A Classification of Rational Isogeny-Torsion Graphs

Garen Chiloyan

UConn

October 5th, 2019

Elliptic Curves

Definition

A rational elliptic curve, E=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 $a_1; a_2; a_3; a_4; a_6$ 2 Q with a point at infinity defined over Q, $O = [0 : 1 : 0]$.

Elliptic Curves

Definition

A rational elliptic curve, E=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 $a_1; a_2; a_3; a_4; a_6$ 2 Q with a point at infinity defined over Q, $O = [0 : 1 : 0]$.

Theorem (Mordell–Weil, 1922)

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

Elliptic Curves

Definition

A rational elliptic curve, E=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 $a_1; a_2; a_3; a_4; a_6$ 2 Q with a point at infinity defined over Q, $O = [0 : 1 : 0]$.

Theorem (Mordell–Weil, 1922)

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

Theorem (Mazur, 1978)

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

$$Z=MZ \text{ with } 1 \quad M \quad 10 \text{ or } M = 12$$

$$Z=2Z \quad Z=2NZ \text{ with } 1 \quad N \quad 4$$

Isogenies

Definition

Let E=Q and E'=Q be elliptic curves. An **isogeny** mapping E to E' is a morphism $: E \ ! \ E'$ such that $(O_E) = O_{E'}$. 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=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 Q-rational subgroups of E and vertices being pairwise non-isomorphic rational elliptic curves isogenous to E that are generated by the finite cyclic Q-rational subgroups of E.

Example of Rational Isogeny Graph

Let E=Q : $y^2 + xy + y = x^3 \quad x^2 \quad 6x \quad 4$ 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?

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

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

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

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

Answer: No!

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?

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.

Theorem (B. Mazur, 1978)

Let $E=Q$ be an elliptic curve. A prime degree 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 $E=Q$ 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. 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:

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

fOg

Isogeny Class 37.a

Isogeny Class 121.a

Isogeny Class 11.a

Isogeny Class 432.e

(Images courtesy of the LMFDB.)

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 with a single elliptic curve with full two-torsion

Isogeny Class 17.a

(Image courtesy of the LMFDB.)

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 with three rational elliptic curves with full two-torsion

Isogeny Class 210.e

(Image courtesy of the LMFDB.)

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

Isogeny Class 30.a

(Image courtesy of the LMFDB.)

For the following, we abbreviate $Z=aZ = [a]$ and $Z=2Z \quad Z=bZ = [2\,;b]$

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

Isogeny Class 162.b

Isogeny Class 1296.f

The following rational isogeny-torsion graphs do not occur.

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

LMFDB Label 27.a

LMFDB Label 432.e

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

LMFDB Label 27.a

LMFDB Label 432.e

The following rational isogeny-torsion graph does not occur.

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

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 $\{O\}, \langle P\rangle, \langle Q\rangle$ 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 $\mathbb{Q}$.

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

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

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

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.

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

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \right\rangle \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$$

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.

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

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

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.

=

+

Attempts at a Full Solution (2)

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

$$\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} ; \quad \begin{matrix} 1 & 0 \\ 0 & 3 \end{matrix} ; \quad \begin{matrix} 3 & 2 \\ 2 & 1 \end{matrix} ; \quad \begin{matrix} 3 & 2 \\ 2 & 3 \end{matrix} \qquad 2\ GL_2(Z{=}4Z)$$

.

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?