A Classification of Rational Isogeny-Torsion Graphs

Garen Chiloyan

UConn

October 5th, 2019

Elliptic Curves

Definition

A rational elliptic curve, $E/\mathbb{Q}$, is a smooth projective curve of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$ with a point at infinity defined over $\mathbb{Q}$, $\mathcal{O} = [0 : 1 : 0]$.

Elliptic Curves

Definition

A rational elliptic curve, $E/\mathbb{Q}$, is a smooth projective curve of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$ with a point at infinity defined over $\mathbb{Q}$, $\mathcal{O} = [0 : 1 : 0]$.

Theorem (Mordell–Weil, 1922)

Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})$ is a finitely generated abelian group, i.e., $E(\mathbb{Q})_{tors}$ is finite abelian and $E(\mathbb{Q}) \cong \mathbb{Z}^{R_{E/\mathbb{Q}}} \times E(\mathbb{Q})_{tors}$.

Elliptic Curves

Definition

A rational elliptic curve, $E/\mathbb{Q}$, is a smooth projective curve of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$ with a point at infinity defined over $\mathbb{Q}$, $\mathcal{O} = [0 : 1 : 0]$.

Theorem (Mordell–Weil, 1922)

Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})$ is a finitely generated abelian group, i.e., $E(\mathbb{Q})_{tors}$ is finite abelian and $E(\mathbb{Q}) \cong \mathbb{Z}^{R_{E/\mathbb{Q}}} \times E(\mathbb{Q})_{tors}$.

Theorem (Mazur, 1978)

$E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups

$$\mathbb{Z}/M\mathbb{Z} \text{ with } 1 \leq M \leq 10 \text{ or } M = 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \text{ with } 1 \leq N \leq 4$$

Isogenies

Definition

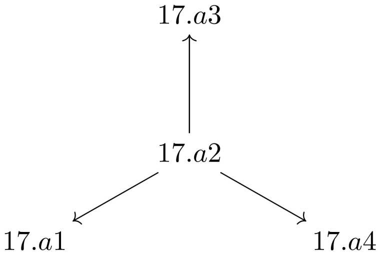
Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be elliptic curves. An **isogeny** mapping E to E' is a morphism $\phi\colon E \to E'$ such that $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$. E and E' are said to be **isogenous** if there exists a nonconstant isogeny from E to E'. The set of all elliptic curves isogenous to E is called the **isogeny class of** E.

Definition

Let $E/\mathbb{Q}$ be a rational elliptic curve. The **isogeny graph** of E is a visualization of the isogeny class of E with edges being rational isogenies generated by the finite cyclic $\mathbb{Q}$-rational subgroups of E and vertices being pairwise non-isomorphic rational elliptic curves isogenous to E that are generated by the finite cyclic $\mathbb{Q}$-rational subgroups of E.

Example of Rational Isogeny Graph

Let $E/\mathbb{Q} : y^2 + xy + y = x^3 - x^2 - 6x - 4$ with LMFDB label 17.a2. Then the following is the rational isogeny graph of E:



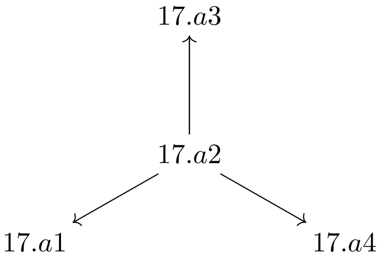
Motivating Examples: Isogeny-Torsion Graphs

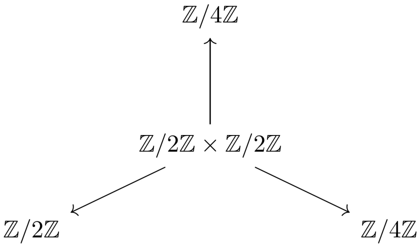
Mazur's theorem establishes the possibilities for $E(\mathbb{Q})_{\text{tors}}$.
Question: What are the possibilities for torsion at every vertex of isogeny graph?

Motivating Examples: Isogeny-Torsion Graphs

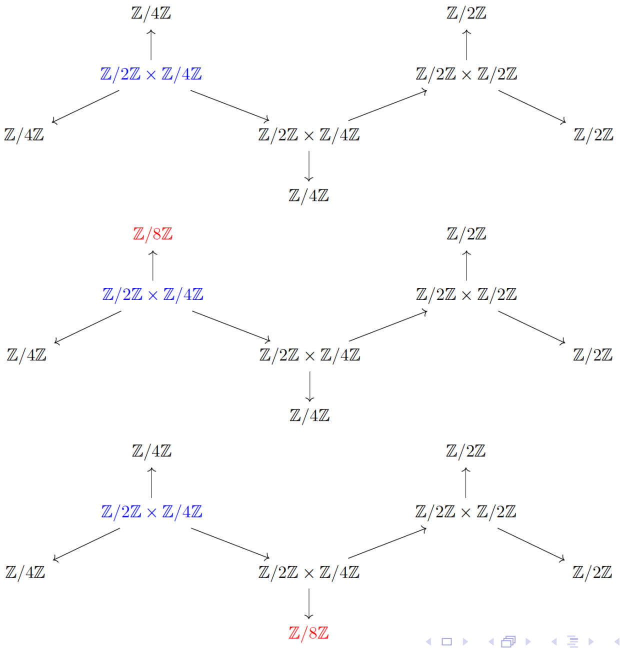
Mazur's theorem establishes the possibilities for $E(\mathbb{Q})_{\text{tors}}$.
Question: What are the possibilities for torsion at every vertex of isogeny graph?

Let $E/\mathbb{Q} : y^2 + xy + y = x^3 - x^2 - 6x - 4$. Then the following are the rational isogeny graph and the rational isogeny-torsion graph of E:



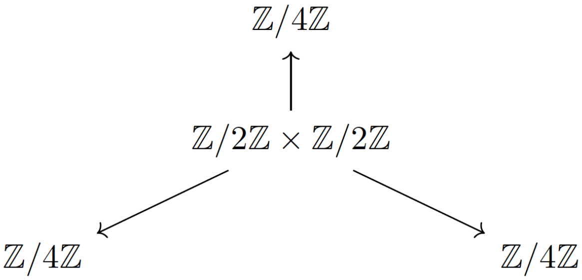


More Examples of Isogeny-Torsion Graphs



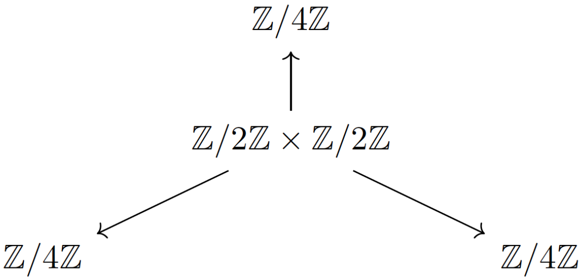
An Opening Question

Is there an example of the following rational isogeny-torsion graph?



An Opening Question

Is there an example of the following rational isogeny-torsion graph?



Answer: **No!**

Main Result

Can we classify ALL rational isogeny-torsion graphs?

In other words, can we classify the size and shape of a rational isogeny graph *and* the torsion groups of its vertices?

Main Result

Can we classify ALL rational isogeny-torsion graphs?

In other words, can we classify the size and shape of a rational isogeny graph *and* the torsion groups of its vertices?

Theorem (C., Lozano-Robledo)

There are at least 37 *and at most* 39 *possible rational isogeny-torsion graphs.*

Work by Mazur and Kenku

Theorem (B. Mazur, 1978)

Let $E/\mathbb{Q}$ be an elliptic curve. A prime degree $\mathbb{Q}$-rational isogeny of E has degree $2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67,$ or 163.

Theorem (M. Kenku, 1982)

Let $E/\mathbb{Q}$ be an elliptic curve. Then there are at most 8 pairwise non-isomorphic rational elliptic curves that are isogenous to E.

Note: There is no analogy to Mazur's or Kenku's theorems for higher degree number fields. $\mathbb{Q}$ is the only number field over which we can classify isogeny-torsion graphs.

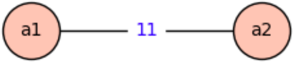
Mazur's and Kenku's theorems give us a classification of the sizes and shapes of all rational isogeny graphs. They are one of the following:

L_k Graphs

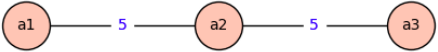
Linear graphs with $k = 1, 2, 3,$ or 4 vertices.

$\{\mathcal{O}\}$

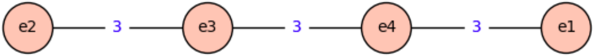
Isogeny Class 37.a



Isogeny Class 121.a



Isogeny Class 11.a

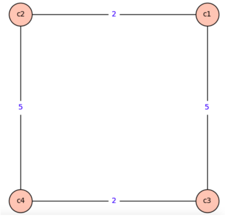


Isogeny Class 432.e

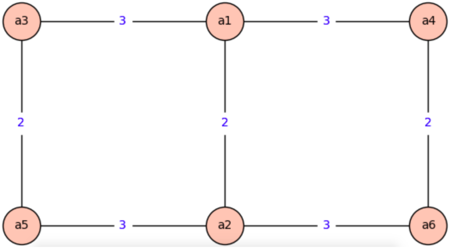
(Images courtesy of the LMFDB.)

R_k Graphs

R_k: **Rectangular** graphs with $k = 4$ or 6 vertices.



Isogeny Class 66.c

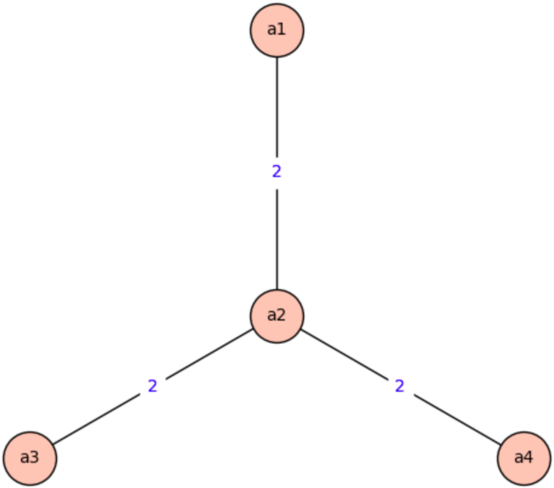


Isogeny Class 14.a

(Images courtesy of the LMFDB.)

T_4 graphs

T_4: Graphs with a single elliptic curve with full two-torsion

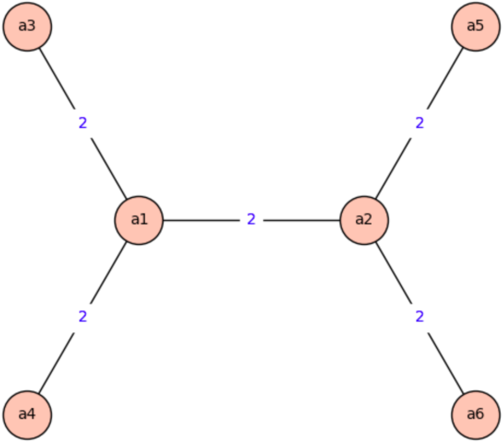


Isogeny Class 17.a

(Image courtesy of the LMFDB.)

T_6 graphs

T_6: Graphs with two rational elliptic curves with full two-torsion and no 3-isogenies

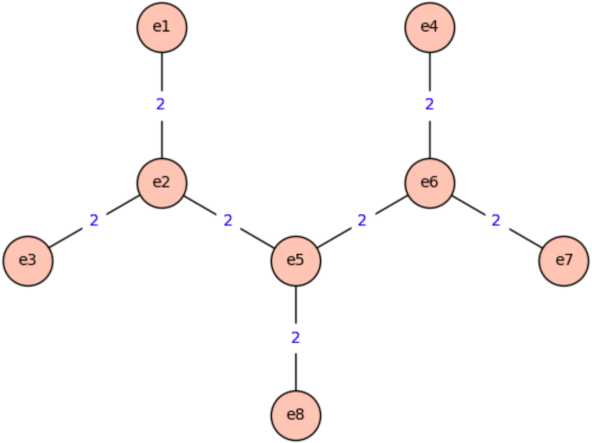


Isogeny Class 21.a

(Image courtesy of the LMFDB.)

T_8 graphs

T_8: Graphs with three rational elliptic curves with full two-torsion

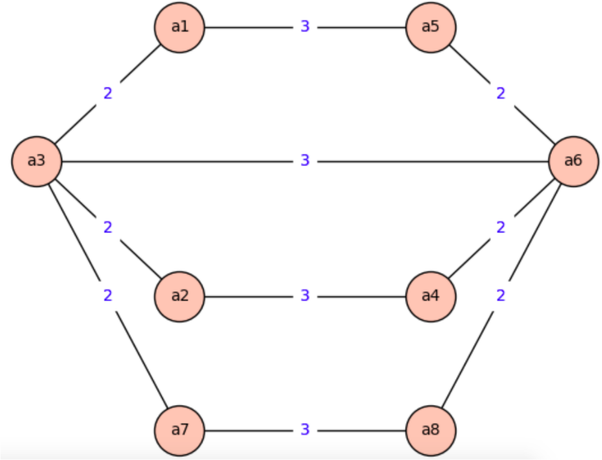


Isogeny Class 210.e

(Image courtesy of the LMFDB.)

S Graphs

S: Graphs with two rational elliptic curves with full two-torsion and a 3-isogeny



Isogeny Class 30.a

(Image courtesy of the LMFDB.)

Classification of all L_k Graphs

For the following, we abbreviate $\mathbb{Z}/a\mathbb{Z} = [a]$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} = [2, b]$

Graph Type	Isomorphism Types	LMFDB Label
L_1	([1])	37.a
L_2	([1],[1])	75.c
	([2],[2])	46.a
	([3],[1])	44.a
	([5],[1])	38.b
	([7],[1])	26.b
L_3	([1],[1],[1])	99.d
	([3],[3],[1])	19.a
	([5],[5],[1])	11.a
	([9],[3],[1])	54.b
L_4	([1],[1],[1],[1])	432.e
	([3],[3],[3],[1])	27.a

TABLE 2. The list of all L_k rational-isogeny graphs

Classification of all R_k Graphs

Graph Type	Isomorphism Types	LMFDB Label
R_4	([1],[1],[1],[1])	400.f
	([2],[2],[2],[2])	49.a
	([3],[3],[1],[1])	50.a
	([5],[5],[1],[1])	50.b
	([6],[6],[2],[2])	20.a
	([10],[10],[2],[2])	66.c
R_6	([2],[2],[2],[2],[2],[2])	98.a
	([6],[6],[6],[6],[2],[2])	14.a

TABLE 4. The list of all R_k rational-isogeny graphs

Classification of all T_k Graphs

Graph Type	Isomorphism Types	LMFDB Label
T_4	([2,2], [2], [2], [2])	120.a
	([2,2], [2], [4], [2])	33.a
	([2,2], [2], [4], [4])	17.a
T_6	([2,4],[4],[4],[2,2],[2],[2])	24.a
	([2,4],[8],[4],[2,2],[2],[2])	21.a
	([2,2],[2],[2],[2,2],[2],[2])	126.a
	([2,2],[4],[2],[2,2],[2],[2])	63.a
T_8	([2,8],[8],[8],[2,4],[4],[2,2],[2],[2])	210.e
	([2,4],[4],[4],[2,4],[4],[2,2],[2],[2])	195.a
	([2,4],[4],[4],[2,4],[8],[2,2],[2],[2])	15.a
	([2,4],[8],[4],[2,4],[4],[2,2],[2],[2])	1230.f
	([2,2],[2],[2],[2,2],[2],[2,2],[2],[2])	45.a
	([2,2],[4],[2],[2,2],[2],[2,2],[2],[2])	75.b

TABLE 3. The list of all T_k rational-isogeny graphs

Classification of all S Graphs

Graph Type	Isomorphism Types	LMFDB Label
S	([2,2],[2],[2],[2],[2,2],[2],[2],[2])	240.b
	([2,2],[2],[2],[4],[2,2],[2],[2],[4])	150.b
	([2,2],[2],[4],[4],[2,2],[2],[4],[4])	X
	([2,6],[6],[6],[6],[2,2],[2],[2],[2])	30.a
	([2,6],[6],[6],[12],[2,2],[2],[2],[4])	90.c
	([2,2],[6],[12],[12],[2,2],[2],[4],[4])	X

TABLE 5. The list of all (possible) S rational-isogeny graphs

Examples of 21-isogenies

Let $E/\mathbb{Q}$ be an elliptic curve with a finite cyclic $\mathbb{Q}$-rational group of order 21. Then there exist examples of the following rational isogeny-torsion graphs:

$$\begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} & \longrightarrow & \mathcal{O} \\ \downarrow & & \downarrow \\ \mathbb{Z}/3\mathbb{Z} & \longrightarrow & \mathcal{O} \end{array}$$

Isogeny Class 162.b

$$\begin{array}{ccc} \mathcal{O} & \longrightarrow & \mathcal{O} \\ \downarrow & & \downarrow \\ \mathcal{O} & \longrightarrow & \mathcal{O} \end{array}$$

Isogeny Class 1296.f

Non-examples of 21-isogenies

The following rational isogeny-torsion graphs do not occur.

$$\begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} & \longrightarrow & \mathcal{O} \\ \downarrow & & \downarrow \\ \mathcal{O} & \longrightarrow & \mathbb{Z}/3\mathbb{Z} \end{array}$$

$$\begin{array}{ccc} \mathbb{Z}/7\mathbb{Z} & \longrightarrow & \mathcal{O} \\ \downarrow & & \downarrow \\ \mathbb{Z}/7\mathbb{Z} & \longrightarrow & \mathcal{O} \end{array}$$

27-isogenies

The following two examples of rational isogeny-torsion graphs with 27-isogenies exist.

$$\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathcal{O}$$

LMFDB Label 27.a

$$\mathcal{O} \longrightarrow \mathcal{O} \longrightarrow \mathcal{O} \longrightarrow \mathcal{O}$$

LMFDB Label 432.e

27-isogenies

The following two examples of rational isogeny-torsion graphs with 27-isogenies exist.

$$\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathcal{O}$$

LMFDB Label 27.a

$$\mathcal{O} \longrightarrow \mathcal{O} \longrightarrow \mathcal{O} \longrightarrow \mathcal{O}$$

LMFDB Label 432.e

The following rational isogeny-torsion graph does not occur.

$$\mathbb{Z}/9\mathbb{Z} \longrightarrow \mathbb{Z}/9\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathcal{O}$$

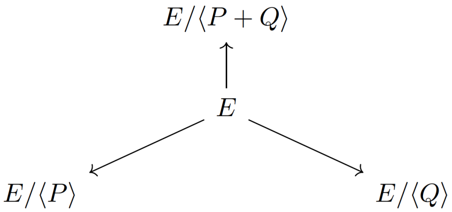
Reasoning: All rational 27-isogenies are CM corresponding to one j-invariant and no twists of this curve produce this graph.

An Example: Classification of T_4 Graphs (1)

Let $E/\mathbb{Q}$ be an elliptic curve. Suppose E has 4 curves in its isogeny class and

$$E(\mathbb{Q})_{\text{tors}} = E[2] = \langle P, Q \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

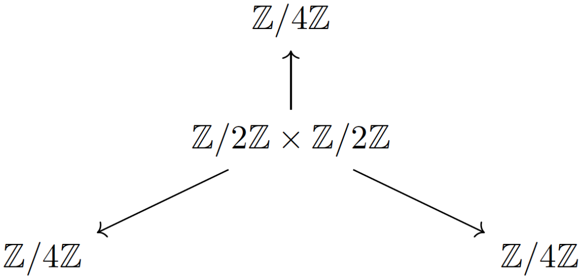
What are the possible isogeny-torsion graphs of E?



- Finite cyclic $\mathbb{Q}$-rational subgroups of E are $\{\mathcal{O}\}, \langle P \rangle, \langle Q \rangle$ and $\langle P+Q \rangle$.
- $(E/\langle P \rangle)(\mathbb{Q})_{\text{tors}}, (E/\langle Q \rangle)(\mathbb{Q})_{\text{tors}}$, and $(E/\langle P+Q \rangle)(\mathbb{Q})_{\text{tors}}$ are cyclic.
- E has a point of order 2 defined over $\mathbb{Q}$, thus all isogenous curves do too, but because $C(E) = 4$, no curve can have a point of order 8 defined over $\mathbb{Q}$. No points of odd order defined over $\mathbb{Q}$.

Classification of T_4 Graphs (2)

Let's assume the following isogeny-torsion graph exists.



Classification of T_4 Graphs (3)

- Assume E is non-CM and $(E/\langle P\rangle)(\mathbb{Q})_{\text{tors}}, (E/\langle Q\rangle)(\mathbb{Q})_{\text{tors}}$, and $(E/\langle P+Q\rangle)(\mathbb{Q})_{\text{tors}}$, are cyclic of order 4. Then the image of the mod 4 Galois representation of E is conjugate to

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \right\} \in GL_2(\mathbb{Z}/4\mathbb{Z})$$

  but no group in the RZB database of images of 2-adic Galois representations of rational non-CM elliptic curves reduces mod 4 to this group.

Classification of T_4 Graphs (3)

- Assume E is non-CM and $(E/\langle P\rangle)(\mathbb{Q})_{\text{tors}}, (E/\langle Q\rangle)(\mathbb{Q})_{\text{tors}}$, and $(E/\langle P+Q\rangle)(\mathbb{Q})_{\text{tors}}$, are cyclic of order 4. Then the image of the mod 4 Galois representation of E is conjugate to

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}\right\} \in GL_2(\mathbb{Z}/4\mathbb{Z})$$

  but no group in the RZB database of images of 2-adic Galois representations of rational non-CM elliptic curves reduces mod 4 to this group.
- Suppose E is CM. Then there are only finitely many j-invariants that correspond to a torsion subgroup with full two-torsion. No quadratic twist will give you an isogeny-torsion graph with all three $(E/\langle P\rangle)(\mathbb{Q})_{\text{tors}}, (E/\langle Q\rangle)(\mathbb{Q})_{\text{tors}}$, and $(E/\langle P+Q\rangle)(\mathbb{Q})_{\text{tors}}$, cyclic of order 4.

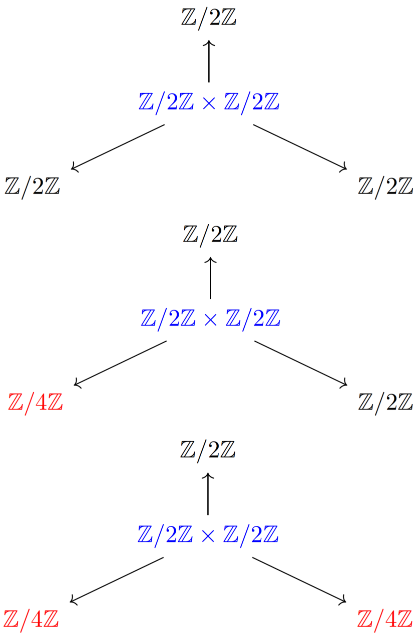
Classification of T_4 Graphs (3)

- Assume E is non-CM and $(E/\langle P\rangle)(\mathbb{Q})_{\text{tors}}, (E/\langle Q\rangle)(\mathbb{Q})_{\text{tors}}$, and $(E/\langle P+Q\rangle)(\mathbb{Q})_{\text{tors}}$, are cyclic of order 4. Then the image of the mod 4 Galois representation of E is conjugate to

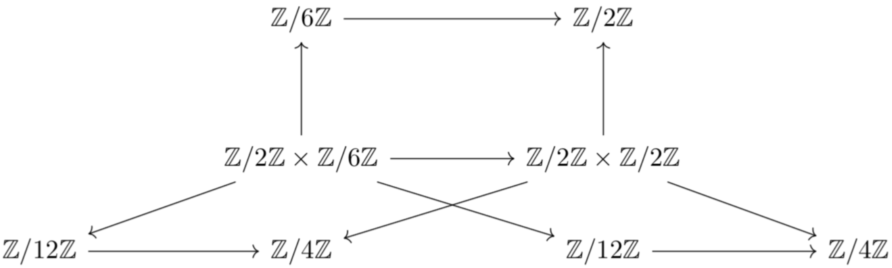
$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \right\} \in GL_2(\mathbb{Z}/4\mathbb{Z})$$

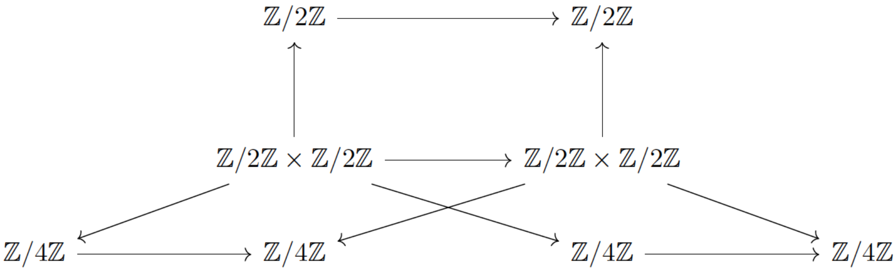
  but no group in the RZB database of images of 2-adic Galois representations of rational non-CM elliptic curves reduces mod 4 to this group.
- Suppose E is CM. Then there are only finitely many j-invariants that correspond to a torsion subgroup with full two-torsion.
  No quadratic twist will give you an isogeny-torsion graph with all three $(E/\langle P\rangle)(\mathbb{Q})_{\text{tors}}, (E/\langle Q\rangle)(\mathbb{Q})_{\text{tors}}$, and $(E/\langle P+Q\rangle)(\mathbb{Q})_{\text{tors}}$, cyclic of order 4.
- Isogeny classes with LMFDB labels $120.a, 33.a$, and $17.a$ correspond to T_4 isogeny graphs with zero, one, and two point-wise rational groups of order 4 respectively.

All T_4 Graphs

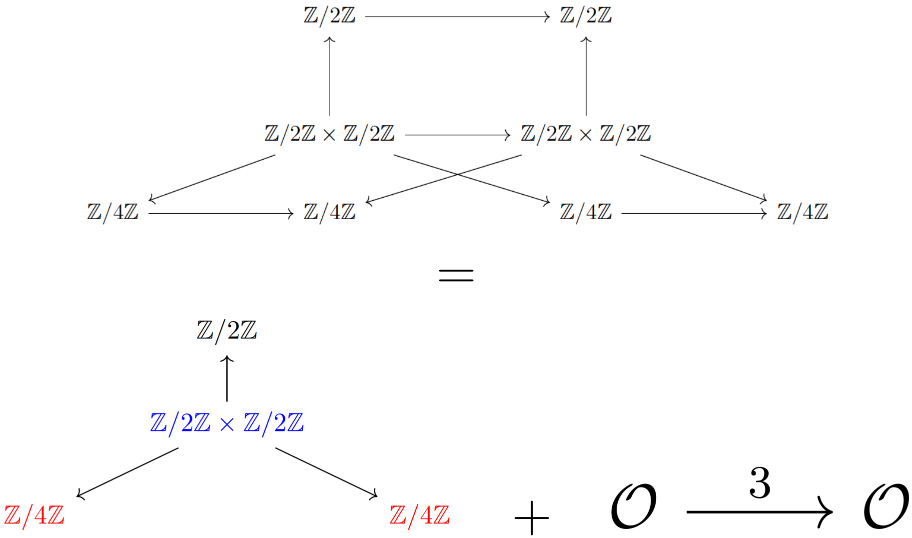


Graphs Not Yet Ruled Out





Attempts at a Full Solution (1)



Attempts at a Full Solution (2)

- The image of the mod 4 Galois representations of the two unconfirmed graphs are conjugate to

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \right\} \in GL_2(\mathbb{Z}/4\mathbb{Z})$$

.

- Find the image in RZB database and get its j-invariant.
- Add a 3-isogeny to these images by comparing it to j-invariant of a curve with a 3-isogeny
- This defines a curve of genus $1, 3$, or 7. And we have not been able to find all rational points of those curves as of yet

Questions?