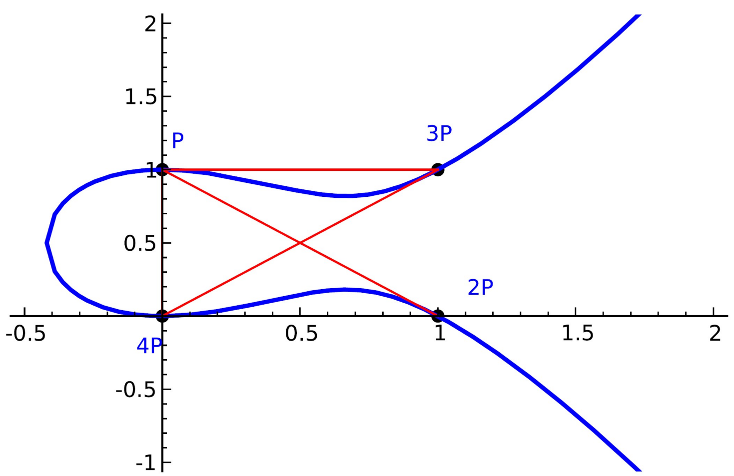
Boston University, April 5th, 2021.

"Towards a classification of adelic Galois representations attached to elliptic curves over $\mathbb{Q}$"



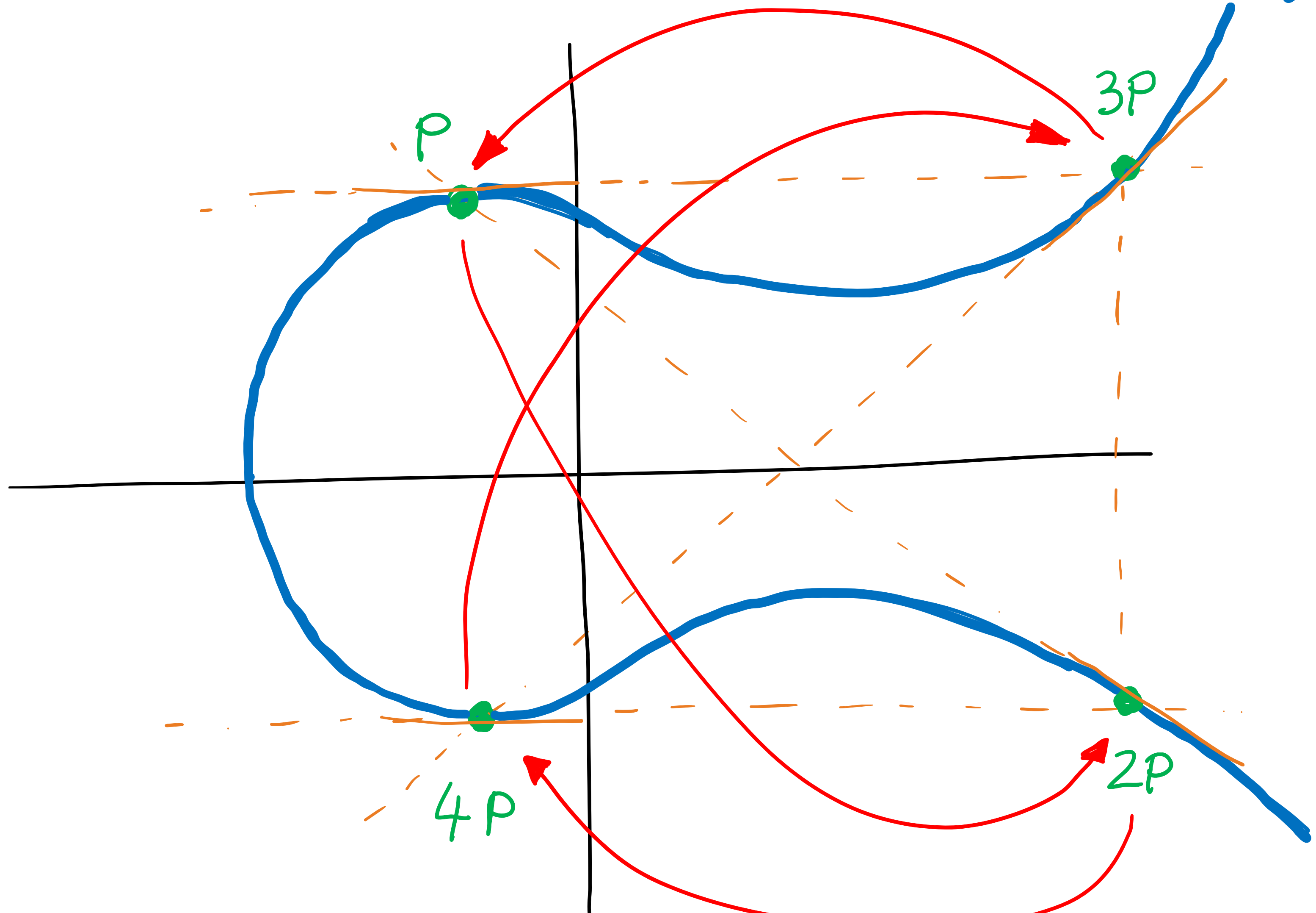
Álvaro Lozano-Robledo

University of Connecticut

$E/\mathbb{Q}$ an elliptic curve.

$$\rho_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL(2, \hat{\mathbb{Z}})$$

example: the Galois action on a point of order 5.



Let $E/\mathbb{Q}$ be an elliptic curve.

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

- $E(\overline{\mathbb{Q}})$ is NOT finitely generated but its torsion subgroup is well-understood!

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}}$

$$E(\overline{\mathbb{Q}})_{tors} = \bigcup_{n \geq 2} E[n]$$

and
$$E[n] = \underbrace{E(\overline{\mathbb{Q}})[n]}_{\text{n-torsion subgroup}} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

$E(\overline{\mathbb{Q}})[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ ⟲ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ... fixed points?
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \| \; G_{\mathbb{Q}}$

- Over $\mathbb{Q}$:

Thm. (Mazur) $E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & N = 1, 2, \ldots, 10, \text{ or } 12, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & M = 1, 2, 3, \text{ or } 4. \end{cases}$

(and ∞'ly many j's for each possibility!)

- How about (cyclic) $G_{\mathbb{Q}}$-invariant subgroups? (not just pointwise-fixed)

Thm. (Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, Ogg, ...)

If $\langle P \rangle \subseteq E(\overline{\mathbb{Q}})$ is finite, $G_{\mathbb{Q}}$-invariant, then

$\langle P \rangle \cong \mathbb{Z}/N\mathbb{Z}$ w/ $\begin{cases} N = 1, \ldots, 10, \text{ or } 12, 13, 16, 18, 25 \\ \text{or} \\ N = 11, 14, 15, 17, 19, 21, 27, 37, 43, 67, \text{ or } 163 \end{cases}$

(∞'ly many j's for each possibility)

$j = -2^{15} \cdot 3 \cdot 5^3$

(only $< \infty$ j's)

NOTE: $\left\{ \langle P \rangle \circlearrowleft G_{\mathbb{Q}} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isogenies} \\ E \to E' / \mathbb{Q} \\ \text{w/ cyclic kernel} \end{array} \right\}$

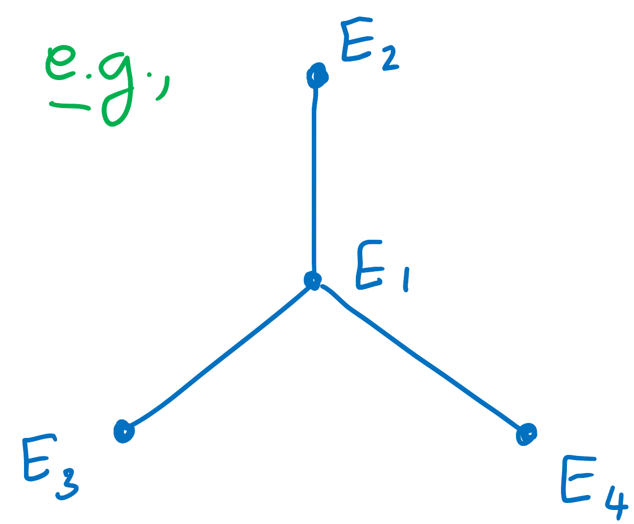
- Combine previous two results... $E_{/\mathbb{Q}} \longrightarrow E'_{/\mathbb{Q}}$ an isogeny.

Q. What are the possible combinations for the pair

$$\left(E(\mathbb{Q})_{tors},\ E'(\mathbb{Q})_{tors} \right) ?$$

More generally... consider the entire $\mathbb{Q}$-isogeny class of E.

e.g.,

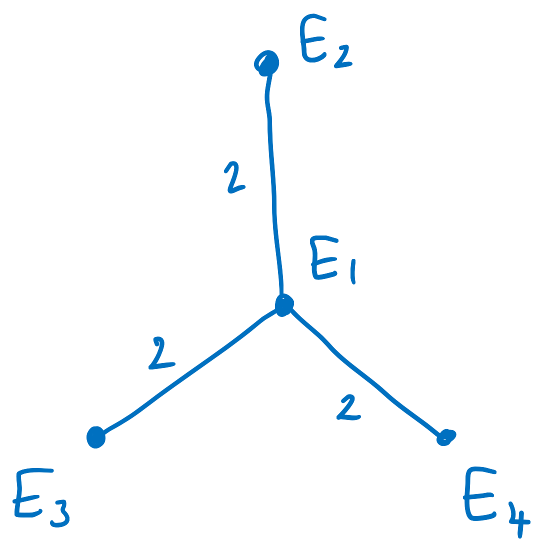


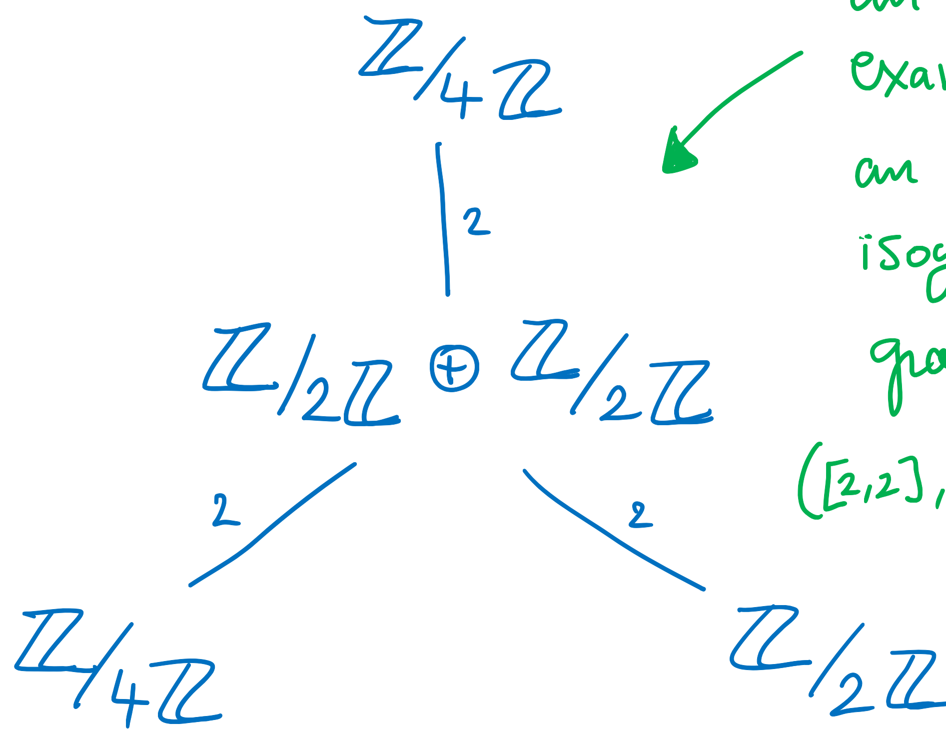
What are the possibilities for

$$\left(E_i(\mathbb{Q})_{tors} \right)_{i=1}^{4} ?$$

Example $E = E_1 : y^2 + xy + y = x^3 - x^2 - 6x - 4$

(17.a2)





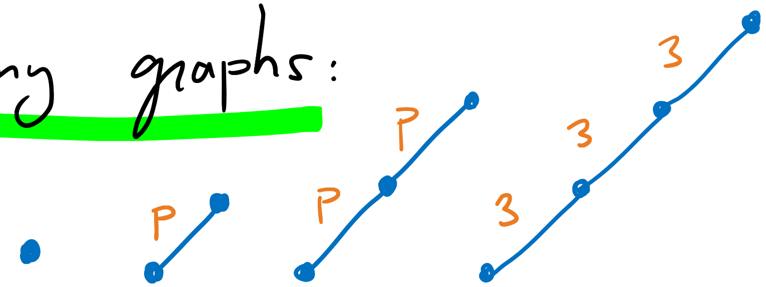
an example of an isogeny-torsion graph, of type ([2,2], [4], [4], [2])

Thm. (Chiloyan, L-R.)

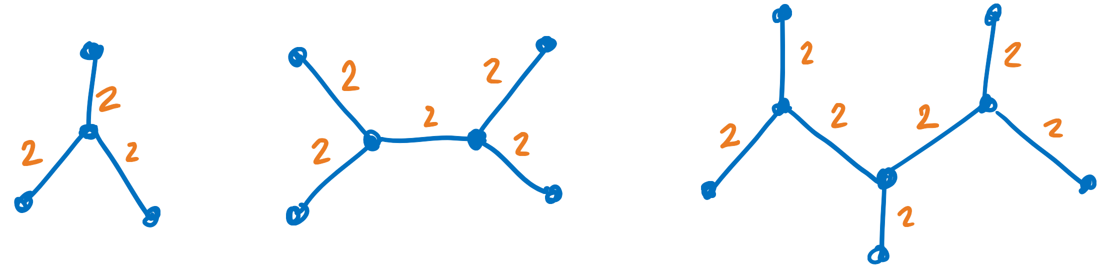
There are 52 iso. types of isogeny-torsion graphs attached to isogeny classes over $\mathbb{Q}$.

Types of isogeny graphs:

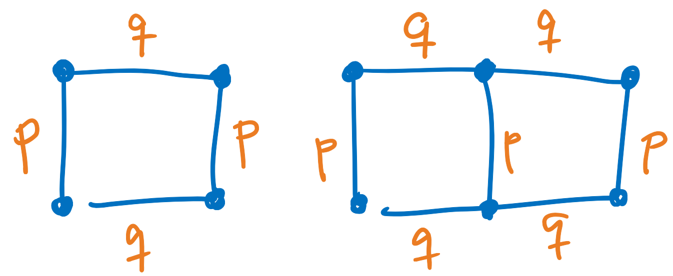
- Linear:



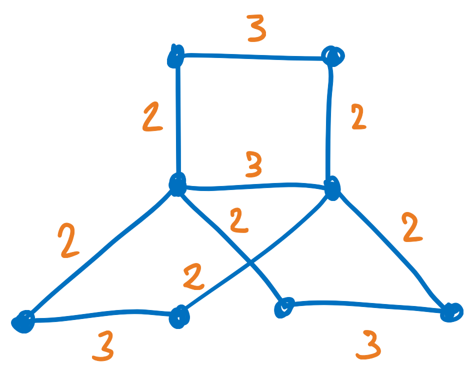
- T_k-graphs:



- Rectangular:



- S graphs:



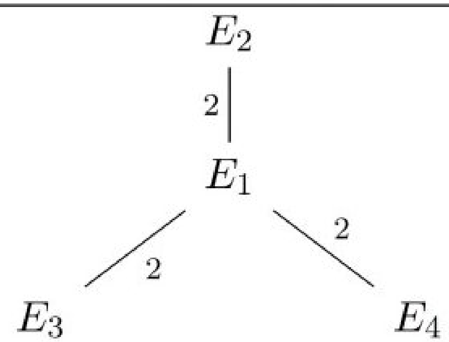
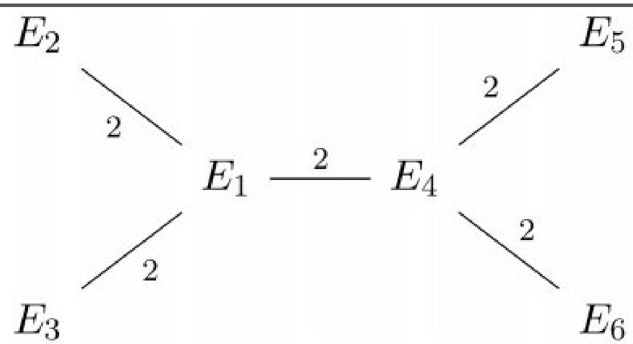
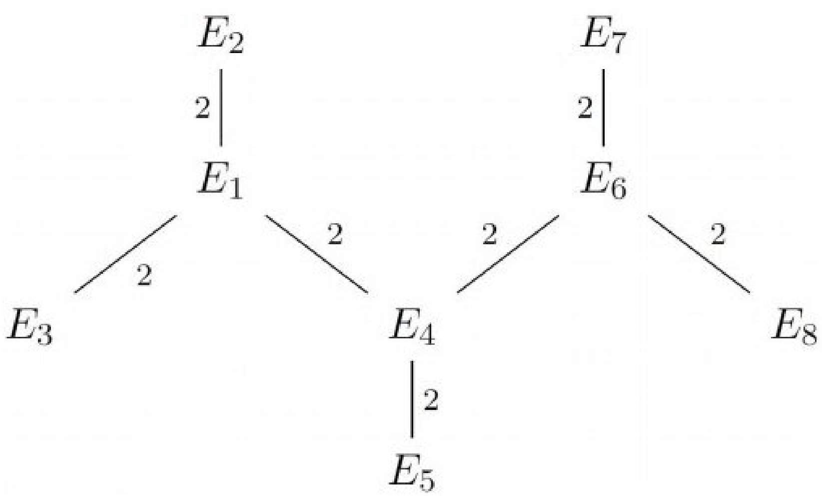
<table>
<tr><th>Graph Type</th><th>Label</th><th>Isomorphism Types</th><th>LMFDB Label</th></tr>
<tr><td rowspan="3">
</td><td rowspan="3">T_4</td><td>([2,2], [2], [2], [2])</td><td>120.a</td></tr>
<tr><td>([2,2], [4], [2], [2])</td><td>33.a</td></tr>
<tr><td>([2,2], [4], [4], [2])</td><td>17.a</td></tr>
<tr><td rowspan="4">
</td><td rowspan="4">T_6</td><td>([2,4],[4],[4],[2,2],[2],[2])</td><td>24.a</td></tr>
<tr><td>([2,4],[8],[4],[2,2],[2],[2])</td><td>21.a</td></tr>
<tr><td>([2,2],[2],[2],[2,2],[2],[2])</td><td>126.a</td></tr>
<tr><td>([2,2],[4],[2],[2,2],[2],[2])</td><td>63.a</td></tr>
<tr><td rowspan="6">
</td><td rowspan="6">T_8</td><td>([2,8],[8],[8],[2,4],[4],[2,2],[2],[2])</td><td>210.e</td></tr>
<tr><td>([2,4],[4],[4],[2,4],[4],[2,2],[2],[2])</td><td>195.a</td></tr>
<tr><td>([2,4],[4],[4],[2,4],[8],[2,2],[2],[2])</td><td>15.a</td></tr>
<tr><td>([2,4],[8],[4],[2,4],[4],[2,2],[2],[2])</td><td>1230.f</td></tr>
<tr><td>([2,2],[2],[2],[2,2],[2],[2,2],[2],[2])</td><td>45.a</td></tr>
<tr><td>([2,2],[4],[2],[2,2],[2],[2,2],[2],[2])</td><td>75.b</td></tr>
</table>

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

What do these results (Mazur/$\mathbb{Q}$, isogenies/$\mathbb{Q}$, isogeny-torsion/$\mathbb{Q}$, ...) have in common?

All this information is captured by the (adelic) Galois representation of E.

$$E[n] \circlearrowleft G_{\mathbb{Q}} \rightsquigarrow \rho_{E,n} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[n])$$

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}, \qquad \mathrm{Aut}(E[n]) \cong GL(2, \mathbb{Z}/n\mathbb{Z})$$

ex (of Mazur's theorem)

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

$$E[8] = \langle P\ ,\ Q \rangle$$

s.t. $4Q \in E(\mathbb{Q})$, and $P \in E(\mathbb{Q})$.

$$\rho_{E,8} : G_{\mathbb{Q}} \longrightarrow \left\{ \begin{pmatrix} 1 & 2b \\ 0 & c \end{pmatrix} : \begin{array}{l} c \equiv 1 \bmod 2 \\ b, c \in \mathbb{Z}/8\mathbb{Z} \end{array} \right\}$$

$$\subseteq GL(2, \mathbb{Z}/8\mathbb{Z})$$

ex (of isogenies$/\mathbb{Q}$)

$E/\mathbb{Q}$, $\langle P \rangle \subseteq E(\overline{\mathbb{Q}})$ of order 163, $E[163] = \langle P, Q \rangle$

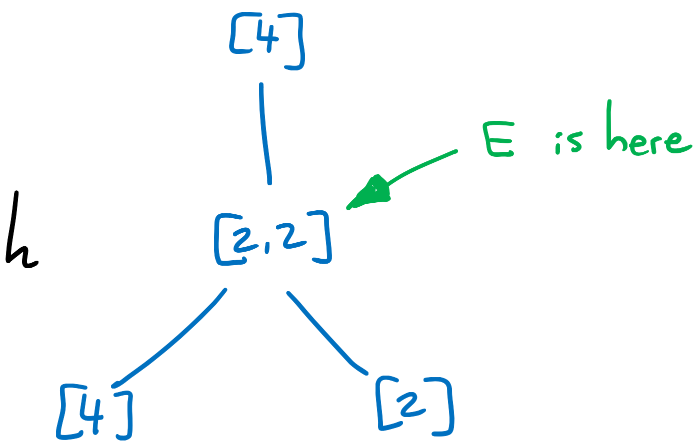
$\circlearrowleft G_{\mathbb{Q}}$

$$\rho_{E,163} : G_{\mathbb{Q}} \longrightarrow \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : \begin{array}{l} a,b,c \in \mathbb{Z}/163\mathbb{Z} \\ a,c \neq 0 \bmod 163 \end{array} \right\}$$

$$\subseteq GL(2, \mathbb{Z}/163\mathbb{Z})$$

<u>ex</u> (of isogeny-torsion graphs)

$E/\mathbb{Q}$ with a T_4-isogeny-torsion graph



$$\rho_{E,4} : G_{\mathbb{Q}} \longrightarrow \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \right\}$$

$$\subseteq GL(2, \mathbb{Z}/4\mathbb{Z})$$

Put all $\rho_{E,n}$ together!

$$T(E) = \varprojlim E[n] \cong \varprojlim \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

$$= \hat{\mathbb{Z}} \oplus \hat{\mathbb{Z}}$$

$G_{\mathbb{Q}} \circlearrowright T(E)$

$$\rightsquigarrow \quad \rho_E : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(T(E)) \cong GL(2, \hat{\mathbb{Z}})$$

Q: What are the possible images of $\rho_E \subseteq GL(2, \hat{\mathbb{Z}})$?
(up to conjugation!)

Mazur's "Program B"

(from "Rational points on modular curves.")

in Modular Functions of One Variable V.

B. Given a number field K and a subgroup H of $GL_2\hat{\mathbb{Z}} = \prod_p GL_2\,\mathbb{Z}_p$ classify all elliptic curves $E_{/K}$ whose associated Galois representation on torsion points maps $\mathrm{Gal}(\bar{K}/K)$ into $H \subset GL_2\hat{\mathbb{Z}}$.

Thm. (Serre) If $E/\mathbb{Q}$ does not have CM, then

$\operatorname{Im} \rho_E$ is open (finite index) in $GL(2, \hat{\mathbb{Z}})$.

Moreover, $[GL(2,\hat{\mathbb{Z}}) : \operatorname{Im} \rho_E] \geq 2$. (index is in fact even!)

Serre's Question. If $E/\mathbb{Q}$ does not have CM,

is $\rho_E \bmod p \twoheadrightarrow GL(2, \mathbb{F}_p)$ for all $p > 37$?

Conjecture. (Zywina) If $E/\mathbb{Q}$ does not have CM, then except for a finite number of exceptions ($j \in J$, w/ J finite):

$$[GL(2,\hat{\mathbb{Z}}) : \operatorname{Im} \rho_E] \in \left\{ \begin{array}{l} 2,4,6,8,10,12,16,20,24,30,32,36,40,48,54,60, \\ 72,84,96,108,112,120,144,192,220,240,288, \\ 336,360,384,504,576,768,864,1152,1200,1296,1536 \end{array} \right\}$$

The CM case

$E/\mathbb{Q}(j_{K,f})$ w/ $j(E) = j_{K,f}$

Thm. (L-R.) Let $j_{K,f}$ be a CM j-invariant w/ CM by $\mathcal{O}_{K,f} \subseteq K$, and

- if $\Delta_K \cdot f^2 \equiv 0 \bmod 4$, let $\delta = \Delta_K f^2/4$, $\phi = 0$,
- if $\Delta_K \cdot f^2 \equiv 1 \bmod 4$, let $\delta = (\Delta_K - 1) f^2/4$, $\phi = f$.

For $N \geq 2$, define $$\mathcal{C}_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a+b\phi & b \\ \delta b & a \end{pmatrix} : \begin{array}{l} a,b \in \mathbb{Z}/N\mathbb{Z} \\ a^2 + ab\phi - \delta b^2 \in (\mathbb{Z}/N\mathbb{Z})^\times \end{array} \right\}$$

and $$\mathcal{N}_{\delta,\phi}(N) = \left\langle \mathcal{C}_{\delta,\phi}(N), \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix} \right\rangle,$$

and $$\mathcal{N}_{\delta,\phi} = \varprojlim \mathcal{N}_{\delta,\phi}(N).$$

Then, $\operatorname{Im} \rho_E \subseteq \mathcal{N}_{\delta,\phi}$ and $d_E = [\mathcal{N}_{\delta,\phi} : \operatorname{Im} \rho_E]$

divides $\mathcal{O}_{K,f}^\times$ (so it divides 4 or 6, and divides 2 if $j \neq 0, 1728$).

(See also Bourdon + Clark's work on CM!)

The 2-adic case

Thm. (Rouse, Zureick-Brown)

Let $E/\mathbb{Q}$ be an elliptic curve w/o CM. Then, the image of

$$\rho_{E,2^\infty} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(T_2(E)) \cong GL(2,\mathbb{Z}_2)$$

is one of 1208 possibilities (up to conjugation).

Moreover, the index $[GL(2,\mathbb{Z}_2) : \mathrm{Im}\,\rho_{E,2^\infty}]$ divides 64 or 96,

and $\rho_{E,2}$ is defined modulo 32.

(Whoa!)

The largest possible adelic image

An elliptic curve $E/\mathbb{Q}$ w/ $[GL(2,\hat{\mathbb{Z}}) : \operatorname{Im} \rho_E] = 2$ is called a Serre curve.

Cojocaru, Grant, Jones : "almost all" curves are Serre curves (except 'thin' sets)

Daniels : explicit infinite family of Serre curves.

Why is $[GL(2,\hat{\mathbb{Z}}) : \operatorname{Im} \rho_E]$ even?

- Either $\Delta_E = \square \implies \operatorname{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq \{0\}$ or $\mathbb{Z}/3\mathbb{Z}$

  $\implies [GL(2,\mathbb{Z}_2) : \operatorname{Im} \rho_{E,2^\infty}]$ is even.

- Or $\Delta_E \neq \square$

$$
\begin{tikzcd}
 & & & \mathbb{Q}(E[n]) \arrow[dl, dash] \\
\mathbb{Q}(E[2]) \arrow[dr, dash] & & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \arrow[dd, dash] & \\
 & \mathbb{Q}(\sqrt{\Delta_E}) \arrow[dr, dash] & & \\
 & & \mathbb{Q} &
\end{tikzcd}
$$

$\rightsquigarrow$ "**Galois entanglement**" between $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E[n])$.

example $E : y^2 + y = x^3 + x^2 \, , \; \Delta_E = -43$

$$\begin{tikzcd}
 & & & \mathbb{Q}(E[43]) \\
\mathbb{Q}(E[2]) \arrow[dr, no head] & & \mathbb{Q}(\zeta_{43}) \arrow[ur, no head] & \\
 & \mathbb{Q}(\sqrt{-43}) \arrow[ur, no head] \arrow[d, no head] & & \\
 & \mathbb{Q} \arrow[uur, no head] & &
\end{tikzcd}$$

In this case:

- $\rho_{E,2^\infty} : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{Z}_2)$

and

- $\rho_{E,43^\infty} : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{Z}_{43})$

are surjective.

But ρ_E is NOT surjective b/c $\rho_{E,86} : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{Z}/86\mathbb{Z})$ is not surjective (image is index 2).

(However, here $[GL(2,\hat{\mathbb{Z}}) : \mathrm{Im}\, \rho_E] = 2$.)

$\uparrow$ Serre!

example $E: y^2 + y = x^3 - x^2$, $\Delta_E = -11$.

$$\begin{tikzcd}[column sep=small]
 & & & \mathbb{Q}(E[11]) \arrow[dl, dash] \\
\mathbb{Q}(E[2]) \arrow[dr, dash] & & \mathbb{Q}(\zeta_{11}) \arrow[dl, dash] & \\
 & \mathbb{Q}(\sqrt{-11}) \arrow[d, dash] & & \\
 & \mathbb{Q} & &
\end{tikzcd}$$

Here $\rho_{E,2^\infty}$ and $\rho_{E,11^\infty}$ are surjective BUT entangled ($\rho_{E,22}$).

index 24.

AND $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/5\mathbb{Z} \implies \rho_{E,5}: G_{\mathbb{Q}} \to \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \subseteq GL(2, \mathbb{F}_5)$

$$\implies [GL(2, \hat{\mathbb{Z}}) : \mathrm{Im}\, \rho_E] \geq 48.$$

But wait! There is more!

Example $E: y^2 + y = x^3 - x^2$, $\Delta_E = -11$.

- Here $\rho_{E,2^\infty}$ and $\rho_{E,11^\infty}$ are surjective but entangled ($\rho_{E,22}$).
- $E(\mathbb{Q})[5] \cong \mathbb{Z}/5\mathbb{Z} \implies \rho_{E,5}: G_{\mathbb{Q}} \longrightarrow \left\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}\right\} \subseteq GL(2, \mathbb{Z}/5\mathbb{Z})$
- E has a $\mathbb{Q}$-isogeny of degree 25! (to $y^2+y = x^3-x^2-7820x-263580$)

$$\implies \rho_{E,25}: G_{\mathbb{Q}} \longrightarrow \left\{\begin{pmatrix} \overset{1 \bmod 5}{*} & * \\ 0 & * \end{pmatrix}\right\} \underset{\text{index } 120}{\subseteq} GL(2, \mathbb{Z}/25\mathbb{Z})$$

$$\implies [GL(2, \hat{\mathbb{Z}}) : \operatorname{Im} \rho_E] \geq 240 \; !!$$

(ex. If $j(E) = -7 \cdot 11^3$, then index ≥ 2736.)

How bad can entanglements be? (joint with Harris Daniels)

Q When is $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$?

ex $E: y^2 = x^3 + 405x - 9882$

then $\mathbb{Q}(E[2]) = \mathbb{Q}(E[3]) = \mathbb{Q}(E[6]) = \mathbb{Q}(\zeta_3, \sqrt[3]{3})$

ex $E: y^2 = x^3 + 13x - 34$

then $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4]) = \mathbb{Q}(i)$.

(VERTICAL)

Thm. (Daniels, L-R.)

(1) If $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[p^{n+1}])$

then $p=2$, $n=1$ (and explicit param. of all examples).

(2) If $\mathbb{Q}(E[p^n]) \cap \mathbb{Q}(\zeta_{p^{n+1}}) = \mathbb{Q}(\zeta_{p^{n+1}})$

then $p=2$.

ex $E: y^2 = x^3 - 11x - 14$

then $\mathbb{Q}(\zeta_{2^{n+1}}) \subseteq \mathbb{Q}(E[2^n])$ for all $n > 1$.

(HORIZONTAL)

Thm. (Daniels, L-R.)

(1) If $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[q^m])$,

then $p^n = 2$, $q^m = 3$ (plus param.)

(2) If $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$ is abelian,

(a) Either $m=2$, $n=4$, and $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4]) = \mathbb{Q}(i)$,

(b) Or $m=3$, $n=6$, with

$$\mathbb{Q}(E[2]) \subsetneq \mathbb{Q}(E[3]) = \mathbb{Q}(E[6]).$$

What types of entanglements are there?

(joint w/ Harris Daniels and Jackson Morrow)

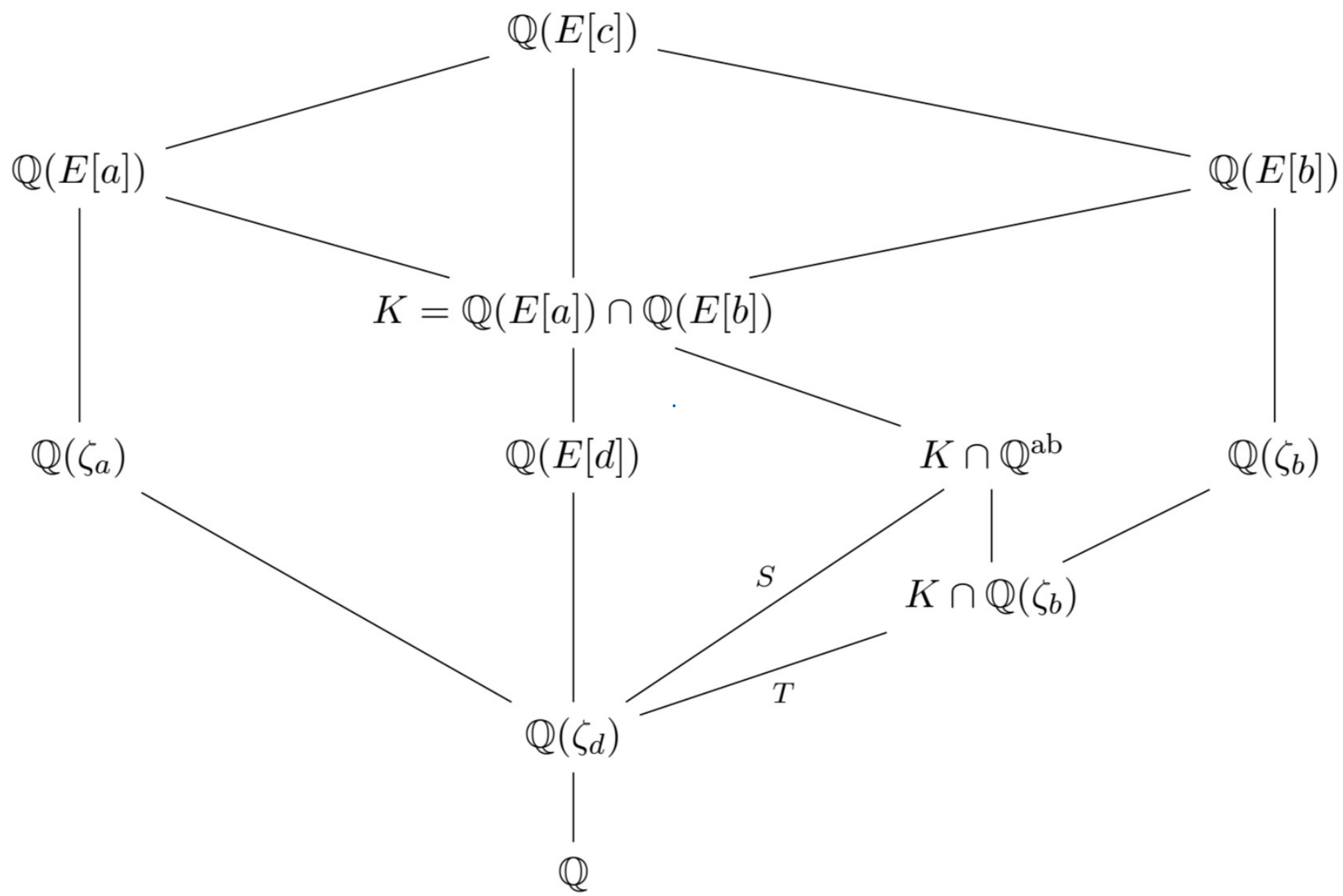


FIGURE 3.1. An abelian (a, b)-entanglement of type S, and a Weil (a, b)-entanglement of type T, where $c = \mathrm{lcm}(a, b)$ and $d = \gcd(a, b)$.

Types of abelian entanglements:

$$\begin{tikzcd}
 & & \mathbb{Q}(E[c]) \arrow[dll, dash] \arrow[dd, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(E[a]) \arrow[drr, dash] \arrow[dd, dash] & & & & \mathbb{Q}(E[b]) \arrow[dll, dash] \arrow[dd, dash] \\
 & & K = \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) \arrow[d, dash] \arrow[dr, dash] & & \\
\mathbb{Q}(\zeta_a) \arrow[ddrr, dash] & & \mathbb{Q}(E[d]) \arrow[dd, dash] & K \cap \mathbb{Q}^{\mathrm{ab}} \arrow[d, dash] \arrow[ddl, dash, "S"'] & \mathbb{Q}(\zeta_b) \arrow[dl, dash] \\
 & & & K \cap \mathbb{Q}(\zeta_b) \arrow[dl, dash, "T"] & \\
 & & \mathbb{Q}(\zeta_d) \arrow[d, dash] & & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

FIGURE 3.1. An abelian (a, b)-entanglement of type S, and a Weil (a, b)-entanglement of type T, where $c = \mathrm{lcm}(a, b)$ and $d = \gcd(a, b)$.

- Serre entanglements
  - $\hookrightarrow$ either $\rho_{E,2^\infty}$ is not surjective
  - $\hookrightarrow$ or $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_n)$
- CM entanglements
  $E/\mathbb{Q}$ w/ CM by K
  for $N, M \geq 3$.

$$\begin{tikzcd}
\mathbb{Q}(E[N]) & & \mathbb{Q}(E[M]) \\
 & K \arrow[ul, dash] \arrow[ur, dash] \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

- Weil entanglements (see diagram)

example Let d be sq. free integer, $t \neq 1$, $t \in \mathbb{Q}$.

Let $E_t^d : dy^2 = x^3 - 27t(t^3+8)x + 54(t^6 - 20t^3 - 8)$

then

$$\operatorname{Im} \rho_{E_t^d, 3} = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}$$

s.t. $\mathbb{Q}(E_t^d[3]) = \mathbb{Q}(\sqrt{-3}, \sqrt{d})$.

If n is minimal s.t. $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_n)$

then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(E[3]) \cap \mathbb{Q}(E[n])$ which results in an entanglement.

(a $(3,n)$-Weil entanglement of type $\mathbb{Z}/2\mathbb{Z}$)

Abelian (p,q)-entanglements

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{E,p}} \mathrm{Im}\,\rho_{E,p} \subseteq \mathrm{Aut}(E[p]) \subseteq GL(2,\mathbb{F}_p)$$

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{E,q}} \mathrm{Im}\,\rho_{E,q} \subseteq \mathrm{Aut}(E[q]) \subseteq GL(2,\mathbb{F}_q)$$

Want: $F = \left(\mathbb{Q}(E[p]) \cap \mathbb{Q}(E[q])\right) \cap \mathbb{Q}^{ab}$

Thm (Daniels, L-R.)

$E/\mathbb{Q}$ ell curve, $p>2$ prime.

$$\mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab} = \begin{cases} \mathbb{Q}(\zeta_p) & \text{if } \mathrm{Im}\,\rho_{E,p} \text{ is } \begin{cases} \text{full/surjective} \\ \text{exceptional} \end{cases} \\ \mathbb{Q}(\zeta_p)\cdot K \text{ w/ } [K:\mathbb{Q}]=2 & \text{if } \mathrm{Im}\,\rho_{E,p} \text{ is } \begin{cases} \text{norm. split} \\ \text{norm non-split} \end{cases} \\ \mathbb{Q}(\zeta_p)\cdot K \text{ w/ } [K:\mathbb{Q}] \mid (p-1) & \text{if } \mathrm{Im}\,\rho_{E,p} \text{ is Borel} \end{cases}$$

Example E "1922.c2"

one of an infinite family!

- $\underbrace{\mathrm{Im}\,\rho_{E,2}}_{\mathbb{Q}(E[2]) = \text{cyclic cubic, disc} = 31^2} \subseteq GL(2, \mathbb{F}_2)$

- $\underbrace{\mathrm{Im}\,\rho_{E,7}}_{\text{Borel}\ \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}} \subseteq GL(2, \mathbb{F}_7)$

cuts out a cyclic sextic disc $= -31^5$

$$F = \left(\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[7])\right) \cap \mathbb{Q}^{ab} = \mathbb{Q}(E[2])$$ is cyclic cubic, disc $= 31^2$.

- E is not CM
- Entanglement is not quadratic $\Rightarrow$ not Serre.
- Entanglement field $F \not\subseteq \mathbb{Q}(\zeta_2)$ and $\not\subseteq \mathbb{Q}(\zeta_7)$ $\Rightarrow$ not Weil

example

Let $d \neq -2, -3, 5$ be square-free, and let E^d be a twist of

$$E: y^2 + xy + y = x^3 - 126x - 552$$

Here $\mathbb{Q}(E^d[p]) \cap \mathbb{Q}^{ab} = \mathbb{Q}(\zeta_p, \sqrt{d})$ for $p = 3, 5$.

Thus, $\mathbb{Q}(E^d[3]) \cap \mathbb{Q}(E^d[5]) = \mathbb{Q}(\sqrt{d})$.

- E is NOT CM $\longrightarrow$ ent. is NOT of CM type.
- ent. b/w 3- and 5-division fields $\Longrightarrow$ NOT of Serre type.
- $\mathbb{Q}(\sqrt{d}) \not\subseteq \mathbb{Q}(\zeta_3), \mathbb{Q}(\zeta_5) \Longrightarrow$ NOT of Weil type.

example

E "1369.f2"

- $\underbrace{\mathrm{Im}\,\rho_{E,3}}_{\text{Normalizer of a non-split Cartan}} \subseteq GL(2,\mathbb{F}_3)$

$$\mathbb{Q} \overset{2}{—} F = \mathbb{Q}(\sqrt{37}) \overset{C_{ns}}{—} \mathbb{Q}(E[3])$$

- $\underbrace{\mathrm{Im}\,\rho_{E,5}}_{\text{Borel}} \subseteq GL(2,\mathbb{F}_5)$

$\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}$ cyclic quartic

$$\mathbb{Q} — F = \mathbb{Q}(\sqrt{37}) — \mathbb{Q}(P)$$

$$F = \left(\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[5])\right) \cap \mathbb{Q}^{ab} = \mathbb{Q}(\sqrt{37})$$

- Non-CM
- Non-Serre
- Non-Weil

DANIELS, L-R., MORROW:

(upcoming!)

Theorem A. *Let $E/\mathbb{Q}$ be an elliptic curve, and let p and q be distinct primes such that E has an abelian (p,q)-entanglement of type S, for some finite abelian group S. Then, there is a finite set $J \subset \mathbb{Q}$, that does not depend on p, q, or S, such that if $j(E) \notin J$ and the entanglement is not of Weil, Serre, or CM type, then $S = \mathbb{Z}/3\mathbb{Z}$ and $(p,q) = (2,7)$, and $j(E)$ belongs to one of three explicit one-parameter families of j-invariants (which appear in Section 8.1 of [DM20]).*

Theorem B. *There are infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves E over $\mathbb{Q}$ with:*

(1) *a Weil $(3,n)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$ where $3 \nmid n$,*
(2) *a Weil $(5,n)$-entanglement of type $\mathbb{Z}/4\mathbb{Z}$ where $5 \nmid n$,*
(3) *a Weil $(7,n)$-entanglement of type $\mathbb{Z}/6\mathbb{Z}$ where $6 \nmid n$,*
(4) *a Weil (m,n)-entanglement of type $\mathbb{Z}/2\mathbb{Z}$ where $n \geqslant 3$ and $m \in \{3,4,5,6,7,9\}$.*

Theorem C. *Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order $\mathcal{O}_K$ in an imaginary quadratic field K with $\Delta_K \neq -4, -8$ and $j(E) \neq 0$ or with CM by an order of $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{-2})$. For a choice of compatible bases of $E[n]$ for each $n \geqslant 2$, the index of the image of ρ_E in $\mathcal{N}_{\delta,\phi}(\widehat{\mathbb{Z}})$ is 2.*

Theorem D. *Let $\ell > 3$ be a prime number. Suppose that $\ell - 1 = 2e$ where $e = 2g+1$ is some odd integer. There exist infinitely many principally polarized abelian varieties $A/\mathbb{Q}$ of dimension g which have a Weil $(2,\ell)$-entanglement of type $\mathbb{Z}/e\mathbb{Z}$.*

Thank

You !

alvaro.lozano-robledo@uconn.edu