}$ is equal to $\ell^r$.

Now we will prove that $\phi(\ell^r P_{m+r}) \cap \phi(Q_{m+r}) = \{0\}$. Now let us say that there are integers $\alpha$ and $\beta$ such that $[\alpha] \phi(\ell^r P_{m+r}) = [\beta] \phi(Q_{m+r})$. Then $\phi(\ell \alpha P_{m+r}) = \phi(\ell \beta Q_{m+r})$. Hence, $[\alpha \ell^r] P_{m+r} = [\beta] Q_{m+r} \in \langle Q_{\ell^r} \rangle \subseteq \langle Q_{m+r} \rangle$ and hence, $[\alpha \ell^r] P_{m+r} \in \langle Q_{m+r} \rangle$. Thus, $[\alpha \ell^r] P_{m+r} = 0$. Therefore, $\phi(\ell^r P_{m+r}) \cap \phi(Q_{m+r}) = \{0\}$.
and hence, \([\alpha]\phi([\ell^m]P_{\ell^{m+r}}) = \phi([\alpha\ell^m]P_{\ell^{m+r}}) = \mathcal{O}\). This means that \(\langle \phi([\ell^r]P_{\ell^{m+r}}) \rangle \cap \langle \phi(Q_{\ell^{m+r}}) \rangle = \{\mathcal{O}\} \).

(3) Next, we see that
\[
\sigma(\phi([\ell^r]P_{\ell^{m+r}})) = \phi([\ell^r]\sigma(P_{\ell^{m+r}})) = \phi([\ell^r][A]P_{\ell^{m+r}} + [B]Q_{\ell^{m+r}})] = [A]\phi([\ell^r]P_{\ell^{m+r}}) + [\ell^r \cdot B]\phi(Q_{\ell^{m+r}}).
\]

Finally, we see that
\[
\sigma(\phi(Q_{\ell^{m+r}})) = \phi(\sigma(Q_{\ell^{m+r}})) = \phi([C]P_{\ell^{m+r}} + [D]Q_{\ell^{m+r}}) = \phi([\ell^r]P_{\ell^{m+r}} + [D]\phi(Q_{\ell^{m+r}}).
\]

\[\square\]

**Remark 2.20.** Let \(E\) and \(E'\) be elliptic curves defined over \(\mathbb{Q}\). Let \(\phi: E \to E'\) be a \(\mathbb{Q}\)-isogeny with a finite, cyclic, \(\mathbb{Q}\)-rational kernel. Let \(\ell\) be the greatest power of \(\ell\) that divides the order of \(\text{Ker}(\phi)\). Let \(m\) be a non-negative integer. Given \(\overline{\rho}_{E,\ell^{m+r}}(G_{\mathbb{Q}})\), we may use Lemma 2.19 to compute \(\overline{\rho}_{E',\ell^m}(G_{\mathbb{Q}})\). Therefore, \(\rho_{E',\ell^m}(G_{\mathbb{Q}})\) is determined by \(\rho_{E,\ell^{m+r}}(G_{\mathbb{Q}})\) (and vice versa).

**Corollary 2.21.** Let \(E\) and \(E'\) be elliptic curves defined over \(\mathbb{Q}\) and let \(\ell\) be a prime number. Suppose that \(E\) is \(\mathbb{Q}\)-isogenous to \(E'\) by an isogeny that is defined over \(\mathbb{Q}\) with a finite, cyclic kernel of degree not divisible by \(\ell\). Then \(\rho_{E,\ell^{m+r}}(G_{\mathbb{Q}})\) is conjugate to \(\rho_{E',\ell^m}(G_{\mathbb{Q}})\).

**Proof.** Use Lemma 2.19 with \(r = 0\).

\[\square\]

**Corollary 2.22.** Let \(\ell\) be a prime and let \(E\) and \(E'\) be elliptic curves defined over \(\mathbb{Q}\). Suppose that \(E\) is \(\mathbb{Q}\)-isogenous to \(E'\) by an isogeny \(\phi\) with a finite, cyclic, \(\mathbb{Q}\)-rational kernel. Let \(\alpha\) be an integer that is not divisible by \(\ell\). Then \(\rho_{E,\ell^{m+r}}(G_{\mathbb{Q}})\) contains \(s_\alpha = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}\) if and only if \(\rho_{E',\ell^m}(G_{\mathbb{Q}})\) contains \(s_\alpha\).

**Proof.** Suppose that \(\rho_{E,\ell^{m+r}}(G_{\mathbb{Q}})\) contains \(s_\alpha\). Let \(r\) be the non-negative integer such that \(\ell^r\) is the greatest power of \(\ell\) that divides \(\text{Ker}(\phi)\) and let \(m\) be a non-negative integer. Then \(\overline{\rho}_{E,\ell^{m+r}}(G_{\mathbb{Q}})\) contains \(s_\alpha\). As \(s_\alpha\) is in the center of \(\text{GL}(2, \mathbb{Z}/\ell^{m+r}\mathbb{Z})\), it does not matter what basis we use for \(E[\ell^{m+r}]\). By Lemma 2.19, \(s_\alpha\) is an element of \(\overline{\rho}_{E',\ell^m}(G_{\mathbb{Q}})\). The converse is proved simply by switching the roles of \(E\) and \(E'\) and using the dual of \(\phi\).

\[\square\]

**Corollary 2.23.** Let \(\ell\) be a prime and let \(E\) and \(E'\) be elliptic curves defined over \(\mathbb{Q}\). Suppose that \(E\) is \(\mathbb{Q}\)-isogenous to \(E'\) by an isogeny \(\phi\) with a finite, cyclic, \(\mathbb{Q}\)-rational kernel. Then \(\rho_{E,\ell^{m+r}}(G_{\mathbb{Q}})\) contains \(-1\cdot \text{id}\) if and only if \(\rho_{E',\ell^m}(G_{\mathbb{Q}})\) contains \(-1\cdot \text{id}\).

**Proof.** Use Corollary 2.22 with \(\alpha = -1\).

\[\square\]

**Lemma 2.24** (Generalized Hensel’s Lemma). Let \(p\) be a prime and let \(f(x)\) be a polynomial with integer coefficients. Suppose that \(f(a) \equiv 0 \pmod{p^j}\), \(p^r \mid f'(a)\), and that \(j \geq 2r + 1\). Then there is a unique \(t\) (modulo \(p\)) such that \(f(a + tp^{j-r}) \equiv 0 \pmod{p^{j+1}}\).

3. **Classification of 2-adic Galois Images attached to elliptic curves defined over \(\mathbb{Q}\) with CM**

In [1], Lozano-Robledo classified the image of \(\ell\)-adic Galois representations attached to elliptic curves defined over \(\mathbb{Q}\) with CM for all primes \(\ell\). In this section, we will briefly go over the results from [1] that are important in this paper.
For the rest of the paper, let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic imaginary field, let $\mathcal{O}_K$ be the ring of integers of $K$ with discriminant $\Delta_K$. Then $\Delta_K = d$ if $d$ is congruent to 1 modulo 4 and $\Delta_K = 4d$ otherwise. Let $f$ be a positive integer and let $\mathcal{O}_{K,f}$ be the order of $K$ of conductor $f$.

**Theorem 3.1** (Theorem 1.1, [1]). Let $E/\mathbb{Q}$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, let $N$ be an even integer greater than or equal to 4 and let $\overline{\rho}_{E,N} : G_{\mathbb{Q}} \to \text{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

- If $\Delta_K \cdot f^2 \equiv 0 \mod 4$, then set $\delta = \frac{\Delta_K f^2}{4}$ and $\phi = 0$.
- If $\Delta_K \cdot f^2 \equiv 1 \mod 4$, then set $\delta = \frac{(\Delta_K - 1)}{4} \cdot f^2$ and $\phi = f$.

Define the group $C_{\delta,\phi}(N)$ to be the subgroup of $\text{GL}(2, \mathbb{Z}/N\mathbb{Z})$ consisting of all matrices of the form $\begin{bmatrix} a + b\phi & b \\ \delta b & a \end{bmatrix}$ and define $N_{\delta,\phi}(N)$ to be the group $N_{\delta,\phi}(N) = \left\langle C_{\delta,\phi}(N), \begin{bmatrix} -1 & 0 \\ \phi & 1 \end{bmatrix} \right\rangle$. Then

1. there is a $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N]$ such that the image of $\overline{\rho}_{E,N}(G_{\mathbb{Q}})$ is contained in $N_{\delta,\phi}(N)$
2. and $C_{\delta,\phi}(N) \equiv (\mathcal{O}_{K,f}/N\mathcal{O}_{K,f})^\times$ is a subgroup of $N_{\delta,\phi}(N)$ of index 2.

**Theorem 3.2** (Theorem 1.2, [1]). Let $E/\mathbb{Q}$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$.

- If $\Delta_K \cdot f^2 \equiv 0 \mod 4$, then set $\delta = \frac{\Delta_K f^2}{4}$ and $\phi = 0$.
- If $\Delta_K \cdot f^2 \equiv 1 \mod 4$, then set $\delta = \frac{(\Delta_K - 1)}{4} \cdot f^2$ and $\phi = f$.

Let $\rho_E$ be the Galois representation $\rho_E : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{lim Aut}(E[N]) \cong \text{GL}(2, \hat{\mathbb{Z}})$ and let $N_{\delta,\phi} = \text{lim N}_{\delta,\phi}(N)$. Then there is a compatible system of bases of $E[N]$ such that the image of $\rho_E$ is contained in $\hat{N}_{\delta,\phi}$, and the index of the image of $\rho_E$ in $N_{\delta,\phi}$ is a divisor of the order of $\mathcal{O}_{K,f}^\times$. In particular, the index is a divisor of 4 or 6.

From now on, let $H_f = K(j_{K,f})$

**Theorem 3.3** (Theorem 1.6, [1]). Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by an order $\mathcal{O}_{K,f}$ in an imaginary field $K$ with $j_E \neq 0, 1728$. Then, for every $m \geq 1$, we have $\text{Gal}(H_f(E[2^m])/H_f) \subseteq (\mathcal{O}_{K,f}/2^m\mathcal{O}_{K,f})^\times$. Suppose that $\text{Gal}(H_f(E[2^n])/H_f) \subseteq (\mathcal{O}_{K,f}/2^n\mathcal{O}_{K,f})^\times$ for some positive integer $n$ and assume that $n$ is the smallest such integer. Then $n \leq 3$ and for all $m \geq 3$, we have

$$\text{Gal}(H_f(E[2^m])/H_f) \cong (\mathcal{O}_{K,f}/2^m\mathcal{O}_{K,f})^\times / \{\pm 1\}.$$

Further, there are two possibilities:

1. If $n \leq 2$, then $\text{Gal}(H_f(E[4])/H_f) \cong (\mathcal{O}_{K,f}/4\mathcal{O}_{K,f})^\times / \{\pm 1\}$ and:
   - $\text{disc}(\mathcal{O}_{K,f}) = \Delta_K \cdot f^2 \equiv 0 \mod 16$. In particular, we have either
     - $\Delta_K \equiv 1 \mod 4$ and $f \equiv 0 \mod 4$, or
     - $\Delta_K \equiv 0 \mod 4$ and $f \equiv 0 \mod 2$.
   - (b) $\mathbb{Q}(i) \subseteq H_f$.
   - (c) For each $m \geq 2$, there is a $\mathbb{Z}/2^m\mathbb{Z}$-basis of $E[2^m]$ such that the image of the Galois representation $\rho_{E,2^m} : \text{Gal}(\overline{\mathbb{Q}}_f/H_f) \to \text{GL}(2, \mathbb{Z}/2^m\mathbb{Z})$ is one of the groups
     $$J_1 = \left\langle \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ \delta & 1 \end{bmatrix} \right\rangle \text{ or } J_2 = \left\langle \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ -\delta & -1 \end{bmatrix} \right\rangle \subseteq C_{5,0}(2^m)$.

2. If $n = 3$, then $\text{Gal}(H_f(E[4])/H_f) \cong (\mathcal{O}_{K,f}/4\mathcal{O}_{K,f})^\times$ and:
   - (a) $\Delta_K \equiv 0 \mod 8$.
   - (b) For each $m \geq 3$, there is a $\mathbb{Z}/2^m\mathbb{Z}$-basis of $E[2^m]$ such that the image of the Galois representation $\rho_{E,2^m} : \text{Gal}(\overline{\mathbb{Q}}_f/H_f) \to \text{GL}(2, \mathbb{Z}/2^m\mathbb{Z})$ is the group
     $$J_1 = \left\langle \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ \delta & 1 \end{bmatrix} \right\rangle \text{ or } J_2 = \left\langle \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ -\delta & -1 \end{bmatrix} \right\rangle \subseteq C_{3,0}(2^m)$.
Finally, there is some \( \epsilon \in \{\pm 1\} \) and \( \alpha \in \{3,5\} \) such that the image of \( \rho_{E,2^\infty} \) is a conjugate of
\[
\langle \begin{bmatrix} 1 & \epsilon \\ \epsilon^{-1} & \alpha \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \rangle = \langle \begin{bmatrix} 1 & \epsilon \\ \epsilon^{-1} & \alpha \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \rangle \subseteq \text{GL}(2, \mathbb{Z}_2).
\]

**Corollary 3.4.** Let \( E/\mathbb{Q} \) be an elliptic curve with \( \mathcal{CM} \) by an order \( \mathcal{O}_{K,f} \) in the number field \( K \) with discriminant \( \Delta_K \) and conductor \( f \) and \( j_E \neq 0, 1728 \). Let \( m \) be a non-negative integer. Then \( \overline{\rho}_{E,2^{m+3}}(G_\mathbb{Q}) \) is conjugate to the full lift of \( \overline{\rho}_{E,8}(G_\mathbb{Q}) \) inside the group \( \mathcal{N}_{h,\phi}(2^{2+m}) \).

**Corollary 3.5.** Let \( E/\mathbb{Q} \) be an elliptic curve with \( \mathcal{CM} \) by an order \( \mathcal{O}_{K,f} \) in the number field \( K \) with discriminant \( \Delta_K \) and conductor \( f \) and \( j_E \neq 0, 1728 \). If \( \Delta_K : f^2 \) is not divisible by \( 8 \), then \( \rho_{E,2^\infty}(G_\mathbb{Q}) \) is conjugate to \( \mathcal{N}_{h,\phi}(2^\infty) \).

**Theorem 3.6 (Theorem 1.7, [1]).** Let \( E/\mathbb{Q} \) be an elliptic curve with \( j_E = 1728 \) and let \( c \in \mathbb{G}_\mathbb{Q} \) represent complex conjugation and \( \gamma = \rho_{E,2^\infty}(G_\mathbb{Q}(c)). \) Let \( G_{E,2^\infty} \) be the image of \( \rho_{E,2^\infty} \) and let \( G_{E,K,2^\infty} = \rho_{E,2^\infty}(G_{\mathbb{Q}(i)}) \). Then, there is a \( \mathbb{Z}_2 \)-basis of \( T_2(E) = \lim_{\to \infty} E[2^n] \) such that \( G_{E,K,2^\infty} \) is one of the following groups:

- If \( [\mathcal{C}, 0](2^\infty) : G_{E,K,2^\infty} = 1 \), then \( G_{E,K,2^\infty} \) is all of \( \mathcal{C}, 0(2^\infty) \), i.e.,
  \[
  G_1 = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \text{GL}(2, \mathbb{Z}_2) : a^2 + b^2 \equiv 0 \mod 2 \right\}.
  \]

- If \( [\mathcal{C}, 0](2^\infty) : G_{E,K,2^\infty} = 2 \), then \( G_{E,K,2^\infty} \) is one of the following groups:
  \[
  G_{2,a} = \left\{ \begin{bmatrix} -3 & 1 \\ -2 & 1 \end{bmatrix} \right\} \text{ or } G_{2,b} = \left\{ \begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix} \right\}.
  \]

- If \( [\mathcal{C}, 0](2^\infty) : G_{E,K,2^\infty} = 4 \), then \( G_{E,K,2^\infty} \) is one of the following groups:
  \[
  G_{4,a} = \left\{ \begin{bmatrix} 5 & 2 \\ -2 & -1 \end{bmatrix} \right\} \text{ or } G_{4,b} = \left\{ \begin{bmatrix} 2 & 1 \\ -1 & -2 \end{bmatrix} \right\}.
  \]

Moreover, \( G_{E,2^\infty} = \langle \gamma, G_{E,K,2^\infty} \rangle = \langle \gamma', G_{E,K,2^\infty} \rangle \) is generated by one of the groups above, and an element
\[
\gamma' \in \left\{ e_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, e_{-1} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, e_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, e_{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\},
\]
such that \( \gamma \equiv \gamma' \mod 4 \).

**Theorem 3.7 (Theorem 1.8, [1]).** Let \( E/\mathbb{Q} \) be an elliptic curve with \( j_E = 0 \), and let \( c \in \mathbb{G}_\mathbb{Q} \) represent complex conjugation. Let \( G_{E,2^\infty} \) be the image of \( \rho_{E,2^\infty} \) and let \( G_{E,K,2^\infty} = \rho_{E,2^\infty}(G_{\mathbb{Q}(\sqrt{-3})}) \). Then there is a \( \mathbb{Z}_2 \)-basis of \( T_2(E) \) such that the image \( G_{E,2^\infty} \) of \( \rho_{E,2^\infty} \) is one of the following groups of \( \text{GL}(2, \mathbb{Z}_2) \), with \( \gamma = \rho_{E,2^\infty}(c) \).

- Either, \( [\mathcal{C}, 1](2^\infty) : G_{E,K,2^\infty} = 3 \), and
  \[
  G_{E,2^\infty} = \left\{ \gamma', \text{Id}, \begin{bmatrix} 7 & 4 \\ 4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 6 \\ -4 & -3 \end{bmatrix} \right\} \left\{ \begin{bmatrix} a + b & b \\ -b & a \end{bmatrix} \in \text{GL}(2, \mathbb{Z}_2) : a \not\equiv 0 \mod 2, b \equiv 0 \mod 2 \right\},
  \]
and \( \left\{ \begin{bmatrix} a + b & b \\ -b & a \end{bmatrix} \in \text{GL}(2, \mathbb{Z}_2) : a \not\equiv 0 \mod 2, b \equiv 0 \mod 2 \right\} \) is precisely the set of matrices that correspond to the subgroup of cubes of Cartan elements \( \mathcal{C}, 1(2^\infty)^3 \) which is the unique group of index 3 in \( \mathcal{C}, 1(2^\infty) \).
• Or, \([C_{-1,1}(2^\infty) : G_{E,K,2^\infty}] = 1\), and

\[G_{E,2^\infty} = N_{-1,1}(2^\infty) = \langle \gamma', -\text{Id}, \begin{bmatrix} 7 & 4 \\ -4 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ -1 & 1 \end{bmatrix} \rangle\]

\[= \langle \gamma', \left\{ \begin{bmatrix} a + b & b \\ -b & a \end{bmatrix} \in \text{GL}(2, \mathbb{Z}_2) : a \neq 0 \mod 2\sigma b \neq 0 \mod 2 \right\} \rangle\]

where \(\gamma' \in \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}\), and \(\gamma \equiv \gamma' \mod 4\).

**Corollary 3.8.** Let \(E/\mathbb{Q}\) be an elliptic curve with \(j_E = 0\). Then \(E\) has a point of order \(2\) defined over \(\mathbb{Q}\) if and only if \(\rho_{E,2^\infty}(G_\mathbb{Q})\) is conjugate to \(\langle -\text{Id}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 7 & 4 \\ -4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 6 \\ -6 & -3 \end{bmatrix} \rangle\) and \(E\) does not have a point of order \(2\) defined over \(\mathbb{Q}\) if and only if \(\rho_{E,2^\infty}(G_\mathbb{Q})\) is conjugate to \(N_{-1,1}(2^\infty)\).

**Proof.** From the fact that \(j_E = 0\), \(\rho_{E,2^\infty}(G_\mathbb{Q})\) is conjugate to one of two groups. The reduction of the group \(\langle -\text{Id}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 7 & 4 \\ -4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 6 \\ -6 & -3 \end{bmatrix} \rangle\) modulo 2 is a group of order 2 and the reduction of \(N_{-1,1}(2^\infty)\) modulo 2 is a group of order 6. Hence, if \(\rho_{E,2^\infty}(G_\mathbb{Q})\) is conjugate to the former, \(E\) has a point of order 2 defined over \(\mathbb{Q}\) and if \(\rho_{E,2^\infty}(G_\mathbb{Q})\) is conjugate to the latter, then \(E\) does not have a point of order 2 defined over \(\mathbb{Q}\). \(\square\)

4. \(2\)-adic Galois images attached to isogeny-torsion graphs with CM

Here we classify the \(2\)-adic Galois image attached to isogeny-torsion graphs defined over \(\mathbb{Q}\) with CM. We will categorize the proofs based first on isogeny-torsion graphs and then on \(j\)-invariant.

**Proposition 4.1.** Let \(E/\mathbb{Q}\) be an elliptic curve with complex multiplication such that the isogeny graph associated to the \(\mathbb{Q}\)-isogeny class of \(E\) is of \(L_4\) type or of \(L_2(3)\) type. Then \(\rho_{E,2^\infty}(G_\mathbb{Q})\) is conjugate to \(N_{-1,1}(2^\infty)\).

**Proof.** If the isogeny graph associated to the \(\mathbb{Q}\)-isogeny class of \(E\) is of \(L_4\) type, then it looks like the one below with the \(j\)-invariant of the corresponding elliptic curves listed:

\[E_1, j_{E_1} = -12288000 \quad \begin{array}{c} E_2, j_{E_2}=0 \quad \begin{array}{c} E_3, j_{E_3}=0 \quad \begin{array}{c} E_4, j_{E_4} = -12288000 \quad \begin{array}{c} \begin{array}{c} E, j_{E_1}=0 \quad \begin{array}{c} \begin{array}{c} E_2, j_{E_2}=0 \quad \begin{array}{c} \begin{array}{c} \end{array} \end{array} \end{array} \end{array} \end{array} \end{array} \end{array} \end{array} \end{array}\]

and if the isogeny graph associated to the \(\mathbb{Q}\)-isogeny class of \(E\) is of \(L_2(3)\) type, then it looks like the one below with the \(j\)-invariant of the corresponding elliptic curves listed:

\[E, j_{E_1}=0 \quad \begin{array}{c} E_2, j_{E_2}=0 \quad \begin{array}{c} \begin{array}{c} \end{array} \end{array} \end{array}\]

Let \(E'/\mathbb{Q}\) be an elliptic curve that is \(3\)-isogenous to \(E\) with \(j_{E'} = 0\). By Corollary 2.21, \(\rho_{E,2^\infty}(G_\mathbb{Q})\) is conjugate to \(\rho_{E',2^\infty}(G_\mathbb{Q})\). As \(E'\) does not have a point of order 2 defined over \(\mathbb{Q}\), Corollary 3.8 shows that \(\rho_{E,2^\infty}(G_\mathbb{Q})\) is conjugate to \(N_{-1,1}(2^\infty)\). \(\square\)

**Proposition 4.2.** Let \(E/\mathbb{Q}\) be an elliptic curve with CM by a number field \(K\) with discriminant \(\Delta_K\). Suppose that the isogeny graph associated to the \(\mathbb{Q}\)-isogeny class of \(E\) is of \(L_2(p)\) type with \(p \in \{11, 19, 43, 67, 163\}\). Then \(\rho_{E,2^\infty}(G_\mathbb{Q})\) is conjugate to \(N_{\Delta_K-1,1}(2^\infty)\).

**Proof.** The elliptic curve \(E\) is \(p\)-isogenous to an elliptic curve \(E'/\mathbb{Q}\). Moreover, \(j_E = j_{E'}\) and \(j_E \neq 0, 1728\), meaning that \(E\) is a quadratic twist of \(E'\). The isogeny graph associated to the \(\mathbb{Q}\)-isogeny class of \(E\) is of \(L_2(p)\) type (see below).
By Corollary 2.21, \( \rho_{E,2s}(G_Q) \) is conjugate to \( \rho_{E',2s}(G_Q) \). We prove that \( \rho_{E,2s}(G_Q) \) is unaffected by quadratic twisting by showing that -Id is an element of every subgroup of \( \rho_{E,2s}(G_Q) \) of index 2.

By Table 1, \( j_E \in \{-32768, -884736, -884736000, -147197952000, -262537412640768000\} \). Each such elliptic curve has CM by a quadratic imaginary field \( K \) of discriminant \( \Delta_K \), namely, \( -11, -19, -43, -67, \) and \(-163\), respectively. We take an example of each such elliptic curve \( E'/Q \) with \( j \)-invariant equal to one of the five above, namely, the elliptic curves with LMFDB labels 121.b1, 361.a1, 1849.b1, 4489.b1, and 26569.a1, respectively. By the fact that \( j_E = j_{E'} \) and \( j_E \neq 0, 1728, E \) is a quadratic twist of \( E' \). Running code provided by Lozano-Robledo, we see that the conductor of each of the elliptic curves \( E' \) is equal to \( f = 1 \). Hence, \( \Delta_K \cdot f^2 \equiv 1 \pmod{4} \) and so, \( \delta = \frac{\Delta_K - 1}{4} \) and \( \phi = 1 \).

By the fact that \( \Delta_K \cdot f^2 \) is not divisible by 8, Corollary 3.5 shows that, \( \rho_{E',2s}(G_Q) \) is conjugate to \( \mathcal{N}_{\delta,1}(2^\infty) = \left\{ \begin{bmatrix} a+b & b \\ \delta b & a \end{bmatrix} : a, b \in \mathbb{Z}_2 \text{ and } b \text{ not both even} \right\} \).

Note that setting \( a = -1 \) and \( b = 0 \) shows that -Id \( \in \rho_{E',2s}(G_Q) \) for each of the five elliptic curves. Let \( H \) be a subgroup of \( \rho_{E',2s}(G_Q) \) of index 2. Then \( H \) is normal and hence, the squares of all elements of \( \rho_{E',2s}(G_Q) \) are contained in \( H \). Let \( a \) be an integer and let \( b = 1 \). Then

\[
\left( \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} a+1 & 1 \\ \delta & a \end{bmatrix} \right)^2 = \begin{bmatrix} a^2 + a - \delta & 0 \\ 0 & a^2 + a - \delta \end{bmatrix}.
\]

We have to show that we have an equality of the form \( -1 = a^2 + a - \delta \) modulo \( 2^N \) for all non-negative integers \( N \). Let \( p(x) = x^2 + x - \delta + 1 \). Then \( p(0) = 0 \) in \( \mathbb{Z}/2\mathbb{Z} \) because \( \delta \) is odd and \( p'(0) = 1 \neq 0 \mod 2 \). By Hensel’s lemma, there is a unique solution \( a \in \mathbb{Z}_2 \) to the equality \( x^2 + x - \delta = 1 \). Hence, -Id is a square in \( \rho_{E',2s}(G_Q) \) and so, \( H \) contains -Id. By Corollary 2.17 and Corollary 2.21, \( \rho_{E,2s}(G_Q) \) is conjugate to \( \rho_{E',2s}(G_Q) \). Hence, \( \rho_{E,2s}(G_Q) \) is conjugate to \( \mathcal{N}_{\delta,1}(2^\infty) = \mathcal{N}_{\Delta_K - 1}(2^\infty) \).

**Proposition 4.3.** Let \( E/Q \) be an elliptic curve such that the isogeny graph associated to the \( Q \)-isogeny class of \( E \) is of \( R_4(14) \) type. Then \( j_E = 16581375 \) or \( j_E = -3375 \). In the former case, \( \rho_{E,2s}(G_Q) \) is conjugate to \( \mathcal{N}_{-7,0}(2^\infty) \) and in the latter case, \( \rho_{E,2s}(G_Q) \) is conjugate to \( \mathcal{N}_{-7,1}(2^\infty) \).

**Proof.** Let \( E/Q \) be an elliptic curve that has a cyclic, \( Q \)-rational subgroup of order 14. Then the isogeny graph associated to the \( Q \)-isogeny class of \( E \) is below:

\[
\begin{array}{c|c|c}
E_1, j_{E_1} & 16581375 & 2 \\
\hline
7 & E_2, j_{E_2} & -3375 \\
\hline
E_3, j_{E_3} & 16581375 & 2 \\
\hline
E_4, j_{E_4} & -3375 \\
\end{array}
\]

Let \( E/Q \) be the elliptic curve with LMFDB notation 49.a1. Then \( j_E = 16581375 \). Running code provided by Lozano-Robledo, we see that \( E \) has complex multiplication by an order of \( K = \mathbb{Q}(\sqrt{-7}) \) with discriminant \( \Delta_K = -7 \) and conductor \( f = 2 \). Then \( \delta = \frac{-7 \cdot 2}{4} = -7 \). By Corollary 3.5, \( \rho_{E,2s}(G_Q) \) is conjugate to \( \mathcal{N}_{-7,0}(2^\infty) = \left\{ \begin{bmatrix} a & b \\ -7b & a \end{bmatrix} : 2 \nmid a^2 + b^2 \right\} \). We will prove that -Id is contained in all subgroups of \( \mathcal{N}_{-7,0}(2^\infty) \) of index 2. Let \( a = 0 \) and let \( b \) be an integer. Then

\[
\left( \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & b \\ -7b & 0 \end{bmatrix} \right)^2 = \begin{bmatrix} 7b^2 & 0 \\ 0 & 7b^2 \end{bmatrix}.
\]

We have to prove that for each positive integer \( N \), there is a solution to the equation \(-1 = 7b^2\).
Let $p = 2$ and consider the polynomial $f(x) = 7x^2 + 1$. We will use Lemma 2.24. Let $a = 1$. Then $f(a) = 8 \equiv 0 \mod 2^4$. Next we have $f'(x) = 14x$ and $f'(a) = 14$. Letting $\tau = 1$, we have $2^4 || f'(a)$. Setting $j = 3$, we have that $j \geq 2\tau + 1$. So there is a unique integer $t$ modulo 2 such that $f(1 + t \cdot 2^2) \equiv 0 \mod 2^4$.

Now let $a_1 = 1 + t \cdot 2^2$ and let $j = 4$. Then $f(a_1) \equiv 0 \mod 2^4$. Next, we have that because $a_1$ is odd and $f'(x) = 14x$, that $2^4 || f'(a_1)$. Thus, $j \geq 2\tau + 1$ and by Lemma 2.24, there is a unique integer $t$ modulo 2, such that $f(a_1 + t \cdot 2^3) \equiv 0 \mod 2^6$. We can continue using Lemma 2.24 inductively until we find a 2-adic integer $A = a + a_1 + \ldots$ such that $f(A) = 0 \mod 2^N$ for all positive integers $N$. Thus, $-\text{Id}$ is an element of all subgroups of $\mathcal{N}_{-7,0}(2^\infty)$ of index 2. Thus, quadratic twisting does not affect $\rho_{E,2^\infty}(G_Q)$. By Corollary 2.17, if $j_E = 16581375$, then $\rho_{E,2^\infty}(G_Q)$ is conjugate to $\mathcal{N}_{-7,0}(2^\infty)$.

Let $E'/Q$ be an elliptic curve with $j_{E'} = -3375$. Then $E'$ is 2-isogenous to an elliptic curve with $j$-invariant equal to 16581375. By Corollary 2.23, $\rho_{E',2^\infty}(G_Q)$ contains $-\text{Id}$ and hence, $\rho_{E',2^\infty}(G_Q)$ is not affected by quadratic twisting. Using code provided by Lozano-Robledo, we see that $E'$ has complex multiplication by an order of $K = \mathbb{Q}(\sqrt{-7})$ with discriminant $\Delta_K = -7$ and conductor $f = 1$. By the fact that $\Delta_K \cdot f^2 \equiv 1 \mod 4$, we let $\delta = \frac{\Delta_K - 1}{4} \cdot f^2 = -2$. Again, by the fact that $\Delta_K \cdot f^2$ is not divisible by 8, Corollary 3.5 says that $\rho_{E',2^\infty}(G_Q)$ is conjugate to $\mathcal{N}_{-21}(2^\infty)$. □

**Proposition 4.4.** Let $E/Q$ be an elliptic curve such that $E$ has CM. Suppose that the isogeny graph associated to the $Q$-isogeny class of $E$ is of $R_4(6)$ type. Then $j_E = 0$ or $j_E = 54000$. In the former case, $\rho_{E,2^\infty}(G_Q)$ is conjugate to $\left\langle -\text{Id}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 7 & 4 \\ -4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 6 \\ -6 & -3 \end{bmatrix} \right\rangle$ and in the latter case, $\rho_{E,2^\infty}(G_Q)$ is conjugate to $\mathcal{N}_{-3,0}(2^\infty)$.

**Proof.** The isogeny graph associated to the $Q$-isogeny class of $E$ is below

```
E_1, j_{E_1} = 0 \quad 2 \quad E_2, j_{E_2} = 54000
```

```
3
```

```
E_3, j_{E_3} = 0 \quad 2 \quad E_4, j_{E_4} = 54000
```

The elliptic curve $E$ has a point of order 2 defined over $Q$. If $j_E = 0$, then by Corollary 3.8, $\rho_{E,2^\infty}(G_Q)$ is conjugate to $\left\langle -\text{Id}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 7 & 4 \\ -4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 6 \\ -6 & -3 \end{bmatrix} \right\rangle$. If $j_E = 54000$, then $E$ is 2-isogenous to an elliptic curve $E'/Q$ such that $j_{E'} = 0$. Note that $-\text{Id} \in \rho_{E',2^\infty}(G_Q)$ and by Corollary 2.23, $-\text{Id} \in \rho_{E,2^\infty}(G_Q)$. Thus, quadratic twisting does not affect $\rho_{E,2^\infty}(G_Q)$.

Let $E$ be the elliptic curve with LMFDB label 36.a1. Then $j_E = 54000$. Running code provided by Lozano-Robledo, we see that $E$ has CM by an order of $K = \mathbb{Q}(\sqrt{-3})$ with discriminant $\Delta_K = -3$ and conductor $f = 2$. As $\Delta_K \cdot f^2 \equiv 0 \mod 4$, we have $\delta = \frac{\Delta_K - 1}{4} \cdot f^2 = -3$ and $\phi = 0$. Note that $\Delta_K \cdot f^2 = -12$ is not divisible by 8. By Corollary 3.5, $\rho_{E,2^\infty}(G_Q)$ is conjugate to $\mathcal{N}_{-3,0}(2^\infty)$. As $E$ is a quadratic twist of $E$, $\rho_{E,2^\infty}(G_Q)$ is also conjugate to $\mathcal{N}_{-3,0}(2^\infty)$. □

**Proposition 4.5.** Let $E/Q$ be an elliptic curve with $j_E = 8000$. Then $E$ is 2-isogenous to an elliptic curve $E'/Q$ with $j_{E'} = 8000$. The isogeny graph associated to the $Q$-isogeny class of $E$ is of type $L_2(2)$. Denote

```
H_{1,3} = \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -2 & 1 \end{bmatrix} \right\rangle \quad \text{and} \quad H_{-1,3} = \left\langle \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -2 & 1 \end{bmatrix} \right\rangle.
```

Then $\rho_{E,2^\infty}(G_Q)$ fits in the following table.
Let $E/\mathbb{Q}$ be an elliptic curve such that $j_E = 8000$. Then the isogeny graph associated to the $\mathbb{Q}$-isogeny class of $E$ is of $L_2(2)$ type shown below:

![Isogeny graph](image)

| Isogeny graph | $\rho_{E_1, 2^\infty}(G_{\mathbb{Q}})$ | $\rho_{E_2, 2^\infty}(G_{\mathbb{Q}})$ |
|---------------|--------------------------------------|--------------------------------------|
| $E_1$         | $H_{1,3}$                            | $H_{-1,3}$                           |
| $2$           | $\mathcal{N}_{-2,0}(2^\infty)$      | $\mathcal{N}_{-2,0}(2^\infty)$      |

**Proof.** Let $E/\mathbb{Q}$ be an elliptic curve such that $j_E = 8000$. Then the isogeny graph associated to the $\mathbb{Q}$-isogeny class of $E$ is of $L_2(2)$ type shown below:

![Isogeny graph](image)

If $\rho_{E, 2^\infty}(G_{\mathbb{Q}})$ is not conjugate to $\mathcal{N}_{-2,0}(2^\infty)$, then by Theorem 3.3, there are $\epsilon \in \{1, -1\}$ and $\alpha \in \{3, 5\}$, such that $\rho_{E, 2^\infty}(G_{\mathbb{Q}})$ is conjugate to

$$H_{\epsilon, \alpha} = \left\{ \begin{bmatrix} \epsilon & 0 \\ 0 & -\epsilon \end{bmatrix}, \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ \delta & 1 \end{bmatrix} \right\} \text{ or } H'_{\epsilon, \alpha} = \left\{ \begin{bmatrix} \epsilon & 0 \\ 0 & -\epsilon \end{bmatrix}, \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ -\delta & -1 \end{bmatrix} \right\}.$$

Moreover, as $j_E \neq 0, 1728$, all elliptic curves $E'/\mathbb{Q}$ such that $j_{E'} = 8000$ are quadratic twists of $E$. Let $E/\mathbb{Q}$ be the elliptic curve with LMFDB label 256.a1. Then $j_E = 8000$. Using code provided by Lozano-Robledo, we see that $E$ has complex multiplication by an order of $K = \mathbb{Q}(\sqrt{-2})$ with $\Delta_K = -8$ and conductor $f = 1$. We compute that $\delta = \frac{-8\sqrt{2}}{3} = -2$ and thus, $\phi = 0$.

A quick computation reveals that $H_{1,5}$, $H_{-1,5}$, $H'_{1,5}$, and $H'_{-1,5}$ are all equal to $\mathcal{N}_{-2,0}(2^\infty)$ modulo 8. By Corollary 3.4, if $\tilde{\rho}_{E, 8}(G_{\mathbb{Q}})$ is conjugate to $\mathcal{N}_{-2,0}(2^\infty)$ modulo 8, then $\rho_{E, 2^\infty}(G_{\mathbb{Q}})$ is conjugate to $\mathcal{N}_{-2,0}(2^\infty)$. Another quick computation reveals that $H_{1,5}$ is conjugate to $H'_{1,3}$ and $H_{-1,3}$ is conjugate to $H'_{-1,3}$ modulo 8. Neither $H_{1,3}$ nor $H_{-1,3}$ contain -Id and $H_{1,3}$ is not conjugate to $H_{-1,3}$. Moreover, $H_{1,3}$, $H_{1,5}$, and $H_{1,5}$ are quadratic twists modulo 8 with $H_{1,5} = (H_{1,3}, -Id) = (H_{1,3}, -Id)$ modulo 8. In other words, up to conjugation, there are three groups to work with $H_{1,3}$, $H_{1,3}$, and $H_{1,5} = \mathcal{N}_{-2,0}(2^\infty)$.

The elliptic curve $E_1 : y^2 = x^3 - 17280x - 774144$ has LMFDB label 256.a1 and the elliptic curve $E_2 : y^2 = x^3 - 4320x + 96768$ has LMFDB label 256.a2. Moreover, $j_{E_1} = j_{E_2} = 8000$ and $E_1$ is 2-isogenous to $E_2$. By part 2 of Example 9.4 in [1], $\rho_{E_1, 2^\infty}(G_{\mathbb{Q}})$ is conjugate to $H_{-1,3}$ and $\rho_{E_2, 2^\infty}(G_{\mathbb{Q}})$ is conjugate to $H_{1,5}$.

Finally, let $E/\mathbb{Q}$ be the elliptic curve with LMFDB label 2304.h1. Then $j_E = 8000$. Hence, the isogeny graph associated to the $\mathbb{Q}$-isogeny class of $E$ is of $L_2(2)$ type and $E$ is $\mathbb{Q}$-isogenous to one other elliptic curve $E'$ defined over $\mathbb{Q}$. Using code provided by Lozano-Robledo, we see that $\tilde{\rho}_{E, 8}(G_{\mathbb{Q}})$ contains -Id and by Lemma 2.23, $E'$ does too. By the fact that the $j$-invariants of both $E$ and $E'$ equal 8000 and $\tilde{\rho}_{E, 8}(G_{\mathbb{Q}})$ and $\tilde{\rho}_{E', 8}(G_{\mathbb{Q}})$ both contain -Id, we have that $\rho_{E, 2^\infty}(G_{\mathbb{Q}})$ and $\rho_{E, 2^\infty}(G_{\mathbb{Q}})$ are both conjugate to $\mathcal{N}_{-2,0}(2^\infty)$. $\square$

**Proposition 4.6.** Define the following subgroups of $\text{GL}(2, \mathbb{Z}_2)$

- $G_1 = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a^2 + b^2 \neq 0 \mod 2 \right\}$
- $G_{2,a} = \langle \text{Id}, 3 \cdot \text{Id}, \begin{bmatrix} 1 \\ -2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \end{bmatrix} \rangle$
- $G_{2,b} = \langle \text{Id}, 3 \cdot \text{Id}, \begin{bmatrix} 2 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix} \rangle$
- $G_{4,a} = \langle 5 \cdot \text{Id}, \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ -1 \end{bmatrix} \rangle$
- $G_{4,b} = \langle 5 \cdot \text{Id}, \begin{bmatrix} -1 \\ 2 \end{bmatrix}, \begin{bmatrix} -2 \\ -1 \end{bmatrix} \rangle$
Let $\Gamma = \left\{ c_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, c_{-1} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, c'_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, c'_{-1} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}$. Let $E/\mathbb{Q}$ be an elliptic curve such that $j_E = 1728$. Then $\rho_{E,2^\infty}(G_{\mathbb{Q}})$ is conjugate to $\langle H, \gamma \rangle$ where $H$ is one of the seven groups above and $\gamma \in \Gamma$. Either the isogeny graph associated to the $\mathbb{Q}$-isogeny class $E$ is of type $T_4$ or the isogeny graph associated to the $\mathbb{Q}$-isogeny class of $E$ is of type $L_2(2)$. For $\epsilon \in \{ \pm 1 \}$, denote

$$H_{\epsilon} = \left\langle \begin{bmatrix} \epsilon & 0 \\ 0 & -\epsilon \end{bmatrix}, \begin{bmatrix} 5 & 0 \\ 0 & -5 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -4 & -1 \end{bmatrix} \right\} \text{ and } H'_{\epsilon} = \left\langle \begin{bmatrix} \epsilon & 0 \\ 0 & -\epsilon \end{bmatrix}, \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 4 & -1 \end{bmatrix} \right\}.$$

If the isogeny graph associated to the $\mathbb{Q}$-isogeny class of $E$ is of $T_4$ type, then the $\mathbb{Q}$-isogeny class of $E$ consists of four elliptic curves over $\mathbb{Q}$, $E_1$, $E_2$, $E_3$, and $E_4$, such that $j_{E_1} = j_{E_2} = 1728$ and $j_{E_3} = j_{E_4} = 287496$ with the following algebraic data:

| Isogeny graph | Torsion Configuration | $\rho_{E_1,2^\infty}(G_{\mathbb{Q}})$ | $\rho_{E_2,2^\infty}(G_{\mathbb{Q}})$ | $\rho_{E_3,2^\infty}(G_{\mathbb{Q}})$ | $\rho_{E_4,2^\infty}(G_{\mathbb{Q}})$ |
|----------------|----------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|
| $E_0$          | $\langle [2, 2], [2, 2], [2] \rangle$ | $\langle G_{2,a}, c_1 \rangle$ | $\langle G_{2,a}, c'_1 \rangle$ | $\langle G_{4,a}, c'_1 \rangle$ | $N_{-4,0}(2^\infty)$ |
| $E_1$          | $\langle [2, 2], [2, 4], [2] \rangle$ | $\langle G_{4,a}, c_1 \rangle$ | $\langle G_{4,a}, c'_1 \rangle$ | $\langle G_{4,b}, c'_1 \rangle$ | $\langle H_1 \rangle$ |
| $E_2$          | $\langle [2, 2], [4, 4], [2] \rangle$ | $\langle G_{4,b}, c_1 \rangle$ | $\langle G_{4,b}, c'_1 \rangle$ | $\langle H'_1 \rangle$ | $N_{-1,0}(2^\infty)$ |

If the isogeny graph associated to the $\mathbb{Q}$-isogeny class of $E$ is of $L_2(2)$ type, then, the $\mathbb{Q}$-isogeny class of $E$ consists of two elliptic curves over $\mathbb{Q}$, $E_1$ and $E_2$ such that $j_{E_1} = j_{E_2} = 1728$ with the following algebraic data:

| Isogeny graph | Torsion configuration | $\rho_{E_1,2^\infty}(G_{\mathbb{Q}})$ | $\rho_{E_2,2^\infty}(G_{\mathbb{Q}})$ |
|----------------|----------------------|---------------------------------|---------------------------------|
| $E_1$          | $\langle 2, [2] \rangle$ | $\langle G_{2,b}, c_1 \rangle$ | $\langle G_{2,b}, c'_1 \rangle$ |
| $E_2$          | $\langle [2, 2], [2, 4] \rangle$ | $\langle G_{4,c}, c_1 \rangle$ | $\langle G_{4,c}, c'_1 \rangle$ |
| $E_3$          | $\langle [2, 2], [4, 4] \rangle$ | $\langle G_{4,d}, c_1 \rangle$ | $\langle G_{4,d}, c'_1 \rangle$ |
|                | $\langle N_{-1,0}(2^\infty) \rangle$ | $\langle N_{-1,0}(2^\infty) \rangle$ |

**Proof.** Let $E/\mathbb{Q}$ be an elliptic curve with $j_E = 1728$. Then $E$ has CM by an order of $K = \mathbb{Q}(i)$ with discriminant $\Delta_K = -4$ and conductor $f = 1$. Then $\delta = \frac{\Delta_K f^2}{4} = -1$. By Theorem 3.1, $\rho_{E,2^\infty}(G_{\mathbb{Q}})$ is conjugate to a subgroup of $N_{-1,0}(2^\infty) = \langle G_1, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \rangle$. More precisely, by Theorem 3.6, $\rho_{E,2^\infty}(G_{\mathbb{Q}})$ is generated by one of $G_1$, $G_{2,a}$, $G_{2b}$, $G_{4,a}$, $G_{4,b}$, $G_{4,c}$, $G_{4,d}$, and one element of $\Gamma$.

First note that

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}.$$
Let $\gamma, \gamma' \in \Gamma$. By the fact that $G_1$ contains $-\text{Id}$ and $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, we have that $\langle G_1, \gamma \rangle = \langle G_1, \gamma' \rangle = N_{-1,0}(2^\infty)$.

By the fact that $G_{2,a}$ and $G_{2,b}$ contain $-\text{Id}$, $\langle G_{2,a}, c_1 \rangle = \langle G_{2,a}, c_{-1} \rangle$ and $\langle G_{2,b}, c_1 \rangle = \langle G_{2,b}, c_{-1} \rangle$. Similarly, $\langle G_{2,a}, c'_1 \rangle = \langle G_{2,a}, c'_{-1} \rangle$ and $\langle G_{2,b}, c'_1 \rangle = \langle G_{2,b}, c'_{-1} \rangle$. Note that

$$\langle G_{4,a}, c_1 \rangle = \langle 5 \cdot \text{Id}, \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}, c_1 \rangle = \langle 5 \cdot \text{Id}, c_1 \cdot \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}^{-1} c_1 \rangle = \langle 5 \cdot \text{Id}, \begin{bmatrix} 1 & -2 \\ -2 & 1 \end{bmatrix}, c_1 \rangle.$$ 

After switching the orders of the generators of $\langle G_{4,a}, c_1 \rangle$, we see that this last group is conjugate to the group

$$\langle 5 \cdot \text{Id}, \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}, c_{-1} \rangle = \langle G_{4,a}, c_{-1} \rangle.$$ 

Hence, $\langle G_{4,a}, c_1 \rangle$ is conjugate to $\langle G_{4,a}, c_{-1} \rangle$.

Next, note that $\langle G_{4,a}, c'_1 \rangle = \langle 5 \cdot \text{Id}, \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \rangle$ is conjugate to the group

$$\langle 5 \cdot \text{Id}, c_1 \cdot \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}^{-1} c_1, c_1 \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1} c_1 \rangle = \langle 5 \cdot \text{Id}, \begin{bmatrix} 1 & -2 \\ -2 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \rangle.$$ 

After switching the order of the generators, this last group is conjugate to $\langle 5 \cdot \text{Id}, \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \rangle = \langle G_{4,a}, c'_{-1} \rangle$. Hence, $\langle G_{4,a}, c'_1 \rangle$ is conjugate to $\langle G_{4,a}, c'_{-1} \rangle$.

Making similar computations, we see that $\langle G_{4,x}, c_1 \rangle$ is conjugate to $\langle G_{4,x}, c_{-1} \rangle$ and $\langle G_{4,x}, c'_1 \rangle$ is conjugate to $\langle G_{4,x}, c'_{-1} \rangle$ for $x = b, c,$ and $d$. Hence, we work with the case that $\rho_{E,2^\infty}(G_Q)$ is conjugate to $N_{-1,0}(2^\infty)$, $\langle G_{2,a}, c_1 \rangle$, $\langle G_{2,a}, c'_1 \rangle$, $\langle G_{2,b}, c_1 \rangle$, $\langle G_{2,b}, c'_1 \rangle$, $\langle G_{4,a}, c_1 \rangle$, $\langle G_{4,a}, c'_1 \rangle$, $\langle G_{4,b}, c_1 \rangle$, $\langle G_{4,b}, c'_1 \rangle$, $\langle G_{4,c}, c_1 \rangle$, $\langle G_{4,c}, c'_1 \rangle$, $\langle G_{4,d}, c_1 \rangle$, or $\langle G_{4,d}, c'_1 \rangle$.

If $\rho_{E,2^\infty}(G_Q)$ is conjugate to $\langle G_{2,a}, c_1 \rangle$, $\langle G_{4,a}, c_1 \rangle$, or $\langle G_{4,b}, c_1 \rangle$, then $\rho_{E,2^\infty}(G_Q)$ reduces modulo 2 to the trivial group and hence, $E$ has full two-torsion defined over $\mathbb{Q}$. Moreover, $\langle G_{2,a}, c_1 \rangle$ is the only group of those three which contains $-\text{Id}$ and $\langle G_{2,a}, c_1 \rangle = \langle G_{4,a}, c_{1,-1}\rangle = \langle G_{4,b}, c_{1,-1}\rangle$. In other words, $\langle G_{2,a}, c_1 \rangle$, $\langle G_{4,a}, c_1 \rangle$, and $\langle G_{4,b}, c_1 \rangle$ are quadratic twists.

Next, if $\rho_{E,2^\infty}(G_Q)$ is conjugate to one of $\langle G_{2,a}, c'_1 \rangle$, $\langle G_{4,a}, c'_1 \rangle$, or $\langle G_{4,b}, c'_1 \rangle$, then using magma [2], we see that $\rho_{E,2^\infty}(G_Q)$ is conjugate to a subgroup of $\left\{ \begin{bmatrix} *, * \\ 0, * \end{bmatrix} \right\} \subseteq \text{GL}(2, \mathbb{Z}/4\mathbb{Z})$. Thus, $E$ has a cyclic, $Q$-rational subgroup of order 4 that generates a $Q$-rational 4-isogeny with cyclic kernel. Moreover, $\langle G_{2,a}, c'_1 \rangle$ is the only group of those three which contains $-\text{Id}$ and $\langle G_{2,a}, c'_1 \rangle = \langle G_{4,a}, c'_1, -\text{Id} \rangle = \langle G_{4,b}, c'_1, -\text{Id} \rangle$. In other words, $\langle G_{2,a}, c'_1 \rangle$, $\langle G_{4,a}, c'_1 \rangle$, and $\langle G_{4,b}, c'_1 \rangle$ are quadratic twists.

On the other hand, if $\rho_{E,2^\infty}(G_Q)$ is conjugate to any one of the remaining seven groups, $N_{-1,0}(2^\infty)$, $\langle G_{2,b}, c_1 \rangle$, $\langle G_{2,b}, c'_1 \rangle$, $\langle G_{4,c}, c_1 \rangle$, $\langle G_{4,c}, c'_1 \rangle$, $\langle G_{4,d}, c_1 \rangle$, or $\langle G_{4,d}, c'_1 \rangle$ then $E(\mathbb{Q})_{\text{tore}} \cong \mathbb{Z}/2\mathbb{Z}$ and $E$ does not have a cyclic, $Q$-rational subgroup of order 4. Of those seven groups $N_{-1,0}(2^\infty)$, $\langle G_{2,b}, c_1 \rangle$, and $\langle G_{2,b}, c'_1 \rangle$ contain $-\text{Id}$. Moreover, $\langle G_{2,b}, c_1 \rangle = \langle G_{4,c}, c_{1,-1}\rangle = \langle G_{4,d}, c_{1,-1}\rangle$ and $\langle G_{2,b}, c'_1 \rangle = \langle G_{4,c}, c'_{1,-1}\rangle = \langle G_{4,d}, c'_{1,-1}\rangle$. In other words, $\langle G_{2,b}, c_1 \rangle$, $\langle G_{4,c}, c_1 \rangle$, and $\langle G_{4,d}, c_1 \rangle$ are quadratic twists and $\langle G_{2,b}, c'_1 \rangle$, $\langle G_{4,c}, c'_1 \rangle$, and $\langle G_{4,d}, c'_1 \rangle$ are quadratic twists.

First, we will find examples of elliptic curves over $\mathbb{Q}$ whose 2-adic Galois image is conjugate to $\langle G_{2,a}, c'_1 \rangle$, $\langle G_{4,a}, c'_1 \rangle$, and $\langle G_{4,b}, c'_1 \rangle$; the groups that can serve as the 2-adic Galois image attached to an elliptic curve over $\mathbb{Q}$ with $j$-invariant equal to 1728 with a cyclic, $Q$-rational subgroup of order 4, and then classify the 2-adic Galois image of the elliptic curves in their $Q$-isogeny classes. In this case, the isogeny graph associated to the $Q$-isogeny class is of $T_4$ type and $E$ is represented by the elliptic curve labeled $E_2$ (see below):
Example 9.8 in [1] says that for $E = E_2 : y^2 = x^3 + 9x$, $j_{E_2} = 1728$, and $\rho_{E,2^\infty}(G_0)$ is conjugate to $\langle G_{2,a}, c'_1 \rangle$. The $\mathbb{Q}$-isogeny class of $E$ has LMFDB label 576.c. The isogeny-torsion graph associated to 576.c is of type $T_4$ with torsion configuration ([2], [2], [2], [2]). All elliptic curves in the $\mathbb{Q}$-isogeny class of $E$ have CM by an order of $K = \mathbb{Q}(i)$ with discriminant $\Delta_K = -4$.

1. The elliptic curve $E_1/Q$ with LMFDB label 576.c3 is 2-isogenous to $E = E_2$. Moreover, $j_{E_1} = 1728$ and $E_1(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. By Lemma 2.23, $\rho_{E_1,2^\infty}(G_0)$ contains $-\text{Id}$ and hence, $\rho_{E_1,2^\infty}(G_0)$ is conjugate to $\langle G_{2,a}, c'_1 \rangle$.

2. The elliptic curve $E_3/Q$ with LMFDB label 576.c1 is 4-isogenous to $E = E_2$ and $j_{E_3} = 287496$. Using code provided by Lozano-Robledo, we see that $E_3$ has CM by an order of $K = \mathbb{Q}(i)$ with discriminant $\Delta_K = -4$ and conductor $f = 2$. Hence, $\delta = \frac{\Delta_{K} \cdot f^2}{4} = -4$ and $\phi = 0$. By Theorem 3.2, $\rho_{E_3,2^\infty}(G_0)$ is contained in $N_{-4,0}(2^\infty)$. Moreover, $\rho_{E_3,2^\infty}(G_0)$ is a group of level 4 and $\bar{\rho}_{E_3}(G_0)$ is a group of order 16 in $\text{GL}(2,\mathbb{Z}/4\mathbb{Z})$. The reduction of $N_{-4,0}(2^\infty)$ modulo 4 is a group of order 16. In other words, $\rho_{E_3,2^\infty}(G_0)$ is conjugate to $N_{-4,0}(2^\infty)$.

3. The elliptic curve $E_4/Q$ with LMFDB label 576.c2 is 4-isogenous to $E = E_2$. Moreover, $j_{E_4} = 287496$. Thus, it is a quadratic twist of $E_3$. By Corollary 2.23, $\rho_{E_4,2^\infty}(G_0)$ contains $-\text{Id}$. Thus, $\rho_{E_4,2^\infty}(G_0)$ is also conjugate to $N_{-4,0}(2^\infty)$ as the only quadratic twist of $N_{-4,0}(2^\infty)$ that contains $-\text{Id}$ is $N_{-4,0}(2^\infty)$ itself.

Example 9.8 in [1] says that for $E = E_2 : y^2 = x^3 + x$, $j_{E_2} = 1728$, and $\rho_{E,2^\infty}(G_0)$ is conjugate to $\langle G_{4,a}, c'_1 \rangle$. The $\mathbb{Q}$-isogeny class of $E$ has LMFDB label 64.a. The isogeny-torsion graph associated to 64.a is of type $T_4$ with torsion configuration ([2], [2], [2], [2]) (note that in this case, one of the elliptic curves with $j$-invariant $= 287496$ has a point of order 4 defined over $\mathbb{Q}$). Note that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$. All elliptic curves in the $\mathbb{Q}$-isogeny class of $E$ have CM by an order of $K = \mathbb{Q}(i)$ with discriminant $\Delta_K = -4$.

1. The elliptic curve $E_1/Q$ with LMFDB label 64.a3 is 2-isogenous to $E = E_2$. Moreover, $E_1$ is isomorphic to the elliptic curve $y^2 = x^3 - 4x$, $j_{E_1} = 1728$, and $E_1(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. By Example 9.8 in [1], $\rho_{E_1,2^\infty}(G_0)$ is conjugate to $\langle G_{4,a}, c'_1 \rangle$.

2. The elliptic curve $E_3/Q$ with LMFDB label 64.a2 is 4-isogenous to $E = E_2$. Moreover, $E_3$ is isomorphic to the elliptic curve $y^2 = x^3 - 44x + 112$, $j_{E_3} = 287496$, and $E_3(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z}$. The elliptic curve $E_3$ has CM by an order of $K = \mathbb{Q}(i)$ with $\Delta_K = -4$ and conductor $f = 2$. Thus, $\delta = \frac{\Delta_{K} \cdot f^2}{4} = -4$. By Example 9.4 in [1], $\rho_{E_3,2^\infty}(G_0)$ is conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -4 & 1 \end{pmatrix} \subseteq N_{-4,0}(2^\infty) \subseteq \text{GL}(2,\mathbb{Z})$.

3. The elliptic curve $E_4/Q$ with LMFDB label 64.a1 is 4-isogenous to $E = E_2$. Moreover, $E_4$ is isomorphic to the elliptic curve $y^2 = x^3 - 44x - 112$, $j_{E_4} = 287496$, and $E_4(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$. The elliptic curve $E_4$ has CM by an order of $K = \mathbb{Q}(i)$ with $\Delta_K = -4$ and conductor $f = 2$. Thus, $\delta = \frac{\Delta_{K} \cdot f^2}{4} = -4$. By Example 9.4 in [1], $\rho_{E_4,2^\infty}(G_0)$ is conjugate to $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -4 & 1 \end{pmatrix} \subseteq N_{-4,0}(2^\infty) \subseteq \text{GL}(2,\mathbb{Z})$.
Example 9.8 in [1] says that for $E = E_2 : y^2 = x^3 + 4x$, $j_{E_2} = 1728$, and $\rho_{E_2,2\infty}(G_\mathbb{Q})$ is conjugate to $\langle G_{4,b}, c'_1 \rangle$. The $\mathbb{Q}$-isogeny class of $E$ has LMFDB label 32.a. The isogeny-torsion graph associated to 32.a is of type $T_4$ with torsion configuration $(\{2, 2\}, \{4\}, \{2\})$. Note that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. All elliptic curves in the $\mathbb{Q}$-isogeny class of $E$ have CM by an order of $K = \mathbb{Q}(i)$ with discriminant $\Delta_K = -4$.

1. The elliptic curve $E_1/\mathbb{Q}$ with LMFDB label 32.a3 is 2-isogenous to $E = E_2$. Moreover, $E_1$ is isomorphic to the elliptic curve $y^2 = x^3 - x, j_{E_1} = 1728$, and $E_1(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. By Example 9.8 in [1], $\rho_{E_1,2\infty}(G_\mathbb{Q})$ is conjugate to $\langle G_{4,b}, c_1 \rangle$.

2. The elliptic curve $E_3/\mathbb{Q}$ with LMFDB label 32.a2 is 4-isogenous to $E = E_2$. Moreover, $E_3$ is isomorphic to the elliptic curve $y^2 = x^3 - 11x + 14, j_{E_3} = 287496$, and $E_3(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z}$. Moreover, $E_3$ has CM by an order of $K = \mathbb{Q}(i)$ with $\Delta_K = -4$ and conductor $f = 2$. Thus, $\delta = \frac{\Delta_K f^2}{4} = -4$. By Example 9.4 in [1], $\rho_{E_3,2\infty}(G_\mathbb{Q})$ is conjugate to $\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 4 & -1 \end{bmatrix} \rangle \subseteq \mathcal{N}_{-4,0}(2^\infty) \subseteq \text{GL}(2, \mathbb{Z}_2)$.

3. The elliptic curve $E_4/\mathbb{Q}$ with LMFDB label 32.a1 is 4-isogenous to $E = E_2$. Moreover, $E_4$ is isomorphic to the elliptic curve $y^2 = x^3 - 11x - 14, j_{E_4} = 287496$, and $E_4(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$. The elliptic curve $E_4$ has CM by an order of $K = \mathbb{Q}(i)$ with $\Delta_K = -4$ and conductor $f = 2$. Thus, $\delta = \frac{\Delta_K f^2}{4} = -4$. By Example 9.4 in [1], $\rho_{E_4,2\infty}(G_\mathbb{Q})$ is conjugate to the group $\langle \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 4 & -1 \end{bmatrix} \rangle \subseteq \mathcal{N}_{-4,0}(2^\infty) \subseteq \text{GL}(2, \mathbb{Z}_2)$.

Now we move on to classify the 2-adic Galois image of isogeny-torsion graphs of $L_2(2)$ type with CM whose elliptic curves have $j$-invariant equal to 1728. Up to conjugation, there are seven possible 2-adic Galois images, $\mathcal{N}_{-1,0}(2^\infty), \langle G_{2,b}, c_1 \rangle, \langle G_{2,b}, c'_1 \rangle, \langle G_{4,c}, c_1 \rangle, \langle G_{4,c}, c'_1 \rangle, \langle G_{4,d}, c_1 \rangle, \langle G_{4,d}, c'_1 \rangle$. We will prove that there are four distinct arrangements. In this case, the $\mathbb{Q}$-isogeny class of $E$ has two curves, both elliptic curves have $j$-invariant equal to 1728, and the isogeny graph associated to the $\mathbb{Q}$-isogeny class of $E$ is of $L_2(2)$ type (see below):

$$
\begin{array}{c}
E_1 \\
\quad \rightarrow \quad \quad \quad E_2
\end{array}
$$

1. $\langle G_{2,b}, c_{-1} \rangle$ and $\langle G_{2,b}, c'_{-1} \rangle$

Let $E_1 : y^2 = x^2 + 18x$, let $E_2 : y^2 = x^3 - 72x$, let $E'_1 : y^2 = x^3 - 18x$, and let $E'_2 : y^2 = x^3 + 72x$. Then $E_1$ is 2-isogenous to $E_2$ and $E'_1$ is 2-isogenous to $E'_2$. By Example 9.8 in [1], $\rho_{E_1,2\infty}(G_\mathbb{Q})$ is conjugate to $\langle G_{2,b}, c'_{-1} \rangle$ and $\rho_{E_2,2\infty}(G_\mathbb{Q})$ is conjugate to $\langle G_{2,b}, c_{-1} \rangle$.

We claim that $\rho_{E_1,2\infty}(G_\mathbb{Q})$ is conjugate to $\langle G_{2,b}, c_{-1} \rangle$ and $\rho_{E_2,2\infty}(G_\mathbb{Q})$ is conjugate to $\langle G_{2,b}, c'_{-1} \rangle$. Note that $E_1$ is a quadratic twist of $E'_2$ (by 2) and $E_2$ is a quadratic twist of $E'_1$ (by 2). By Corollary 2.23, $\rho_{E_2,2\infty}(G_\mathbb{Q})$ and $\rho_{E_2,2\infty}(G_\mathbb{Q})$ contain -Id. The only quadratic twist of $\langle G_{2,b}, c_{-1} \rangle$ that contains -Id is $\langle G_{2,b}, c_{-1} \rangle$ itself and the only quadratic twist of $\langle G_{2,b}, c'_{-1} \rangle$ that contains -Id is $\langle G_{2,b}, c'_{-1} \rangle$ itself.

2. $\langle G_{4,c}, c_1 \rangle$ and $\langle G_{4,c}, c'_1 \rangle$

Let $E_1 : y^2 = x^2 + 2x$ and let $E_2 : y^2 = x^3 - 8x$. Then $E_1$ is 2-isogenous to $E_2$. By Example 9.8 in [1], $\rho_{E_1,2\infty}(G_\mathbb{Q})$ is conjugate to $\langle G_{4,c}, c'_1 \rangle$ and $\rho_{E_2,2\infty}(G_\mathbb{Q})$ is conjugate to $\langle G_{4,c}, c_1 \rangle$.

3. $\langle G_{4,d}, c_1 \rangle$ and $\langle G_{4,d}, c'_1 \rangle$

Let $E_1 : y^2 = x^2 - 2x$ and let $E_2 : y^2 = x^3 + 8x$. Then $E_1$ is 2-isogenous to $E_2$. By Example 9.8 in [1], $\rho_{E_1,2\infty}(G_\mathbb{Q})$ is conjugate to $\langle G_{4,d}, c_1 \rangle$ and $\rho_{E_2,2\infty}(G_\mathbb{Q})$ is conjugate to $\langle G_{4,d}, c'_1 \rangle$.

4. $\mathcal{N}_{-1,0}(2^\infty)$

Let $E_1/\mathbb{Q}$ be an elliptic curve with $j_{E_1} = 1728$ such that $\rho_{E_1,2\infty}(G_\mathbb{Q})$ is conjugate to $\mathcal{N}_{-1,0}(2^\infty)$. Then the isogeny graph associated to the $\mathbb{Q}$-class of $E_1$ is of $L_2(2)$ type and $E_1$ is 2-isogenous to an elliptic curve $E_2/\mathbb{Q}$ with $j_{E_2} = 1728$. A priori, $\rho_{E_2,2\infty}(G_\mathbb{Q})$ is conjugate to one of the seven
groups, $\mathcal{N}_{-1,0}(2^\infty)$, $\langle G_{2,b}, c_1 \rangle$, $\langle G_{2,b}, c'_1 \rangle$, $\langle G_{4,c}, c_1 \rangle$, $\langle G_{4,c}, c'_1 \rangle$, $\langle G_{4,d}, c_1 \rangle$, or $\langle G_{4,d}, c'_1 \rangle$. We have eliminated six out of the seven possibilities. Hence, $\rho_{E,2^\infty}(G_{Q})$ is conjugate to $\mathcal{N}_{-1,0}(2^\infty)$. Let $E$ be the elliptic curve $y^2 = x^3 + 3x$. Then by Example 9.8 in [1], $\rho_{E,2^\infty}(G_{Q})$ is conjugate to $\mathcal{N}_{-1,0}(2^\infty)$.

□

References

[1] Álvaro Lozano-Robledo. Galois representations attached to elliptic curves with complex multiplication. arXiv: Number Theory, 2018. 3, 3.1, 3.2, 3.3, 3.6, 3.7, 4, 4, 4, 1, 2, 3, 4, 1, 2, 3, 1, 2, 3, 4
[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
[3] Garen Chiloyan and Álvaro Lozano-Robledo. A classification of isogeny-torsion graphs of $\mathbb{Q}$-isogeny classes of elliptic curves. Trans. London Math. Soc., 8(1):1–34, 2021. 1, 1.2, 1, 1.3, 1, 2.1
[4] Monsur Akangbe Kenku. On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class. J. Number Theory, 15(2):199–202, 1982.
[5] Álvaro Lozano-Robledo. On the field of definition of $p$-torsion points on elliptic curves over the rationals. Math. Ann., 357(1):279–305, 2013.
[6] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math., 44(2):129–162, 1978.
[7] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. $\ell$-adic images of galois for elliptic curves over $\mathbb{Q}$ (and an appendix with john voight). Forum of Mathematics, Sigma, 10:e62, 2022.
[8] J. H. Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer, Dordrecht, second edition, 2009.

Email address: garen.chiloyan@gmail.com
URL: https://sites.google.com/view/garenmath/home