A Classification of Rational Isogeny-Torsion Graphs over $\mathbb{Q}$

Garen Chiloyan Joint with Álvaro Lozano-Robledo

University of Connecticut

June 13, 2020

Elliptic Curves

Definition

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

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

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

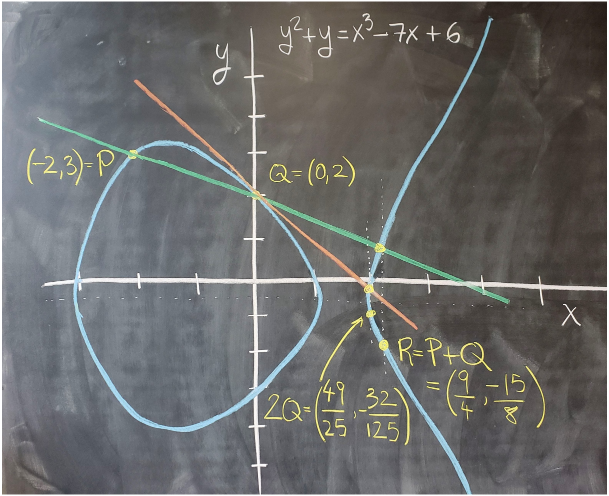
We can dehomogenize to get an affine equation of the form

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

so long as we remember the point at infinity $\mathcal{O}$.

Elliptic Curves as Groups

An elliptic curve has the structure of an abelian group with identity $\mathcal{O}$ under the operation:



$E(\mathbb{Q})$ and $E(\mathbb{Q})_{\text{tors}}$

Definition

Let $E/\mathbb{Q}$ be an elliptic curve. A point $P \in E$ is **defined over** $\mathbb{Q}$ if $P = \mathcal{O}$ or $P = (a, b)$ for some $a, b \in \mathbb{Q}$. The set of all elements of E defined over $\mathbb{Q}$ is denoted $E(\mathbb{Q})$.

Theorem (Mordell-Weil, 1922)

$E(\mathbb{Q})$ is a finitely generated abelian group.

Theorem (Mazur, 1978)

Let $E(\mathbb{Q})_{tors}$ be the set of all elements of $E(\mathbb{Q})$ of finite order. $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups:

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

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \text{ for } N = 2, 4, 6, \text{ or } 8.$$

N-Torsion and Galois Representations

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve and N a positive integer. The set of all elements of E with order divisible by N, denoted $E[N]$, is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

Let $G_{\mathbb{Q}} := Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. $G_{\mathbb{Q}}$ acts on E by $\sigma \cdot (a, b) = (\sigma(a), \sigma(b))$ and fixing the identity $\mathcal{O}$.
The action on E by $G_{\mathbb{Q}}$ commutes with the group operation on E, so $G_{\mathbb{Q}}$ also acts on $E[N]$.

Picking a basis for $E[N]$, we get the mod N representation attached to E

$$\rho_{E,N} \colon G_{\mathbb{Q}} \to Aut(E[N]) \cong GL(2, \mathbb{Z}/N\mathbb{Z})$$

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 $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$. The **degree** of an isogeny is the cardinality of its kernel.
E is said to be **isogenous** to E' if there exists a *non-constant* isogeny mapping E to E'. The set of all elliptic curves isogenous to E is called the **isogeny class of** E.

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve and let H be a finite subgroup of E. There is a unique elliptic curve up to isomorphism, E/H and an isogeny $\phi_H\colon E \to E/H$ such that $\ker(\phi_H) = H$. E/H is said to be **generated** *by H.*
If moreover, $\sigma(H) = H$ for all $\sigma \in G_{\mathbb{Q}}$, then ϕ_H and E/H are rational.
In the case when $\sigma(H) = H$ for all $\sigma \in G_{\mathbb{Q}}$, both H and ϕ_H are said to be **$\mathbb{Q}$-rational***.*

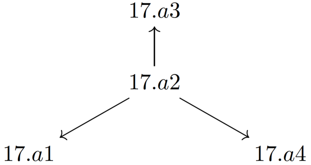
Rational Isogeny Graphs

Definition

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

Example

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:



Initial Questions

Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be isogenous rational elliptic curves.

Questions:

- Given $E(\mathbb{Q})_{\text{tors}}$, what are the possibilities for $E'(\mathbb{Q})_{\text{tors}}$?
- What are the possibilities of rational torsion for each curve isogenous to E?
- What are the possibilities of rational torsion for each vertex of the isogeny graph of E?

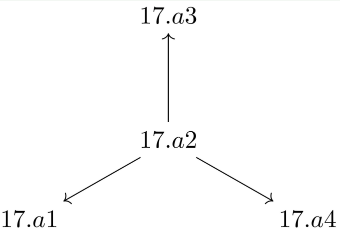
Rational Isogeny-Torsion Graphs

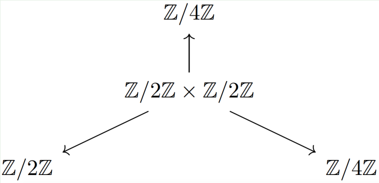
Definition

Let $E/\mathbb{Q}$ be an elliptic curve. The **rational isogeny-torsion graph** of E is the rational isogeny graph of E with the classification of the torsion subgroups of each vertex.

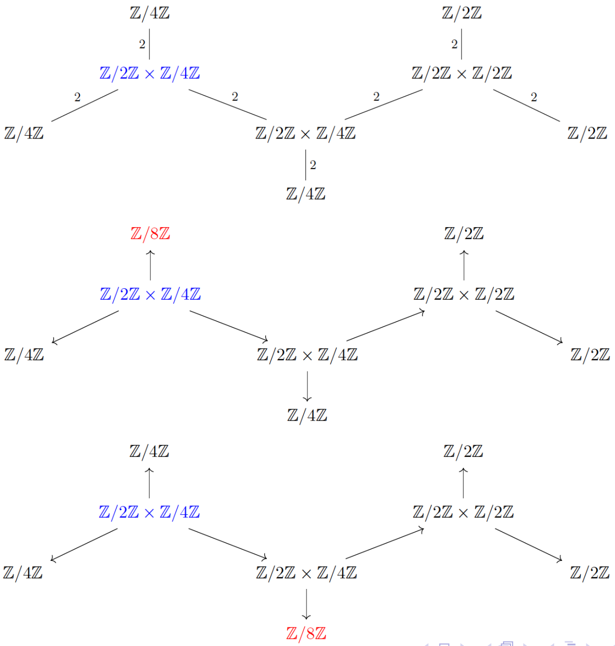
Example

Let $E/\mathbb{Q} : y^2 + xy + y = x^3 - x^2 - 6x - 4.$





More Examples of Isogeny-Torsion Graphs



Classification of Rational Isogeny Graphs

Kenku's theorem (1980) on the classification of the degrees of finite-degree, cyclic, $\mathbb{Q}$-rational isogenies gives a classification of the sizes and shapes of *all* rational isogeny graphs. They are of the following type:

Classification of Rational Isogeny Graphs

Kenku's theorem (1980) on the classification of the degrees of finite-degree, cyclic, $\mathbb{Q}$-rational isogenies gives a classification of the sizes and shapes of *all* rational isogeny graphs. They are of the following type:

- L_k: **L**inear graphs with k vertices ($k = 1, 2, 3, 4$) such that each isogeny is cyclic, $\mathbb{Q}$-rational of p-power degree, for a single prime p, but no curves with full two-torsion.

Classification of Rational Isogeny Graphs

Kenku's theorem (1980) on the classification of the degrees of finite-degree, cyclic, $\mathbb{Q}$-rational isogenies gives a classification of the sizes and shapes of *all* rational isogeny graphs. They are of the following type:

- L_k: **L**inear graphs with k vertices ($k = 1, 2, 3, 4$) such that each isogeny is cyclic, $\mathbb{Q}$-rational of p-power degree, for a single prime p, but no curves with full two-torsion.
- R_k: **R**ectangular graphs with k vertices ($k = 4$ or 6) such that each isogeny is cyclic, $\mathbb{Q}$-rational of degree divisible by p or q for two distinct primes p and q but no curves with full two-torsion.

Classification of Rational Isogeny Graphs

Kenku's theorem (1980) on the classification of the degrees of finite-degree, cyclic, $\mathbb{Q}$-rational isogenies gives a classification of the sizes and shapes of *all* rational isogeny graphs. They are of the following type:

- L_k: **L**inear graphs with k vertices ($k = 1, 2, 3, 4$) such that each isogeny is cyclic, $\mathbb{Q}$-rational of p-power degree, for a single prime p, but no curves with full two-torsion.
- R_k: **R**ectangular graphs with k vertices ($k = 4$ or 6) such that each isogeny is cyclic, $\mathbb{Q}$-rational of degree divisible by p or q for two distinct primes p and q but no curves with full two-torsion.
- T_k: Graphs with k vertices ($k = 4, 6,$ or 8) such that each isogeny is cyclic $\mathbb{Q}$-rational of 2-power degree. In this case, one, two, or three curves in the isogeny class have full **T**wo-**T**orsion.

Classification of Rational Isogeny Graphs

Kenku's theorem (1980) on the classification of the degrees of finite-degree, cyclic, $\mathbb{Q}$-rational isogenies gives a classification of the sizes and shapes of *all* rational isogeny graphs. They are of the following type:

- L_k: **L**inear graphs with k vertices ($k = 1, 2, 3, 4$) such that each isogeny is cyclic, $\mathbb{Q}$-rational of p-power degree, for a single prime p, but no curves with full two-torsion.
- R_k: **R**ectangular graphs with k vertices ($k = 4$ or 6) such that each isogeny is cyclic, $\mathbb{Q}$-rational of degree divisible by p or q for two distinct primes p and q but no curves with full two-torsion.
- T_k: Graphs with k vertices ($k = 4, 6,$ or 8) such that each isogeny is cyclic $\mathbb{Q}$-rational of 2-power degree. In this case, one, two, or three curves in the isogeny class have full **T**wo-**T**orsion.
- S: Graphs with 8 vertices such that each isogeny is cyclic $\mathbb{Q}$-rational of degree divisible by 2 or 3 and two curves in the isogeny class have full two-torsion.

Main Result

MAIN QUESTION
Can we classify ALL rational isogeny-torsion graphs?

In other words, can we classify the size and shape of all rational isogeny graphs *and* the torsion groups of their vertices?

Main Result

MAIN QUESTION
Can we classify ALL rational isogeny-torsion graphs?

In other words, can we classify the size and shape of all rational isogeny graphs *and* the torsion groups of their vertices? **YES!**

Main Result

MAIN QUESTION
Can we classify ALL rational isogeny-torsion graphs?

In other words, can we classify the size and shape of all rational isogeny graphs *and* the torsion groups of their vertices? **YES!**

Theorem (C., Lozano-Robledo)

There are 37 rational isogeny-torsion graphs.
Moreover, there are 12 graphs of L_k type, 8 graphs of R_k type, 13 graphs of T_k type, and 4 graphs of S type.

Note: for the following, we abbreviate $\mathbb{Z}/a\mathbb{Z}$ as $[a]$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ by $[2, b]$.

Table of L_k graphs

Graph Type	Label	Isomorphism Types	LMFDB Label
E_1	L_1	([1])	37.a
$E_1 - E_2$	L_2	([1],[1])	75.c
		([2],[2])	46.a
		([3],[1])	44.a
		([5],[1])	38.b
		([7],[1])	26.b
$E_1 - E_2 - E_3$	L_3	([1],[1],[1])	99.d
		([3],[3],[1])	19.a
		([5],[5],[1])	11.a
		([9],[3],[1])	54.b
$E_1 - E_2 - E_3 - E_4$	L_4	([1],[1],[1],[1])	432.e
		([3],[3],[3],[1])	27.a

TABLE 1. The list of all L_k rational isogeny-torsion graphs

Table of L_k Graphs

- $\mathcal{O}$
- $$\mathbb{Z}/m\mathbb{Z} \overset{p}{\longrightarrow} \mathcal{O}$$
  If $p \geq 11$, then $m = 1$. If $p = 3, 5$, or 7, then $m = 1$ or p.
- $$\mathbb{Z}/2\mathbb{Z} \overset{2}{\longrightarrow} \mathbb{Z}/2\mathbb{Z}$$
- $$\mathbb{Z}/m\mathbb{Z} \overset{p}{\longrightarrow} \mathbb{Z}/m\mathbb{Z} \overset{p}{\longrightarrow} \mathcal{O}$$
  $p = 3$ or 5 and $m = 1$ or p
- $$\mathbb{Z}/9\mathbb{Z} \overset{3}{\longrightarrow} \mathbb{Z}/3\mathbb{Z} \overset{3}{\longrightarrow} \mathcal{O}$$
- $$\mathbb{Z}/m\mathbb{Z} \overset{3}{\longrightarrow} \mathbb{Z}/m\mathbb{Z} \overset{3}{\longrightarrow} \mathbb{Z}/m\mathbb{Z} \overset{3}{\longrightarrow} \mathcal{O}$$
  $m = 1$ or 3

Table of R_k Graphs

Graph Type	Label	Isomorphism Types	LMFDB Label
E_1 — E_2 $\vert$ $\vert$ E_3 — E_4	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
E_1 — E_3 — E_5 $\vert$ $\vert$ $\vert$ E_2 — E_4 — E_6	R_6	([2],[2],[2],[2],[2],[2])	98.a
		([6],[6],[6],[6],[2],[2])	14.a

TABLE 3. The list of all R_k rational isogeny-torsion graphs

R_4 graphs

- $$\begin{array}{ccc} {\color{blue}\mathbb{Z}/m\mathbb{Z}} & \overset{3}{\text{———}} & \mathcal{O} \\ p\,\Big| & & \Big|\,p \\ \mathbb{Z}/m\mathbb{Z} & \underset{3}{\text{———}} & \mathcal{O} \end{array}$$
  $p = 5$ or 7 and $m = 1$ or 3

- $$\begin{array}{ccc} {\color{blue}\mathbb{Z}/m\mathbb{Z}} & \overset{5}{\text{———}} & \mathcal{O} \\ 3\,\Big| & & \Big|\,3 \\ \mathbb{Z}/m\mathbb{Z} & \underset{5}{\text{———}} & \mathcal{O} \end{array}$$
  $m = 1$ or 5

- $$\begin{array}{ccc} {\color{blue}\mathbb{Z}/m\mathbb{Z}} & \overset{p}{\text{———}} & \mathbb{Z}/2\mathbb{Z} \\ 2\,\Big| & & \Big|\,2 \\ \mathbb{Z}/m\mathbb{Z} & \underset{p}{\text{———}} & \mathbb{Z}/2\mathbb{Z} \end{array}$$
  If $p = 3$ or 5, then $m = 2p$ or 2. If $p = 7$, then $m = 2$

R_6 Graphs

- $$\begin{array}{ccccc} \color{blue}{\mathbb{Z}/6\mathbb{Z}} & \overset{3}{\text{———}} & \mathbb{Z}/6\mathbb{Z} & \overset{3}{\text{———}} & \mathbb{Z}/2\mathbb{Z} \\ 2 \mid & & \mid 2 & & \mid 2 \\ \mathbb{Z}/6\mathbb{Z} & \underset{3}{\text{———}} & \mathbb{Z}/6\mathbb{Z} & \underset{3}{\text{———}} & \mathbb{Z}/2\mathbb{Z} \end{array}$$

- $$\begin{array}{ccccc} \color{blue}{\mathbb{Z}/2\mathbb{Z}} & \overset{3}{\text{———}} & \mathbb{Z}/2\mathbb{Z} & \overset{3}{\text{———}} & \mathbb{Z}/2\mathbb{Z} \\ 2 \mid & & \mid 2 & & \mid 2 \\ \mathbb{Z}/2\mathbb{Z} & \underset{3}{\text{———}} & \mathbb{Z}/2\mathbb{Z} & \underset{3}{\text{———}} & \mathbb{Z}/2\mathbb{Z} \end{array}$$

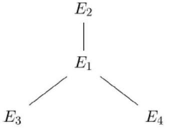
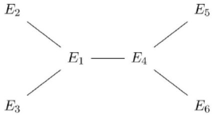
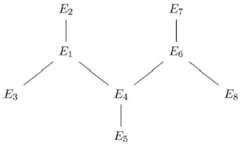
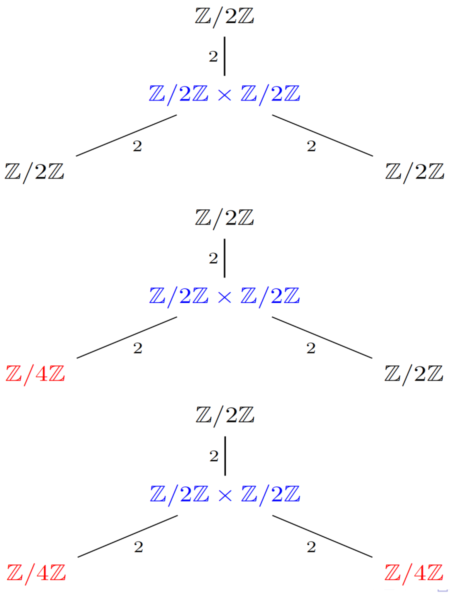
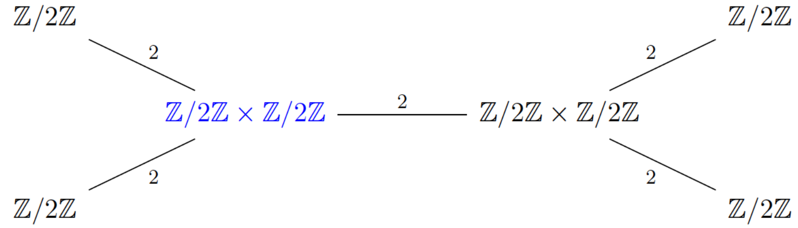
Graph Type	Label	Isomorphism Types	LMFDB Label
	T_4	([2,2], [2], [2], [2])	120.a
		([2,2], [4], [2], [2])	33.a
		([2,2], [4], [4], [2])	17.a
	T_6	([2,4],[4],[4],[2,2],[2],[2])	24.a
		([2,4],[8],[4],[2,2],[2],[2])	21.a
		([2,2],[2],[2],[2,2],[2],[2])	126.a
		([2,2],[4],[2],[2,2],[2],[2])	63.a
	T_8	([2,8],[8],[8],[2,4],[4],[2,2],[2],[2])	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

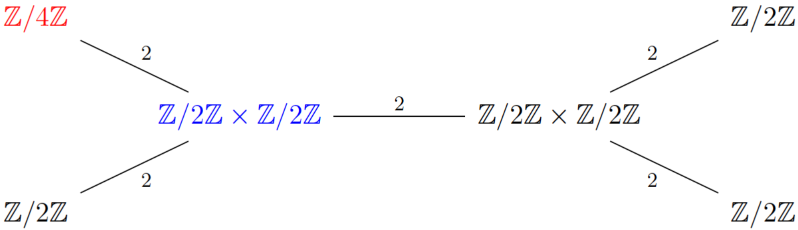
TABLE 2. The list of all T_k rational isogeny-torsion graphs

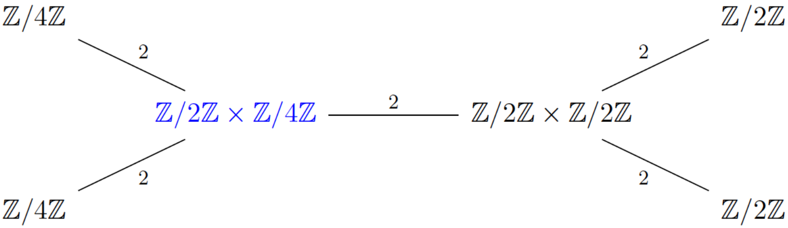
T_4 Graphs


ℤ/2ℤ
2
ℤ/2ℤ × ℤ/2ℤ
2
2
ℤ/2ℤ
ℤ/2ℤ
ℤ/2ℤ
2
ℤ/2ℤ × ℤ/2ℤ
2
2
ℤ/4ℤ
ℤ/2ℤ
ℤ/2ℤ
2
ℤ/2ℤ × ℤ/2ℤ
2
2
ℤ/4ℤ
ℤ/4ℤ

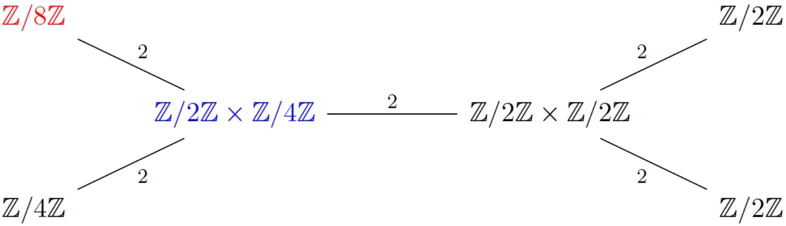
T_6 Graphs with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$





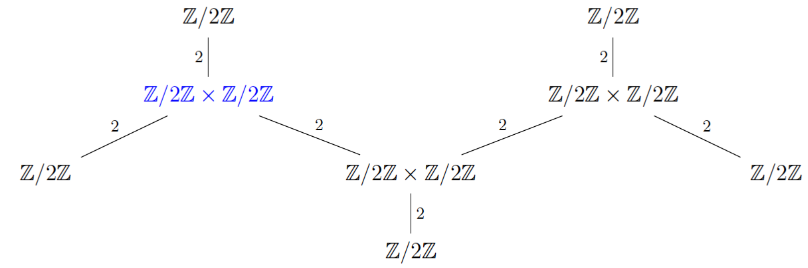


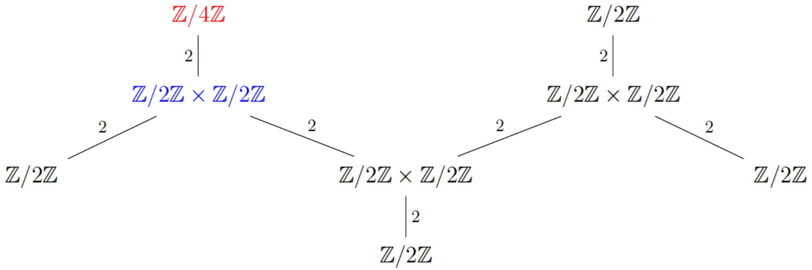
$\mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}$
2
2
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
2
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
2
2
$\mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}$



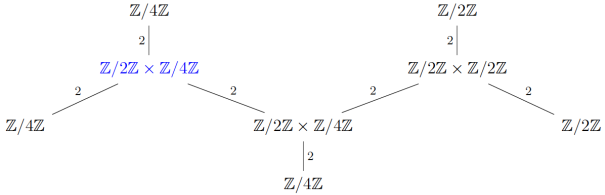
$\mathbb{Z}/8\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}$
2
2
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
2
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
2
2
$\mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}$

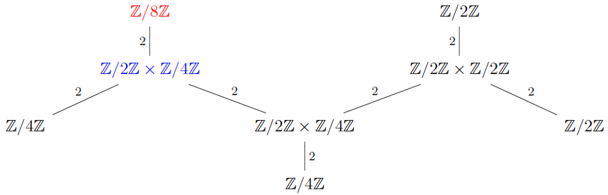
T_8 graphs with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

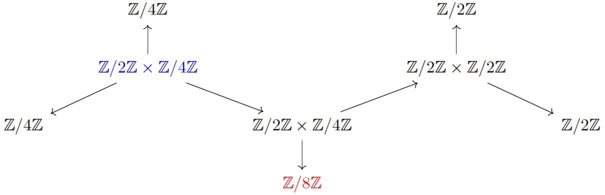




T_8 Graphs with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$







T_8 graphs with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

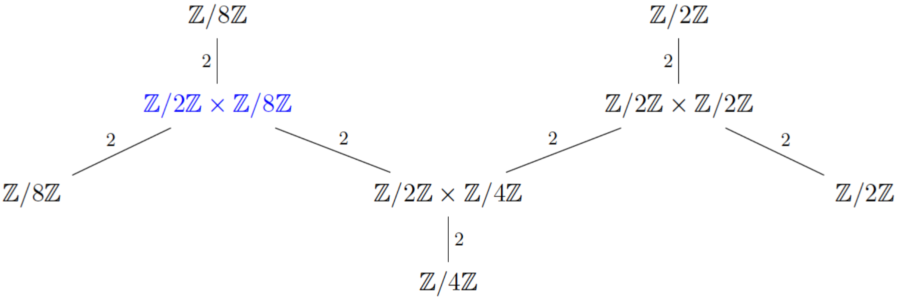


Table of S graphs

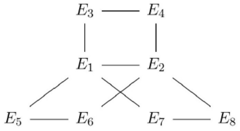
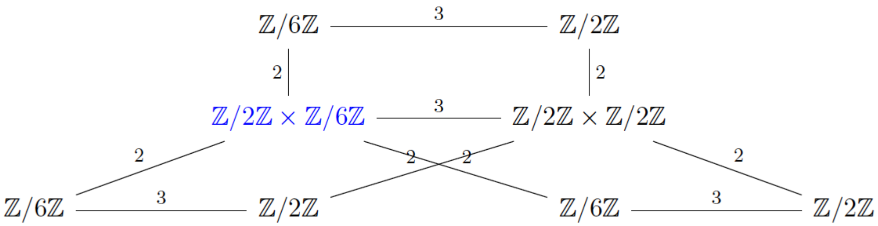
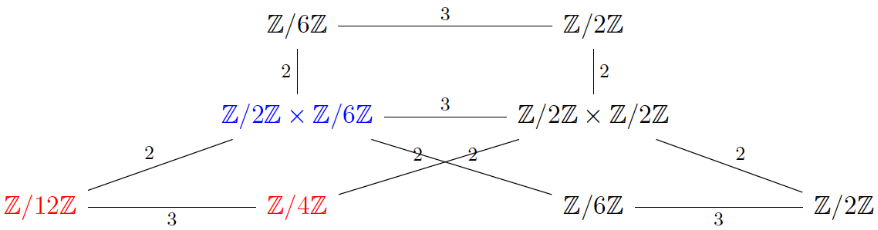
Graph Type	Label	Isomorphism Types	LMFDB Label
	S	([2,2],[2,2],[2],[2],[2],[2],[2],[2])	240.b
		([2,2],[2,2],[4],[4],[2],[2],[2],[2])	150.b
		([2,6],[2,2],[6],[2],[6],[2],[6],[2])	30.a
		([2,6],[2,2],[12],[4],[6],[2],[6],[2])	90.c

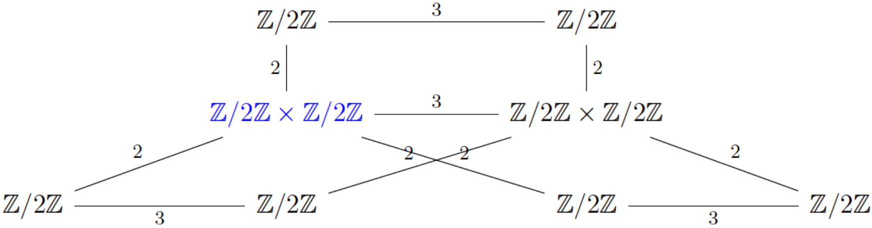
TABLE 4. The list of all (possible) S rational isogeny-torsion graphs

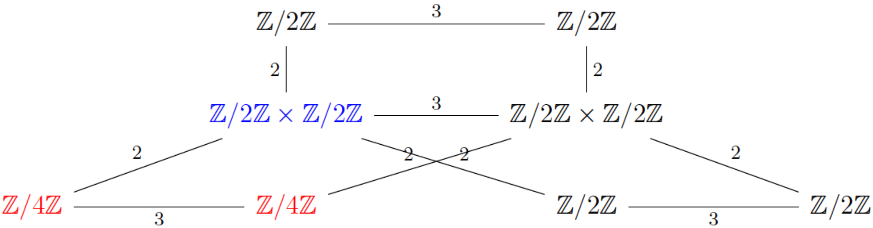
S Type Graphs with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$





S Type Graphs with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$





27-isogenies

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

$$\mathbb{Z}/3\mathbb{Z} \overset{3}{\text{———}} \mathbb{Z}/3\mathbb{Z} \overset{3}{\text{———}} \mathbb{Z}/3\mathbb{Z} \overset{3}{\text{———}} \mathcal{O}$$

LMFDB Label 27.a

$$\mathcal{O} \overset{3}{\text{———}} \mathcal{O} \overset{3}{\text{———}} \mathcal{O} \overset{3}{\text{———}} \mathcal{O}$$

LMFDB Label 432.e

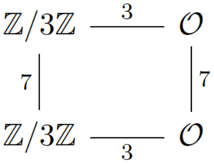
There are no examples of the following rational isogeny-torsion graph.

$$\mathbb{Z}/9\mathbb{Z} \overset{3}{\text{———}} \mathbb{Z}/9\mathbb{Z} \overset{3}{\text{———}} \mathbb{Z}/3\mathbb{Z} \overset{3}{\text{———}} \mathcal{O}$$

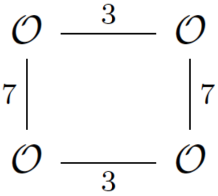
Reasoning: Let E be a curve with a 27-isogeny, then E corresponds to j-invariant $-2^{15} \cdot 3 \cdot 5^3$. If $P \in E[9] \setminus \{\mathcal{O}\}$, then $\mathbb{Q}(x(P))$ is a number field of degree $3, 6$, or 27.

Examples of 21-isogenies

There exist examples of the following rational isogeny-torsion graphs of degree 21



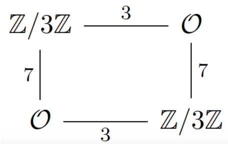
Isogeny Class 162.b



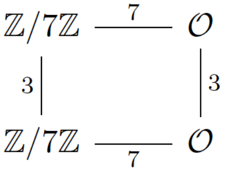
Isogeny Class 1296.f

Non-examples of 21-isogenies

There are no examples of the following rational isogeny-torsion graphs of degree 21.



Reasoning : A rational 7-isogeny maps a point of order 3 defined over $\mathbb{Q}$ to a point of order 3 defined over $\mathbb{Q}$.



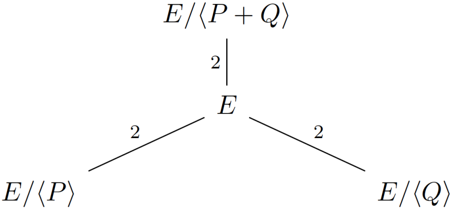
Reasoning : Let $E/\mathbb{Q}$ be a curve with a $\mathbb{Q}$-rational 21-isogeny. Let $P \in E[7] \setminus \{\mathcal{O}\}$, then $\mathbb{Q}(x(P))$ is a number field of degree 3 or 21, not 1. If E' is a quadratic twist of E and $P' \in E'[7]$, then $\mathbb{Q}(x(P)) = \mathbb{Q}(x(P'))$.

Classification of T_4 Graphs (1)

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

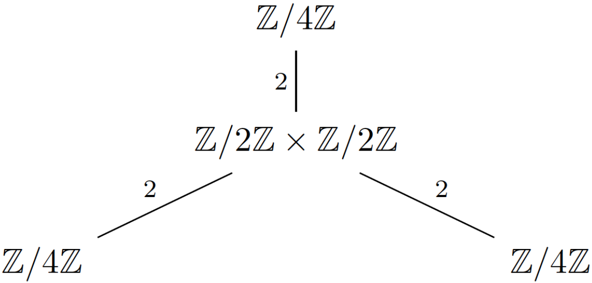
$$E(\mathbb{Q})_{\text{tors}} = \langle P, Q \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

What are the possible isogeny-torsion graphs of E?



- The 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. As there are 4 curves in the isogeny class, no curve isogenous to E can have a point of odd order or order 8 defined over $\mathbb{Q}$.

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



Classification of T_4 Graphs (3)

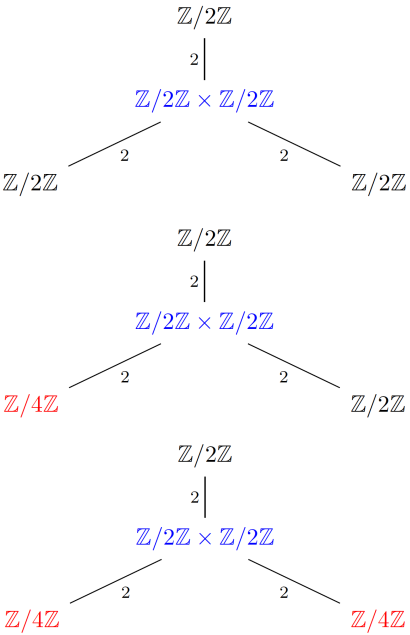
- Assume E is non-CM and $(E/\langle P\rangle)(\mathbb{Q})_{\text{tors}}$, $(E/\langle Q\rangle)(\mathbb{Q})_{\text{tors}}$, and $(E/\langle P+Q\rangle)(\mathbb{Q})_{\text{tors}}$, are cyclic of order 4. Then the image of the mod 4 Galois representation of E is conjugate to

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

  No element of H "behaves like" complex conjugation, ie, no element of H is conjugate over $GL_2(\mathbb{Z}/4\mathbb{Z})$ to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$.
  Thus, there are no curves E without CM that have an isogeny-torsion graph of the form $([2,2],[4],[4],[4])$

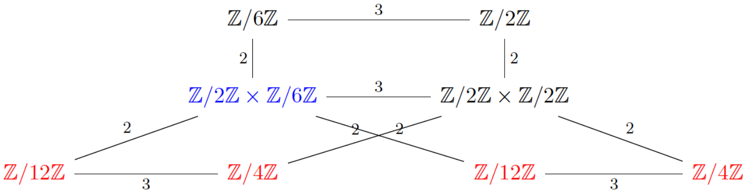
- Suppose E is CM, then there are only finitely many j-invariants that correspond to a torsion subgroup with full two-torsion.
  No such curve corresponding to those j-invariants or their twists will give you an isogeny-torsion graph of the form $([2,2],[4],[4],[4])$.

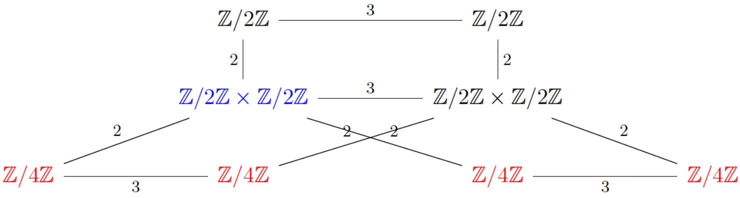
All T_4 Graphs



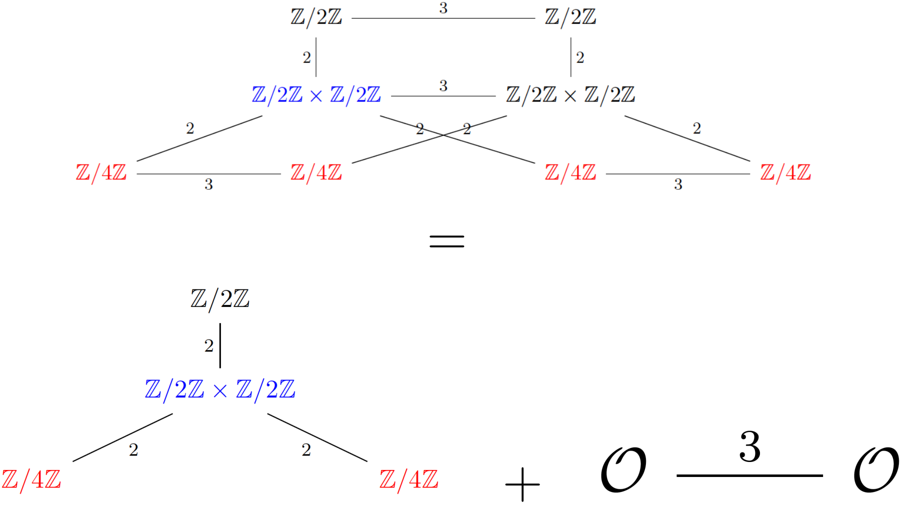
Classification of S Graphs (1)

The hardest part of classifying rational isogeny torsion graphs was eliminating the possibility of the following two graphs





Classification of S Graphs (2)



Classification of S Graphs (3)

- Let $E/\mathbb{Q}$ be a curve with an isogeny-torsion graph from the last slide, then E is non-CM. The image of the mod 4 Galois representation of E is conjugate in $GL_2(\mathbb{Z}/4\mathbb{Z})$ to

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

- All curves with a 2-adic Galois image mod 4 conjugate to H are parametrized by X_{24e} (RZB database) with j-invariant $\frac{(t^4+t^2+1)^3}{t^4(t^2+1)^2}$.
- Add a 3-isogeny. Curves with a 3-isogeny are parametrized by rational points on $X_0(3)$ with $j = \frac{(s+27)(s+243)^3}{s^3}$.
- Equating, we get $\frac{(t^4+t^2+1)^3}{t^4(t^2+1)^2} = \frac{(s+27)(s+243)^3}{s^3}$ and rearranging, we get a curve $C\colon (t^4+t^2+1)^3 s^3 - t^4(t^2+1)^2(s+27)(s+243)^3 = 0$ of genus 13.

Classification of S Graphs (4)

- There is an obvious map $(s,t) \to (s,t^2)$ that maps C to a curve $C'\colon (t^2+t+1)^3s^3 - t^2(t+1)^2(s+27)(s+243)^3 = 0$ of genus 6
- C' has an automorphism $\psi(t,s,z) = (-tz - z^2, ts, tz)$. The quotient curve $C'' = C'/\langle\psi\rangle$ has genus 2 with equation $C''\colon y^2 + x^2y = -x^5 - x^4 + 4x^3 - 2x^2 - 9x + 2$.
- Using a descent, the Jacobian variety, $J(C'')/\mathbb{Q}$ has rank 0 and thus, we can use Chabauty's method to compute the rational points of C''.
- C'' has two rational points, namely, $[-2,-2,1]$ and $[1,0,0]$ which map backwards to the points $[t,s,z] = [-1,0,1], [0,0,1], [0,1,0]$, and $[1,0,0]$ in C'. Each of these points have t or s coordinate to be 0 so they are all cusps (the j invariant is undefined). Thus, the two S graphs we are trying to eliminate in fact do not exist.

Begin at the beginning

MATHEMATICS

Home
Questions
Tags
Users
Unanswered

Isogenies between elliptic curves with specified torsion groups

Asked 4 years, 9 months ago Active 4 years, 9 months ago Viewed 120 times

3

2

For each of the 15 possible torsion groups of an elliptic curve defined over $\mathbb{Q}$ we have an infinite family of curves with that torsion group. This sometimes goes under the name of Kubert normal form or Tate normal form.

I have been wondering if we have something similar for the following setting.

Let's say we have an elliptic curve E with torsion group T and an elliptic curve E' with torsion group T' and an isogeny $E \to E'$.

Is it possible to come up with infinite families of such pairs of isogenous curves E, E' for each (or some) of the 15×14 pairs of torsion groups T, T'?

Or are there any other partial results related to this question?

elliptic-curves

share cite improve this question follow

asked Aug 26 '15 at 17:41
Jesper Petersen
1,058 6 12

and go on till you come to the end, then stop

Harris helped me figure it out!!!

woot

the curve we want has genus 13. It has a map down to a curve of genus 6.

the curve of genus 6 has an automorphism that induces a map down to a curve of genus 2

the curve of genus 2 has a jacobian of rank 0 over Q, and Chabauty computes all the rational points on this curve. There are two points

the two points on genus 2 come from 4 points in genus 6, and they are all cusps!

so no, the elusive graphs do not exist

AWESOME

nice

I'm really happy

what a way to end the year

Questions?