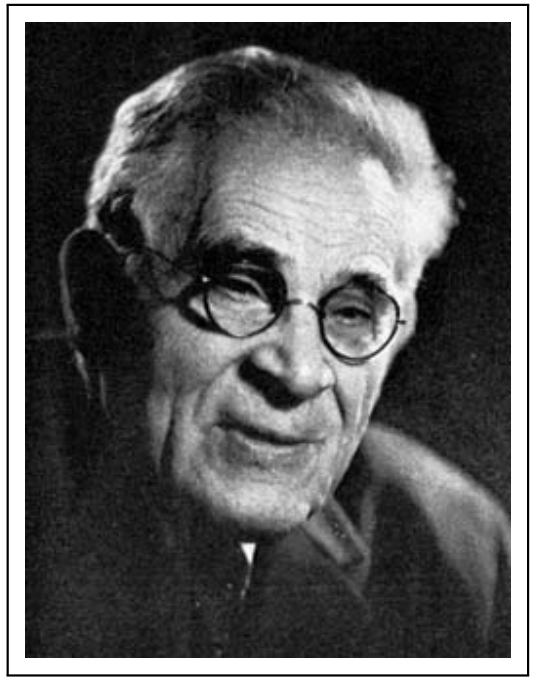
Clasificación de Grafos de Isogenia-Torsión para Curvas Elípticas sobre $\mathbb{Q}$

Garen Chiloyan y Álvaro Lozano-Robledo

Departmento de Matemáticas
Universidad de Connecticut

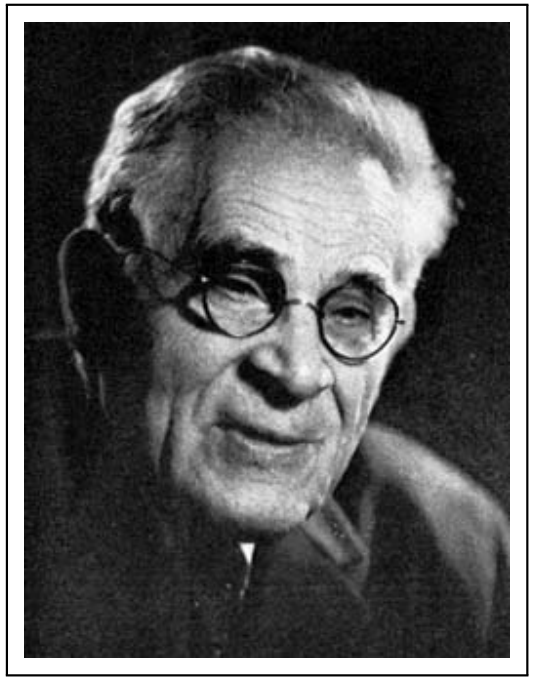
20 de Mayo, 2020
Seminario Latinoamericano
de Teoría de Números



Louis Mordell
$1888 - 1972$

Teorema (Mordell, 1922)

Sea $E/\mathbb{Q}$ una curva elíptica. Entonces, el grupo de puntos $\mathbb{Q}$-racionales de E, denotado por $E(\mathbb{Q})$, es un grupo abeliano finitamente generado. En particular, $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$ donde $E(\mathbb{Q})_{tors}$ es un subgrupo finito y $R_{E/\mathbb{Q}} \geq 0$.



Louis Mordell
1888 – 1972

André Weil
1906 – 1998

Theorem (Mordell–Weil, 1928)

Sea F un cuerpo de números, y sea A/F una variedad abeliana. Entonces, el grupo de puntos F-racionales de A, denotado por $A(F)$, es un grupo abeliano finitamente generado. En particular, $A(F) \cong A(F)_{tors} \oplus \mathbb{Z}^{R_{A/F}}$ donde $A(F)_{tors}$ es un subgrupo finito y $R_{A/F} \geq 0$.

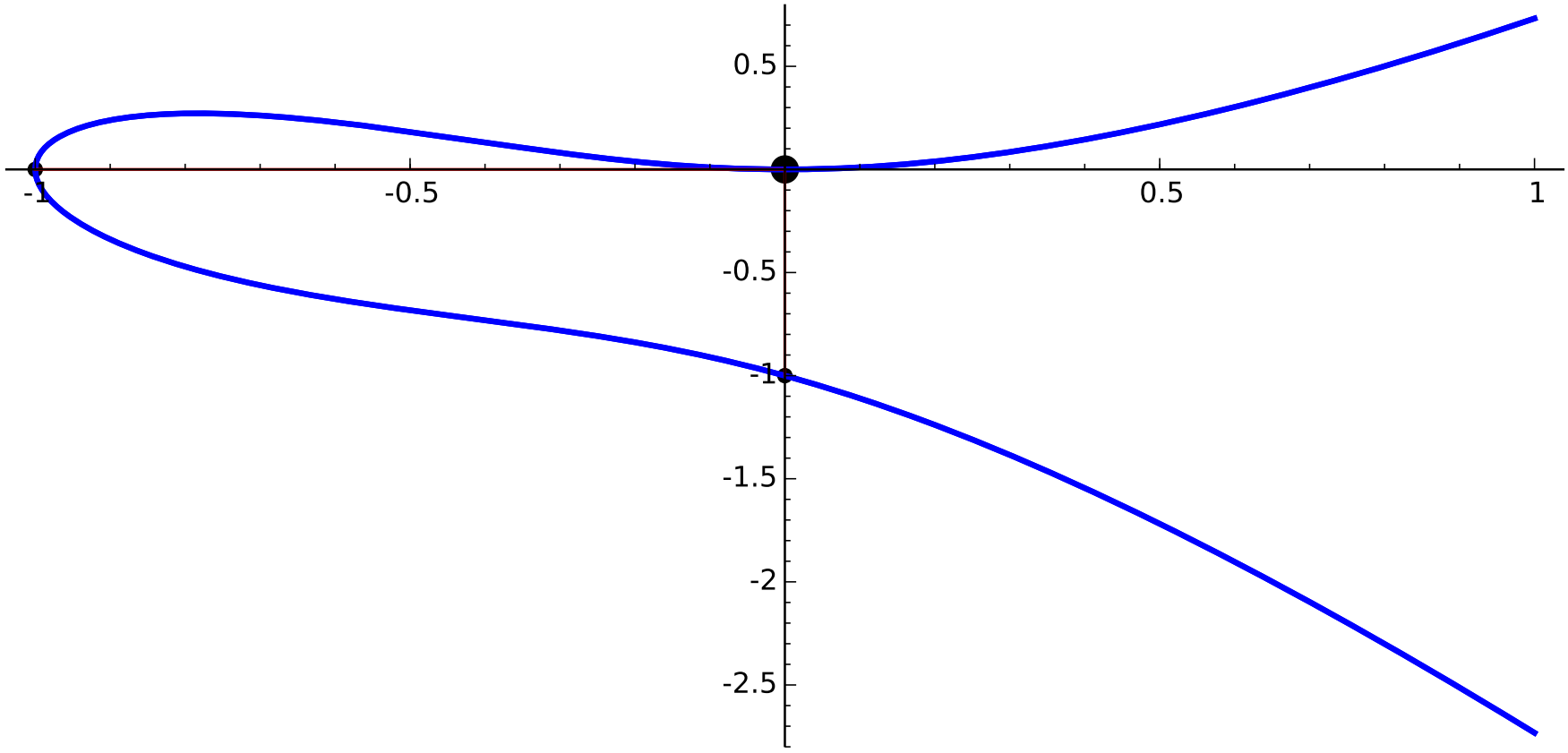
En esta charla: subgrupos de torsión

En esta charla: subgrupos de torsión

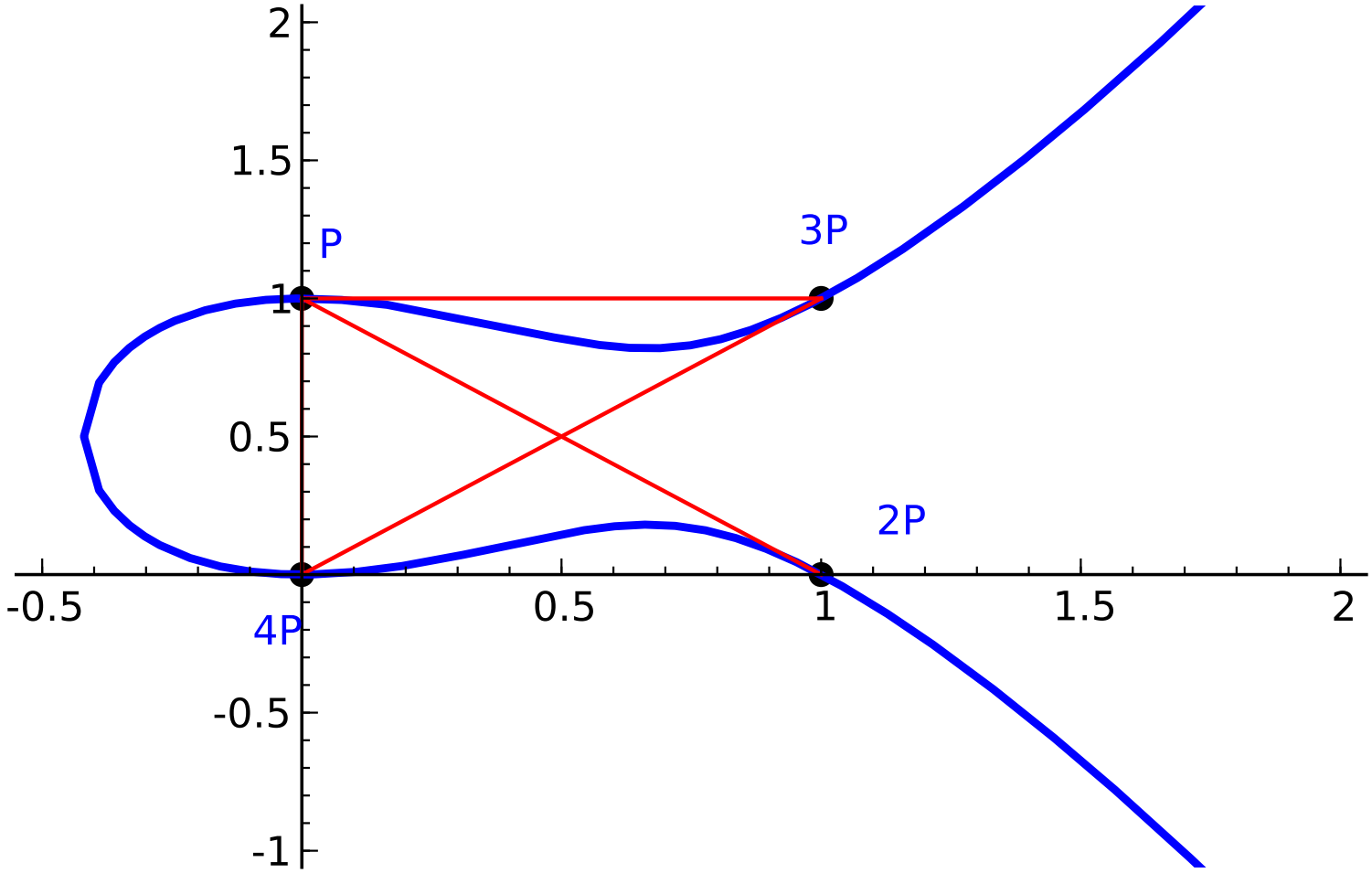
En los últimos años, ha habido un gran progreso en la clasificación de grupos de torsión de curvas elípticas sobre distintos cuerpos (de números y de funciones). Los subgrupos de torsión han capturado mucha atención...

En esta charla: subgrupos de torsión

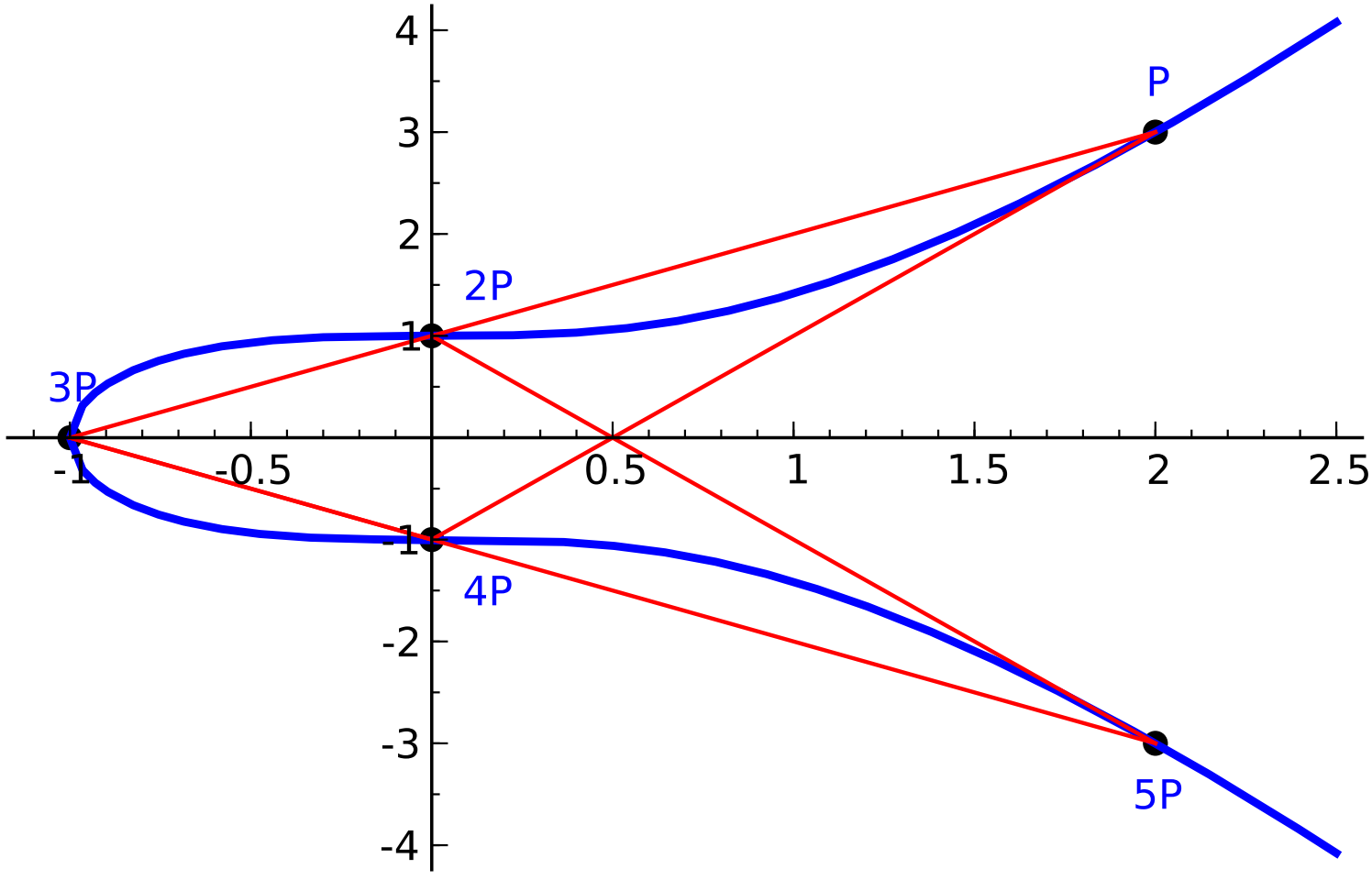
En los últimos años, ha habido un gran progreso en la clasificación de grupos de torsión de curvas elípticas sobre distintos cuerpos (de números y de funciones). Los subgrupos de torsión han capturado mucha atención...



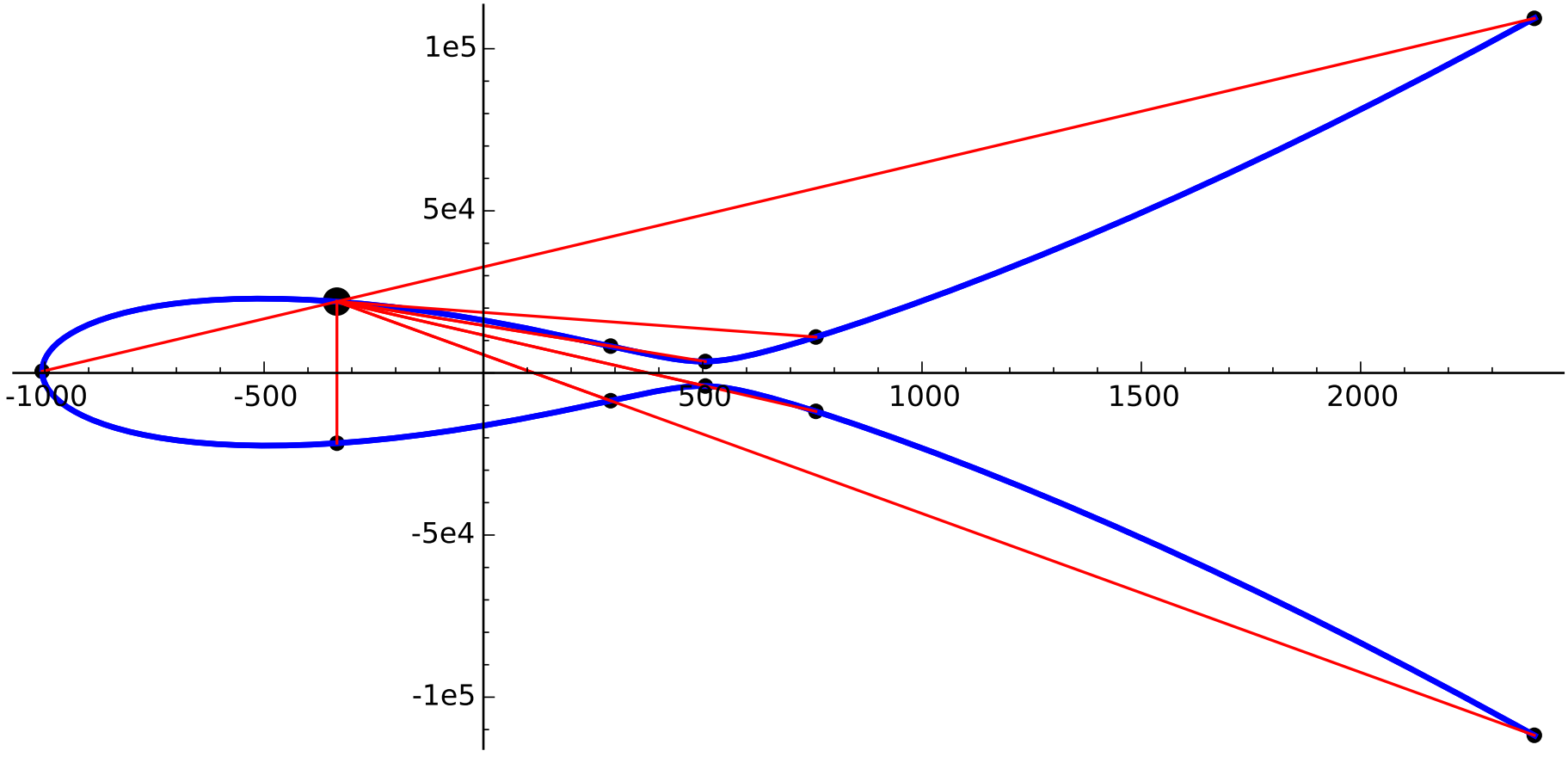
La curva elíptica $E/\mathbb{Q} : y^2 + xy + y = x^3 + x^2$
tiene un punto $P = (0, 0)$ de orden 4.



La curva $E/\mathbb{Q} : y^2 - y = x^3 - x^2$ tiene un punto $P = (0, 1)$ de orden 5.

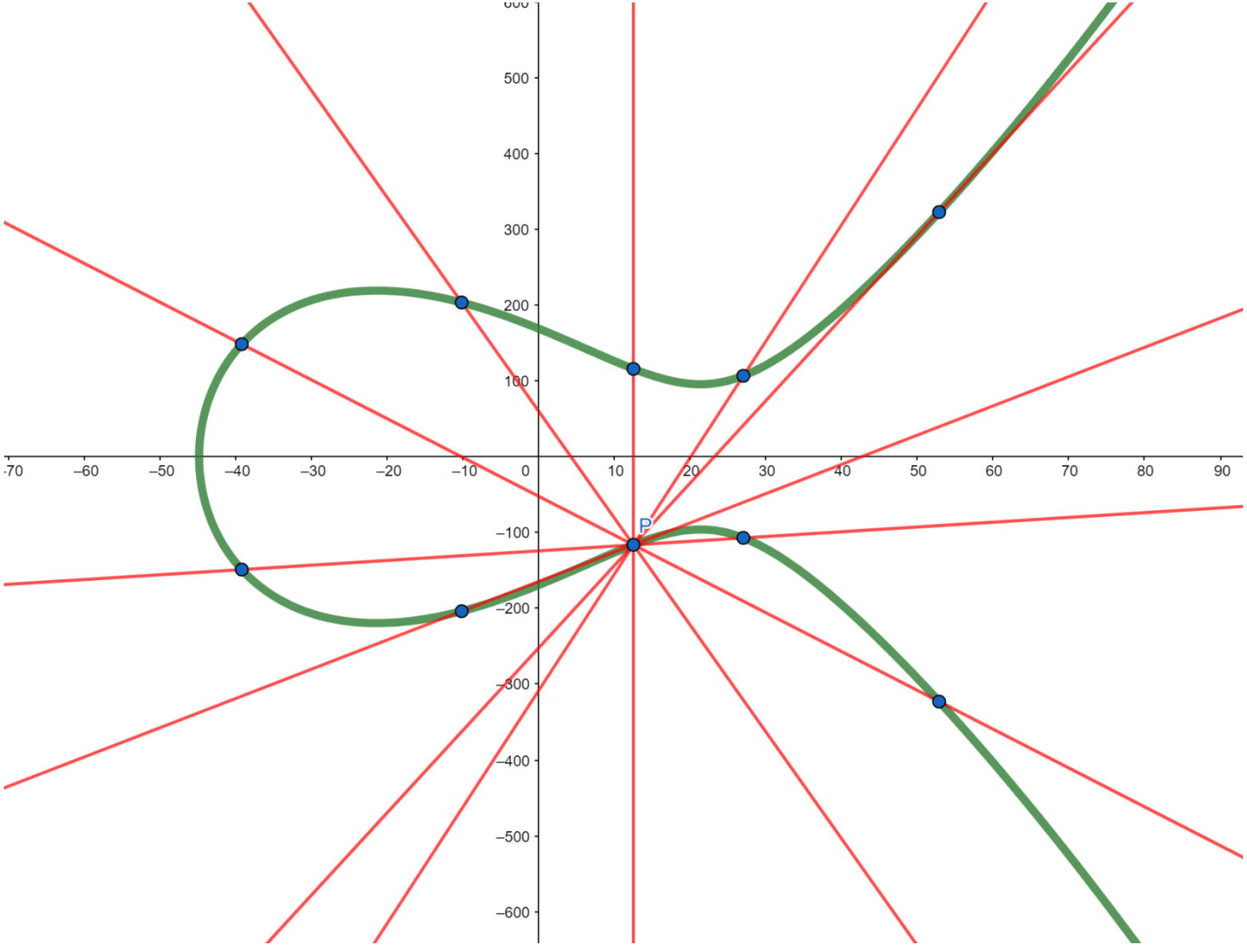


La curva elíptica $E/\mathbb{Q} : y^2 = x^3 + 1$ tiene $P = (2, 3)$ de orden 6.

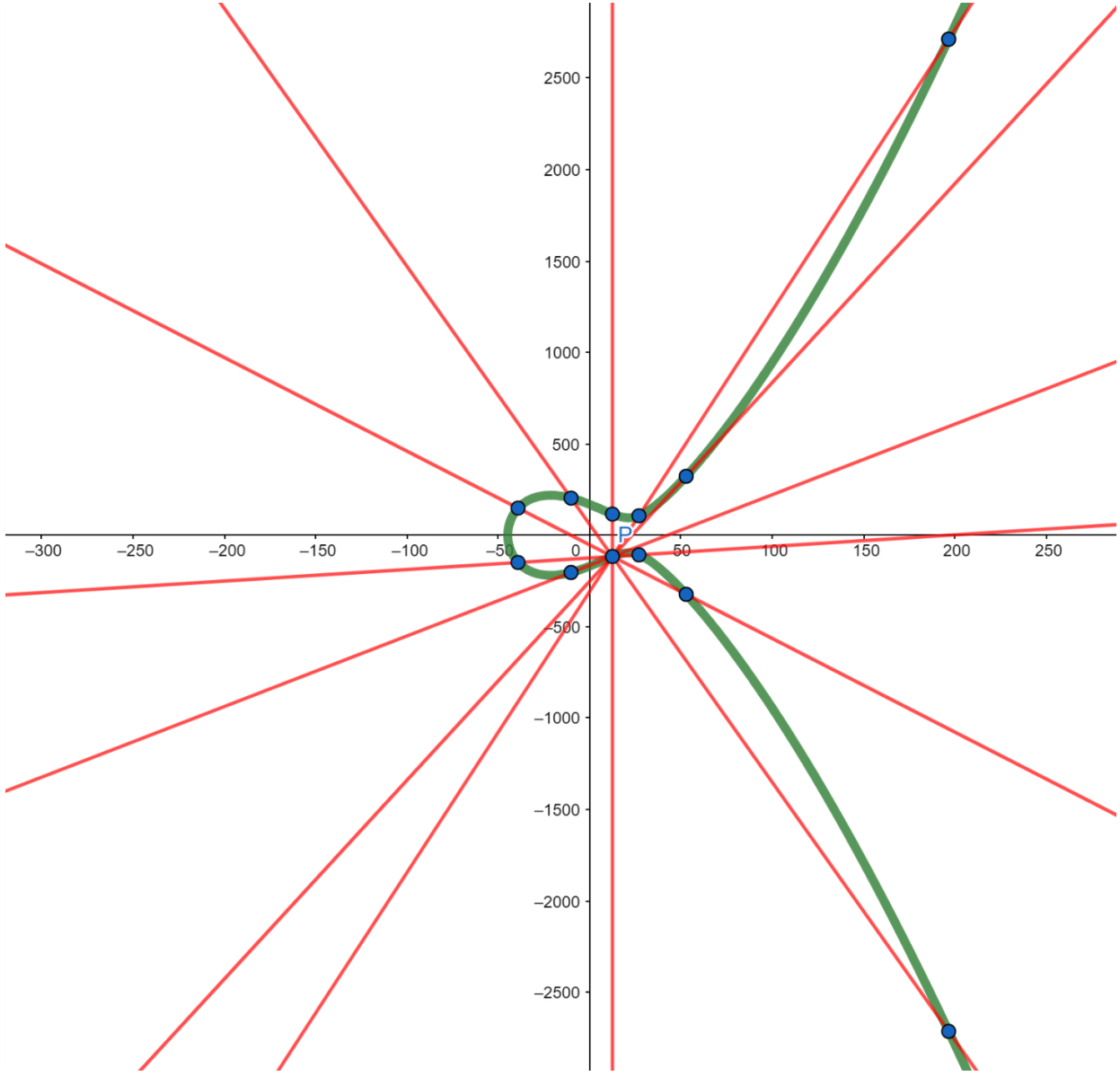


La curva elíptica `30030bt1` tiene un punto de orden 12.

$$y^2 + xy = x^3 - 749461x + 263897441.$$

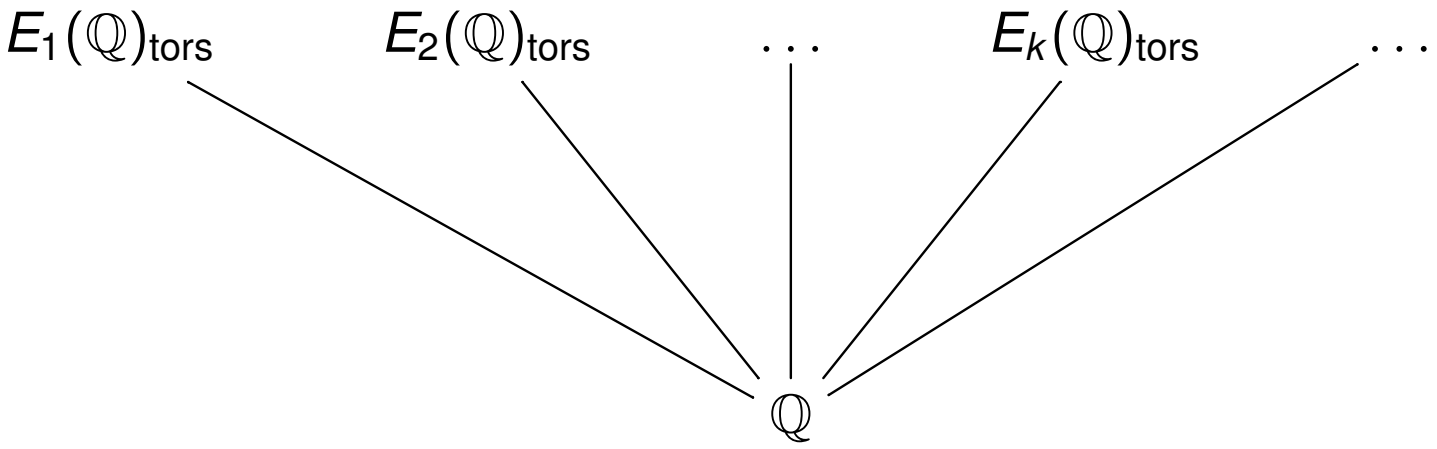


$y^2 = x^3 + (-411864 + 99560\sqrt{17})x + (211240640 - 51226432\sqrt{17})$
tiene un punto de orden 13 sobre $\mathbb{Q}(\sqrt{17})$.

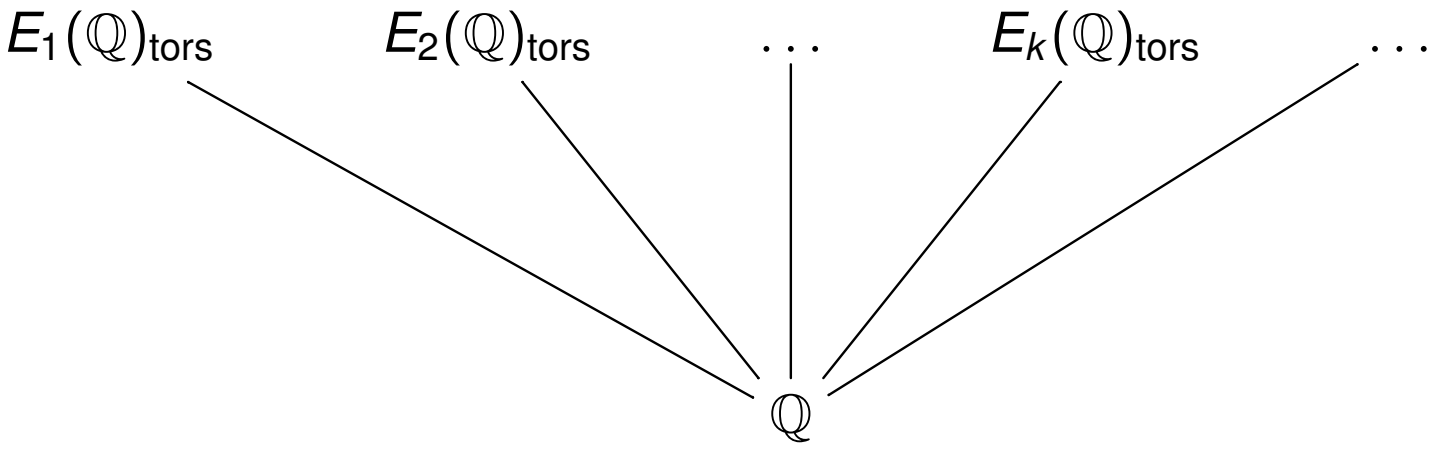


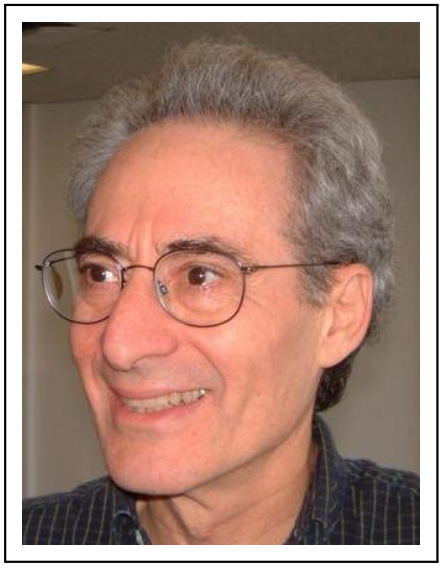
$y^2 = x^3 + (-411864 + 99560\sqrt{17})x + (211240640 - 51226432\sqrt{17})$
tiene un punto de orden 13 sobre $\mathbb{Q}(\sqrt{17})$.

Subgrupos de torsión de curvas elípticas sobre $\mathbb{Q}$



Subgrupos de torsión de curvas elípticas sobre $\mathbb{Q}$





Barry Mazur

Teorema (Conjetura de Levi–Ogg; Mazur, 1977)

Sea $E/\mathbb{Q}$ una curva elíptica. Entonces:

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

Además, cada grupo aparece un número infinito de veces.

Curvas elípticas con un subgrupo de torsión dado

Define $E(a,b) : y^2 + (1-a)xy - by = x^3 - bx^2$.

$E/\mathbb{Q}$	a	b	$G \leq E(\mathbb{Q})_{\text{tors}}$
$E(0,b)$	$a = 0$	$b = t$	$\mathbb{Z}/4\mathbb{Z}$
$E(a,a)$	$a = t$	$b = t$	$\mathbb{Z}/5\mathbb{Z}$
$E(a,b)$	$a = t$	$b = t + t^2$	$\mathbb{Z}/6\mathbb{Z}$
$E(a,b)$	$a = t^2 - t$	$b = t^3 - t^2$	$\mathbb{Z}/7\mathbb{Z}$
$E(a,b)$	$a = \frac{(2t-1)(t-1)}{t}$	$b = (2t-1)(t-1)$	$\mathbb{Z}/8\mathbb{Z}$
$E(a,b)$	$a = t^2(t-1)$	$b = t^2(t-1)(t^2-t+1)$	$\mathbb{Z}/9\mathbb{Z}$
$E(a,b)$	$a = t(t-1)(2t-1)/(t^2-3t+1)$	$b = t^3(t-1)(2t-1)/(t^2-3t+1)^2$	$\mathbb{Z}/10\mathbb{Z}$
$E(a,b)$	$a = \frac{-t(2t-1)(3t^2-3t+1)}{(t-1)^3}$	$b = \frac{t(2t-1)(2t^2-2t+1)(3t^2-3t+1)}{(t-1)^4}$	$\mathbb{Z}/12\mathbb{Z}$
$E(0,b)$	$a = 0$	$b = t^2 - 1/16$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$E(a,b)$	$a = (10-2t)/(t^2-9)$	$b = -2(t-1)^2(t-5)/(t^2-9)^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$E(a,b)$	$a = \frac{(2t+1)(8t^2+4t+1)}{2(4t+1)(8t^2-1)t}$	$b = \frac{(2t+1)(8t^2+4t+1)}{(8t^2-1)^2}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

Aquí trataremos la siguiente generalización del teorema de Mazur:

Sea $E/\mathbb{Q}$ la curva elíptica $y^2 + xy + y = x^3 - x^2 - 6x - 4$ con etiqueta `17.a2` en LMFDB.

Aquí trataremos la siguiente generalización del teorema de Mazur:

Sea $E/\mathbb{Q}$ la curva elíptica $y^2 + xy + y = x^3 - x^2 - 6x - 4$ con etiqueta `17.a2` en LMFDB.

- E tiene una isogenia (morfismo algebraico) definida sobre $\mathbb{Q}$

$$E \longrightarrow E'$$

donde $E' : y^2 + xy + y = x^3 - x^2 - 91x - 310$.

Aquí trataremos la siguiente generalización del teorema de Mazur:

Sea $E/\mathbb{Q}$ la curva elíptica $y^2 + xy + y = x^3 - x^2 - 6x - 4$ con etiqueta `17.a2` en LMFDB.

- E tiene una isogenia (morfismo algebraico) definida sobre $\mathbb{Q}$

$$E \longrightarrow E'$$

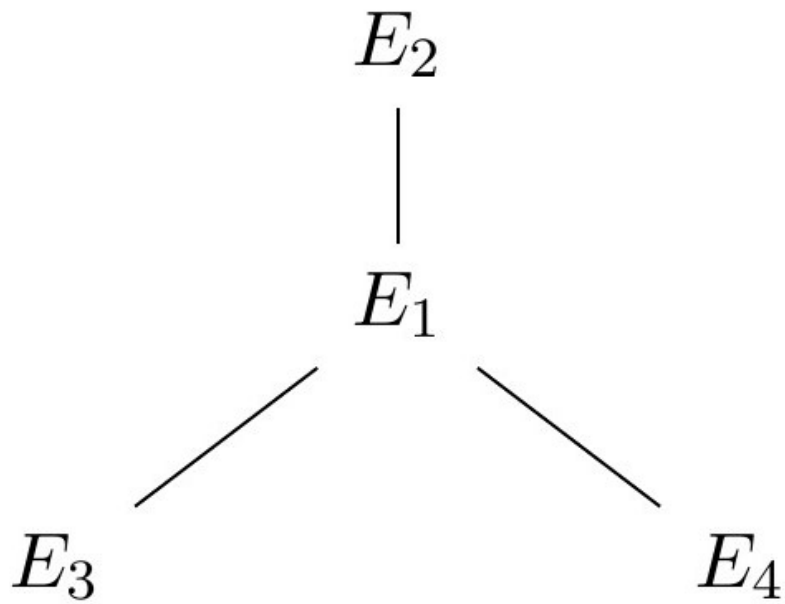
donde $E' : y^2 + xy + y = x^3 - x^2 - 91x - 310$.

Pregunta

¿Cuáles son las posibilidades de $(E(\mathbb{Q})_{\text{tors}}, E'(\mathbb{Q})_{\text{tors}})$?

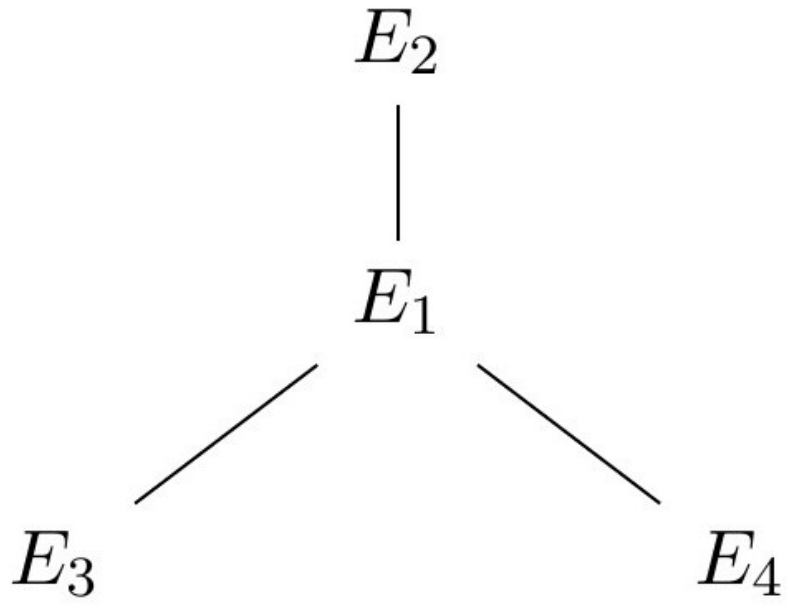
Sea $E/\mathbb{Q}$ la curva elíptica $y^2 + xy + y = x^3 - x^2 - 6x - 4$ con etiqueta `17.a2` en LMFDB.

- De hecho, $E = E_1$ es isógena (sobre $\mathbb{Q}$) a tres curvas (además de sí misma):



Sea $E/\mathbb{Q}$ la curva elíptica $y^2 + xy + y = x^3 - x^2 - 6x - 4$ con etiqueta `17.a2` en LMFDB.

- De hecho, $E = E_1$ es isógena (sobre $\mathbb{Q}$) a tres curvas (además de sí misma):

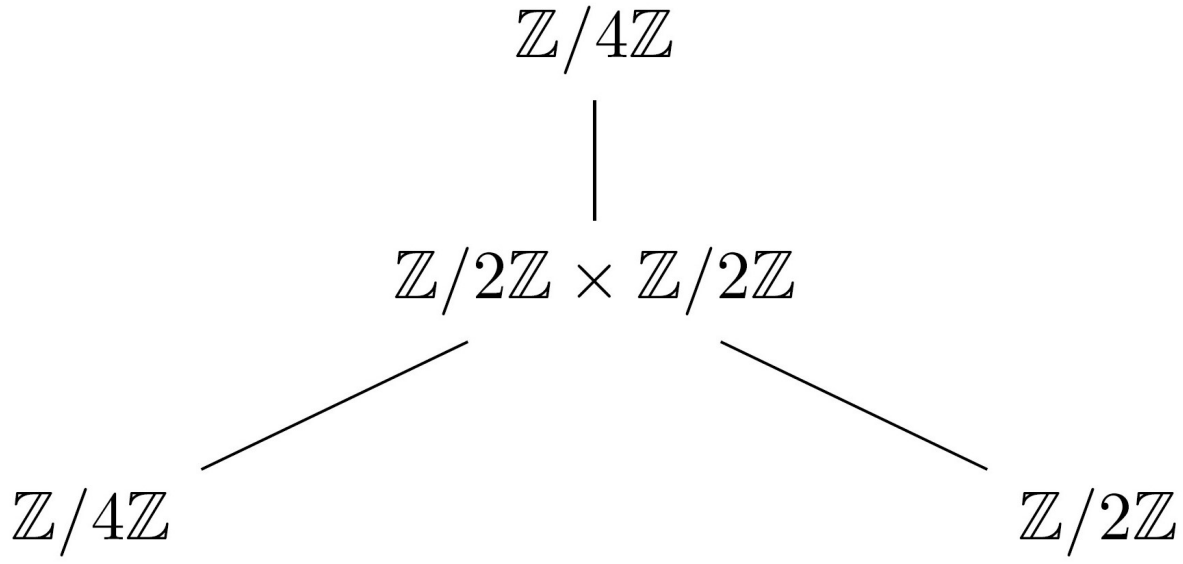


Pregunta

¿Cuáles son las posibilidades de $(E_1(\mathbb{Q})_{\text{tors}}, E_2(\mathbb{Q})_{\text{tors}}, E_3(\mathbb{Q})_{\text{tors}}, E_4(\mathbb{Q})_{\text{tors}})$?

Sea $E/\mathbb{Q}$ la curva elíptica $y^2 + xy + y = x^3 - x^2 - 6x - 4$ con etiqueta `17.a2` en LMFDB.

- En este caso tenemos:



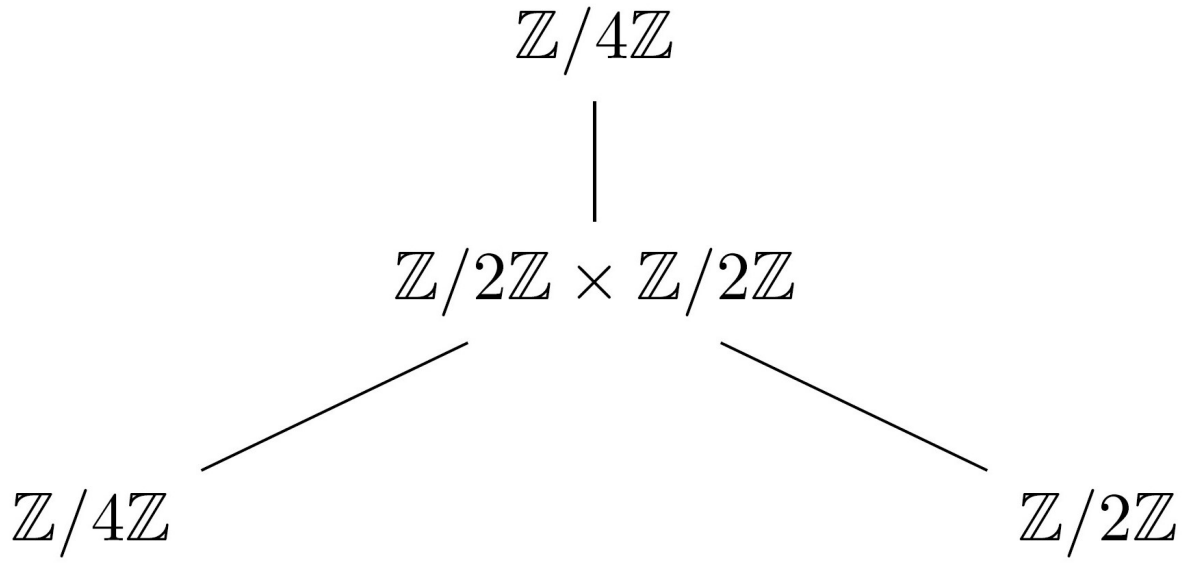
Este es un ejemplo de **grafo de isogenia-torsión**, y lo abreviamos como $([2,2],[4],[4],[2])$ de tipo T_4.

Pregunta

¿Cuáles son las posibilidades de $(E_1(\mathbb{Q})_{\text{tors}}, E_2(\mathbb{Q})_{\text{tors}}, E_3(\mathbb{Q})_{\text{tors}}, E_4(\mathbb{Q})_{\text{tors}})$ en general?

Sea $E/\mathbb{Q}$ la curva elíptica $y^2 + xy + y = x^3 - x^2 - 6x - 4$ con etiqueta `17.a2` en LMFDB.

- En este caso tenemos:



Este es un ejemplo de **grafo de isogenia-torsión**, y lo abreviamos como $([2,2],[4],[4],[2])$ de tipo T_4.

Pregunta

¿Cuáles son las posibilidades de $(E_1(\mathbb{Q})_{\text{tors}}, E_2(\mathbb{Q})_{\text{tors}}, E_3(\mathbb{Q})_{\text{tors}}, E_4(\mathbb{Q})_{\text{tors}})$ en general?

Primero... ¿qué grafos de isogenia existen sobre $\mathbb{Q}$?

Modular Functions of One Variable IV

Proceedings of the International Summer School,
University of Antwerp, RUCA,
July 17 – August 3, 1972

...

REMARKS ON ISOGENIES.

An examination of Table 1 might suggest that an elliptic curve over Q is usually isogenous to several others, and that isogenies of fairly high degree are not uncommon. This is not so - the elliptic curves of low conductor are not at all typical, they have many more interesting properties than they deserve. The tables in fact illustrate almost all the known ways in which isogenies can occur; they miss the 17- and the 37- isogeny, and they also miss the examples of complex multiplication by $\frac{1}{2}(1+\sqrt{-D})$ for D = 19, 43, 67 and 163.

Teorema

Hay 10 *tipos de isomorfismo de grafos de* $\mathbb{Q}$*-isogenias que están asociados a curvas elípticas sobre* $\mathbb{Q}$*.*

Teorema

Hay 10 *tipos de isomorfismo de grafos de* $\mathbb{Q}$*-isogenias que están asociados a curvas elípticas sobre* $\mathbb{Q}$*. En particular, hay*

- 4 *tipos de grafos L (lineales),*
- 3 *tipos de grafos T (torsión* 2*-primaria),*
- 2 *tipos de grafos R (rectangulares), y*
- 1 *tipo de grafo S (especial).*

Teorema

Hay 10 *tipos de isomorfismo de grafos de* $\mathbb{Q}$*-isogenias que están asociados a curvas elípticas sobre* $\mathbb{Q}$*. En particular, hay*

- 4 *tipos de grafos L (lineales),*
- 3 *tipos de grafos T (torsión* 2*-primaria),*
- 2 *tipos de grafos R (rectangulares), y*
- 1 *tipo de grafo S (especial).*

Además, sólo 4 *de estos tipos de grafos están asociados a curvas con multiplicación compleja (CM):* L_2*,* L_4*,* T_4*, y* R_4*. Finalmente, el tipo* L_4 *sólo ocurre en el caso CM.*

Teorema

Hay 10 *tipos de isomorfismo de grafos de* $\mathbb{Q}$*-isogenias que están asociados a curvas elípticas sobre* $\mathbb{Q}$*. En particular, hay*

- 4 *tipos de grafos L (lineales),*
- 3 *tipos de grafos T (torsión* 2*-primaria),*
- 2 *tipos de grafos R (rectangulares), y*
- 1 *tipo de grafo S (especial).*

Además, sólo 4 *de estos tipos de grafos están asociados a curvas con multiplicación compleja (CM):* L_2*,* L_4*,* T_4*, y* R_4*. Finalmente, el tipo* L_4 *sólo ocurre en el caso CM.*

Teorema (Chiloyan–L-R.)

Hay 37 *tipos de grafos de isogenia-torsión sobre* $\mathbb{Q}$*. En particular, hay* 12 *tipos de grafos L,* 13 *tipos de grafos T ,* 8 *tipos de grafos R, y* 4 *tipos de grafos S. Además, hay* 10 *tipos de grafos de isogenia-torsión que están asociados a curvas con CM sobre* $\mathbb{Q}$*.*

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

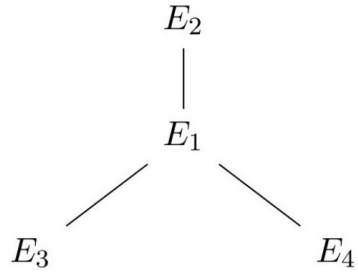
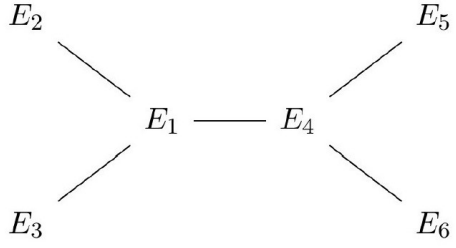
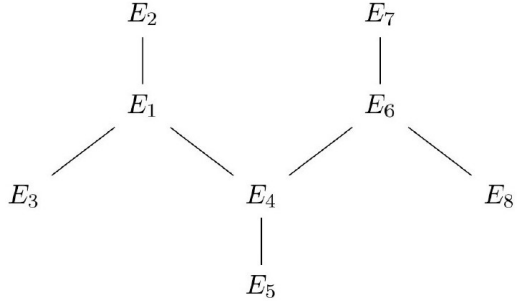
Graph Type	Label	Isomorphism Types	LMFDB Label
	T_4	([2,2], [2], [2], [2])	120.a
		([2,2], [4], [2], [2])	33.a
		([2,2], [4], [4], [2])	17.a
	T_6	([2,4],[4],[4],[2,2],[2],[2])	24.a
		([2,4],[8],[4],[2,2],[2],[2])	21.a
		([2,2],[2],[2],[2,2],[2],[2])	126.a
		([2,2],[4],[2],[2,2],[2],[2])	63.a
	T_8	([2,8],[8],[8],[2,4],[4],[2,2],[2],[2])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

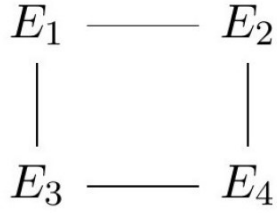
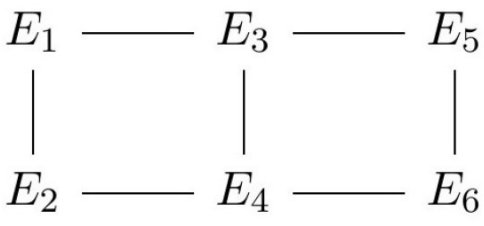
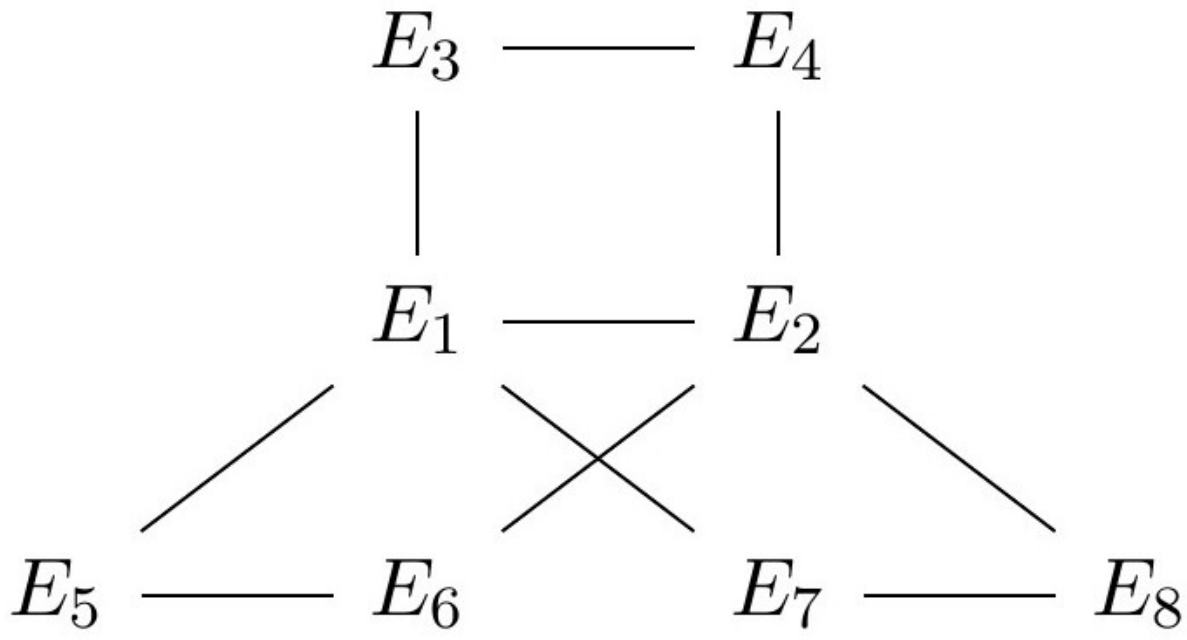
Graph Type	Label	Isomorphism Types	LMFDB Label
	R_4	([1],[1],[1],[1])	400.f
		([2],[2],[2],[2])	49.a
		([3],[3],[1],[1])	50.a
		([5],[5],[1],[1])	50.b
		([6],[6],[2],[2])	20.a
		([10],[10],[2],[2])	66.c
	R_6	([2],[2],[2],[2],[2],[2])	98.a
		([6],[6],[6],[6],[2],[2])	14.a

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



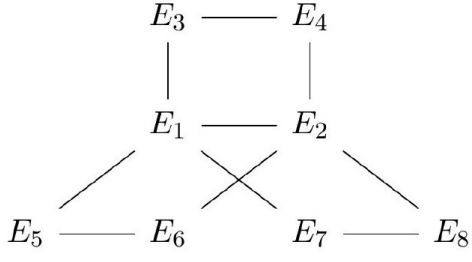
Graph Type	Label	Isomorphism Types	LMFDB Label
	S	([2,2],[2,2],[2],[2],[2],[2],[2],[2])	240.b
		([2,2],[2,2],[4],[4],[2],[2],[2],[2])	150.b
		([2,6],[2,2],[6],[2],[6],[2],[6],[2])	30.a
		([2,6],[2,2],[12],[4],[6],[2],[6],[2])	90.c

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

d_K	j		Type	Torsion config.	LMFDB
-3	0	$y^2 = x^3 + t^3, t = -3, 1$	R_4	$([6],[6],[2],[2])$	36.a4
		$y^2 = x^3 + t^3, t \neq -3, 1$	R_4	$([2],[2],[2],[2])$	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	$([3],[1])$	108.a2
		$y^2 = x^3 + s,\ s \neq t^3, 16t^3$	L_2	$([1],[1])$	225.c1
	$2^4 \cdot 3^3 \cdot 5^3$	$y^2 = x^3 - 15t^2x + 22t^3, t = 1, 3$	R_4	$([6],[6],[2],[2])$	36.a1
		$y^2 = x^3 - 15t^2x + 22t^3, t \neq 1, 3$	R_4	$([2],[2],[2],[2])$	144.a1
	$-2^{15} \cdot 3 \cdot 5^3$	$E^t, t = -3, 1$	L_4	$([3],[3],[3],[1])$	27.a2
		$E^t, t \neq -3, 1$	L_4	$([1],[1],[1],[1])$	432.e1
-4	$2^6 \cdot 3^3$	$y^2 = x^3 + tx, t = -1, 4$	T_4	$([2,2],[4],[4],[2])$	32.a3
		$y^2 = x^3 + tx, t = -4, 1$	T_4	$([2,2],[4],[2],[2])$	64.a3
		$y^2 = x^3 \pm t^2x, t \neq 1, 2$	T_4	$([2,2],[2],[2],[2])$	288.d3
		$y^2 = x^3 + sx,\ s \neq \pm t^2$	L_2	$([2],[2])$	256.b1
	$2^3 \cdot 3^3 \cdot 11^3$	$y^2 = x^3 - 11t^2x + 14t^3, t = \pm 1$	T_4	$([2,2],[4],[4],[2])$	32.a2
		$y^2 = x^3 - 11t^2x + 14t^3, t = \pm 2$		$([2,2],[4],[2],[2])$	64.a1
		$y^2 = x^3 - 11t^2x + 14t^3, t \neq \pm 1, \pm 2$		$([2,2],[2],[2],[2])$	288.d1
-7	$-3^3 \cdot 5^3$		R_4	$([2],[2],[2],[2])$	49.a2
	$3^3 \cdot 5^3 \cdot 17^3$		R_4	$([2],[2],[2],[2])$	49.a1
-8	$2^6 \cdot 5^3$		L_2	$([2],[2])$	256.a1
-11	-2^{15}		L_2	$([1],[1])$	121.b1
-19	$-2^{15} \cdot 3^3$		L_2	$([1],[1])$	361.a1
-43	$-2^{18} \cdot 3^3 \cdot 5^3$		L_2	$([1],[1])$	1849.b1
-67	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$		L_2	$([1],[1])$	4489.b1
-163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$		L_2	$([1],[1])$	26569.a1

TABLE 5. The list of rational j-invariants with CM and the possible isogeny-torsion graphs that occur, where E^t denotes the curve $y^2 = x^3 - 38880t^2x + 2950992t^3$.

Primera parte clave de la clasificación:

La clasificación de grafos de isogenia.

Primera parte clave de la clasificación:

La clasificación de grafos de isogenia.

Un ingrediente principal es un teorema de

Monsur A. Kenku

JOURNAL OF NUMBER THEORY 15, 199–202 (1982)

On the Number of **Q**-Isomorphism Classes of Elliptic Curves in Each **Q**-Isogeny Class

M. A. KENKU*

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540

Communicated by S. Chowla

Received December 17, 1980

It is shown that there are at most eight **Q**-isomorphism classes of elliptic curves in each **Q**-isogeny class.

In the table of elliptic curves published in [1] one finds that the number of vertices in the graph of rational isogenies is at most 8. Serre [12] has asked whether in fact 8 is a universal bound. Below we show that this is so.

Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isógena a como mucho 8 curvas (incluyendo a si misma).

Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isógena a como mucho 8 curvas (incluyendo a si misma). Más concretamente, sea $E/\mathbb{Q}$ una curva elíptica y

- *sea $C(E)$ el número de subgrupos cíclicos $\mathbb{Q}$-racionales de E (incluyendo el grupo $\{\mathcal{O}\}$), y*
- *sea $C_p(E)$ el número de subgrupos cíclicos $\mathbb{Q}$-racionales de E de orden una potencia de un primo p.*

Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isógena a como mucho 8 curvas (incluyendo a si misma). Más concretamente, sea $E/\mathbb{Q}$ una curva elíptica y

- *sea $C(E)$ el número de subgrupos cíclicos $\mathbb{Q}$-racionales de E (incluyendo el grupo $\{\mathcal{O}\}$), y*
- *sea $C_p(E)$ el número de subgrupos cíclicos $\mathbb{Q}$-racionales de E de orden una potencia de un primo p.*

Entonces, $C(E) = \prod_p C_p(E) \leq 8$.

Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isógena a como mucho 8 curvas (incluyendo a si misma). Más concretamente, sea $E/\mathbb{Q}$ una curva elíptica y

- *sea $C(E)$ el número de subgrupos cíclicos $\mathbb{Q}$-racionales de E (incluyendo el grupo $\{\mathcal{O}\}$), y*
- *sea $C_p(E)$ el número de subgrupos cíclicos $\mathbb{Q}$-racionales de E de orden una potencia de un primo p.*

Entonces, $C(E) = \prod_p C_p(E) \leq 8$. Además, cada factor $C_p(E)$ está acotado por:

p	2	3	5	7	11	13	17	19	37	43	67	163	*resto*
$C_p \leq$	8	4	3	2	2	2	2	2	2	2	2	2	1.

Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isógena a como mucho 8 curvas (incluyendo a si misma). Además, $C(E) = \prod_p C_p(E) \leq 8$, hay cotas para cada $C_p(E)$ y

Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isógena a como mucho 8 curvas (incluyendo a si misma). Además, $C(E) = \prod_p C_p(E) \leq 8$, hay cotas para cada $C_p(E)$ y

1. *Si $C_p(E) = 2$ para $p > 7$, then $C_q(E) = 1$ para todo otro primo q.*
2. *Si $C_7(E) = 2$, entonces $C(E) \leq 4$. Además, $C_3(E) = 2$, ó $C_2(E) = 2$, ó $C(E) = 2$.*
3. *$C_5(E) \leq 3$ y si $C_5(E) = 3$, entonces $C(E) = 3$.*
4. *Si $C_5(E) = 2$, entonces $C(E) \leq 4$. Además, o bien $C_3(E) = 2$, ó $C_2(E) = 2$, ó $C(E) = 2$.*
5. *$C_3(E) \leq 4$ y si $C_3(E) = 4$, entonces $C(E) = 4$.*
6. *Si $C_3(E) = 3$, entonces $C(E) \leq 6$. Además, $C_2(E) = 2$ ó $C(E) = 3$.*
7. *Si $C_3(E) = 2$, entonces $C_2(E) \leq 4$.*

Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isogena a como mucho 8 curvas...

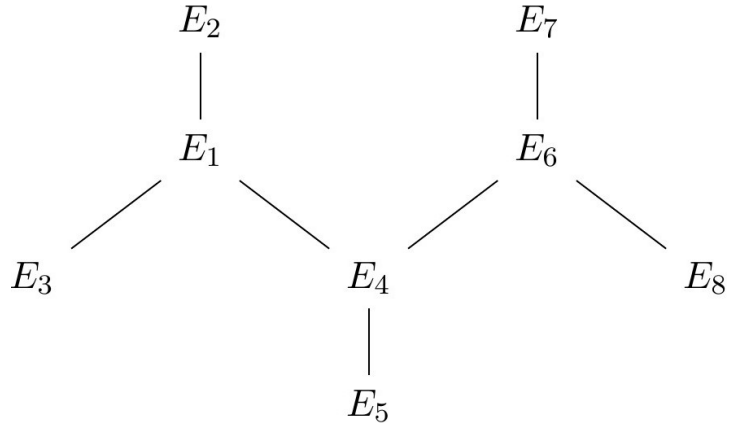
Por ejemplo,

Teorema (Kenku)

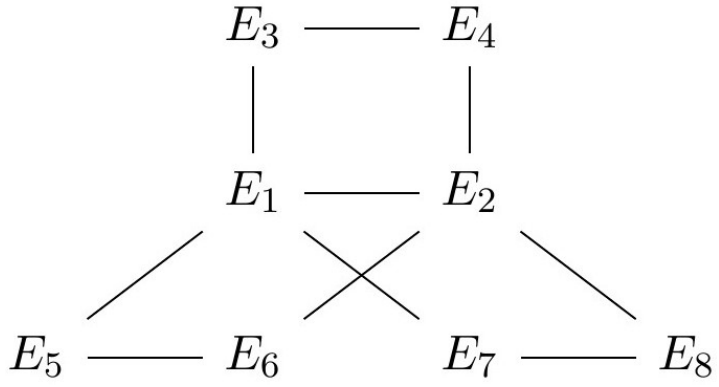
Una curva elíptica es $\mathbb{Q}$-isogena a como mucho 8 curvas...

Por ejemplo, si $C(E) = 8$, entonces

- $C(E) = C_2(E) = 8$ y tenemos el grafo T_8:



- o bien $C(E) = C_2(E) \cdot C_3(E) = 4 \cdot 2$ y tenemos el grafo S:



Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isogena a como mucho 8 curvas...

Por ejemplo, si $C(E) = 8$, entonces

Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isogena a como mucho 8 curvas...

Por ejemplo, si $C(E) = 8$, entonces

- Si $C(E) = C_2(E) = 8$ y E no tiene 8-isogenias, entonces E tiene que tener por lo menos dos 4-isogenias independientes.

Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isogena a como mucho 8 curvas...

Por ejemplo, si $C(E) = 8$, entonces

- Si $C(E) = C_2(E) = 8$ y E no tiene 8-isogenias, entonces E tiene que tener por lo menos dos 4-isogenias independientes.
- O bien E tiene una 8-isogenia, y una 2-isogenia independiente.

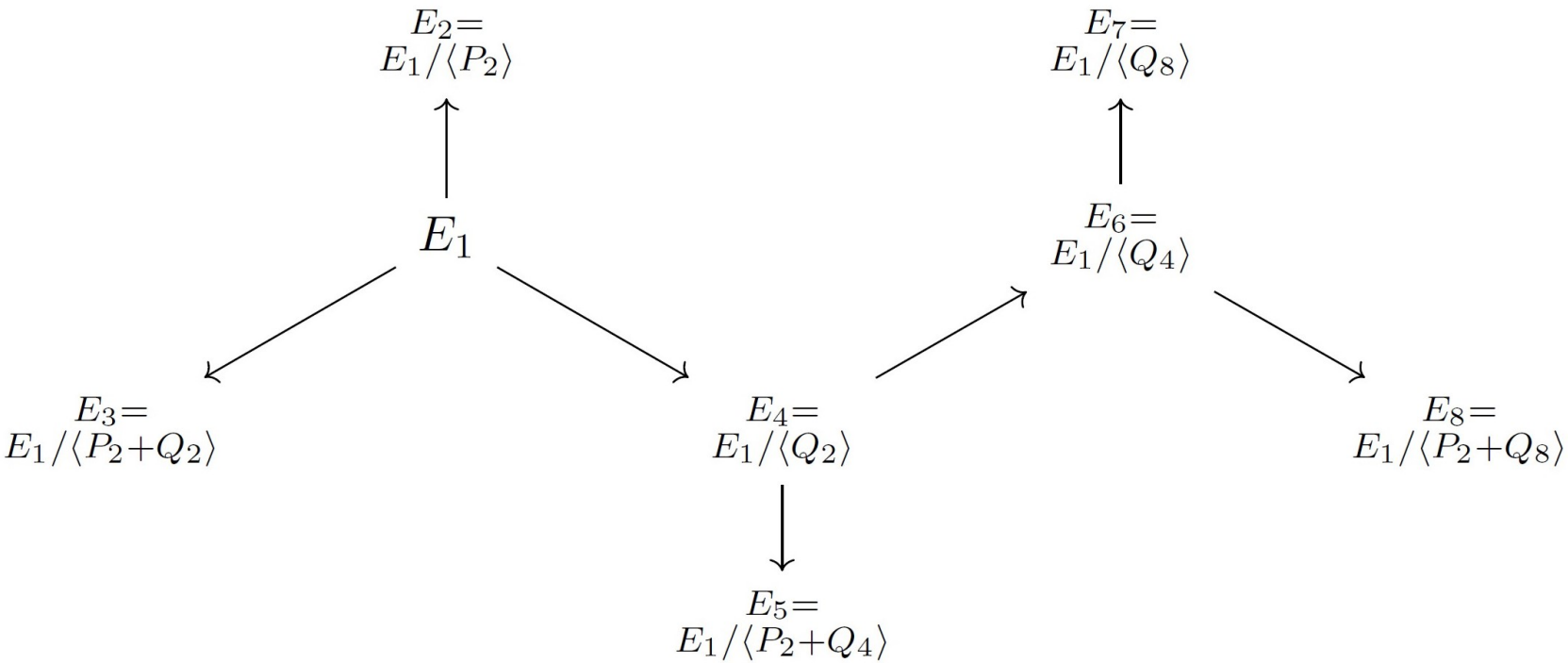
Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isogena a como mucho 8 curvas...

Por ejemplo, si $C(E) = 8$, entonces

- Si $C(E) = C_2(E) = 8$ y E no tiene 8-isogenias, entonces E tiene que tener por lo menos dos 4-isogenias independientes.
- O bien E tiene una 8-isogenia, y una 2-isogenia independiente.

En ambos casos llegamos al grafo:



Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isogena a como mucho 8 curvas...

Por ejemplo, si $C(E) = 8$, entonces

Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isogena a como mucho 8 curvas...

Por ejemplo, si $C(E) = 8$, entonces

- Si $C(E) = C_2(E) \cdot C_3(E) = 4 \cdot 2$, entonces $C_2(E) = 4$ implica que una de las curvas tiene 2-torsión definida sobre $\mathbb{Q}$, y $C_3(E) = 2$ implica que existe una 3-isogenia.

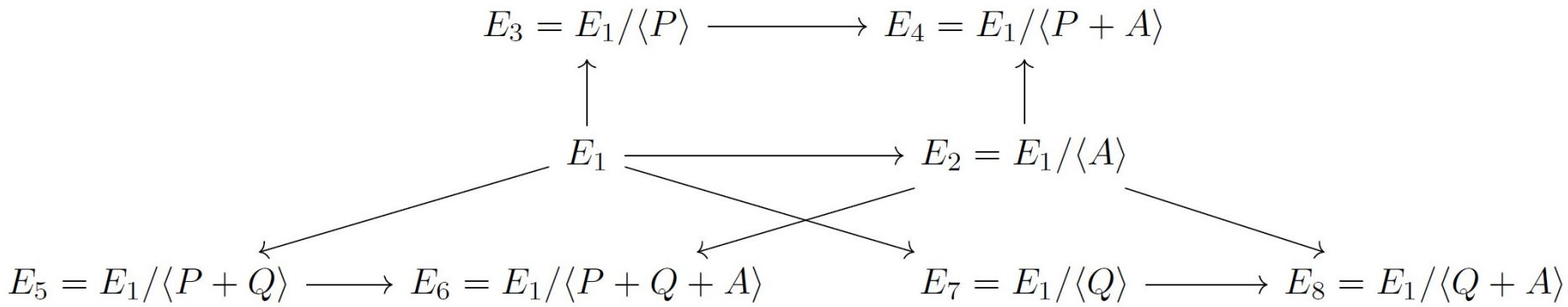
Teorema (Kenku)

Una curva elíptica es $\mathbb{Q}$-isogena a como mucho 8 curvas...

Por ejemplo, si $C(E) = 8$, entonces

- Si $C(E) = C_2(E) \cdot C_3(E) = 4 \cdot 2$, entonces $C_2(E) = 4$ implica que una de las curvas tiene 2-torsión definida sobre $\mathbb{Q}$, y $C_3(E) = 2$ implica que existe una 3-isogenia.

En este caso llegamos al grafo:



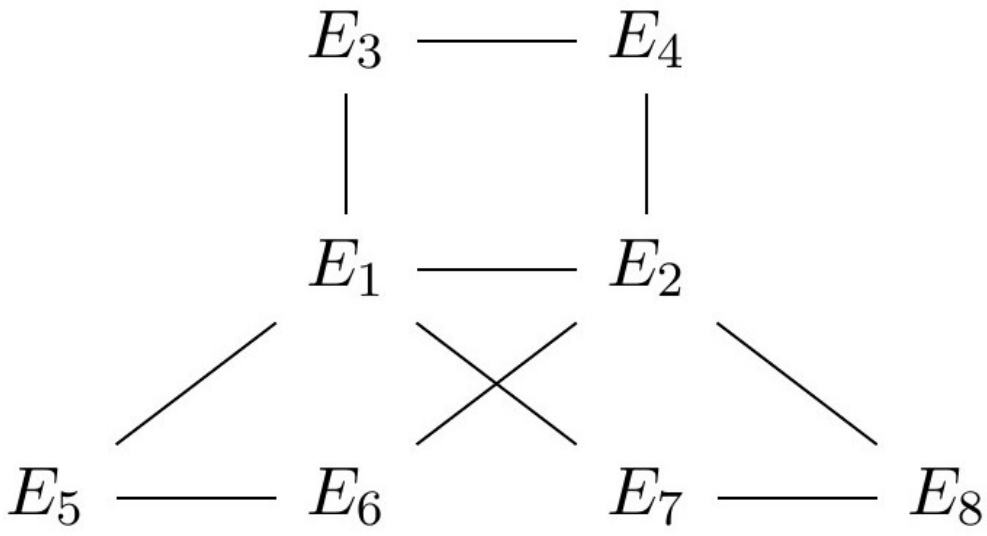
Segunda parte de la clasificación:

clasificación de grafos de isogenia-torsión.

Segunda parte de la clasificación:

clasificación de grafos de isogenia-torsión.

Un ejemplo: consideremos los grafos de isogenia-torsión de tipo *S*



Un ejemplo: consideremos los grafos de isogenia-torsión de tipo *S*. Estas son las posibles configuraciones que aparecen:

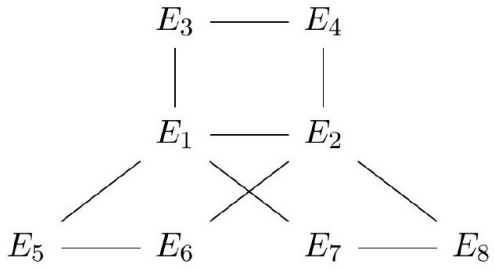
Graph Type	Label	Isomorphism Types	LMFDB Label
	S	([2,2],[2,2],[2],[2],[2],[2],[2],[2])	240.b
		([2,2],[2,2],[4],[4],[2],[2],[2],[2])	150.b
		([2,6],[2,2],[6],[2],[6],[2],[6],[2])	30.a
		([2,6],[2,2],[12],[4],[6],[2],[6],[2])	90.c

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

Un ejemplo: consideremos los grafos de isogenia-torsión de tipo S. Estas son las posibles configuraciones que aparecen:

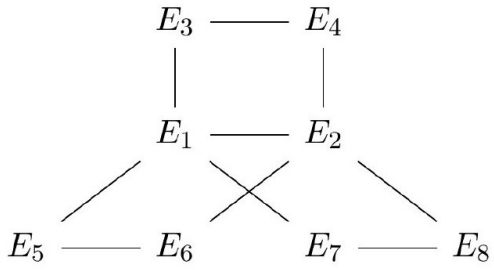
Graph Type	Label	Isomorphism Types	LMFDB Label
	S	([2,2],[2,2],[2],[2],[2],[2],[2],[2])	240.b
		([2,2],[2,2],[4],[4],[2],[2],[2],[2])	150.b
		([2,6],[2,2],[6],[2],[6],[2],[6],[2])	30.a
		([2,6],[2,2],[12],[4],[6],[2],[6],[2])	90.c

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

Pregunta

¿Son las configuraciones

$$([2,2],[2,2],[4],[4],[4],[4],[2],[2])$$

ó

$$([2,6],[2,2],[12],[4],[12],[4],[6],[2])$$

posibles?

Pregunta

¿Son las configuraciones $([2,2],[2,2],[4],[4],[4],[4],[2],[2])$ ó $([2,6],[2,2],[12],[4],[12],[4],[6],[2])$ posibles?

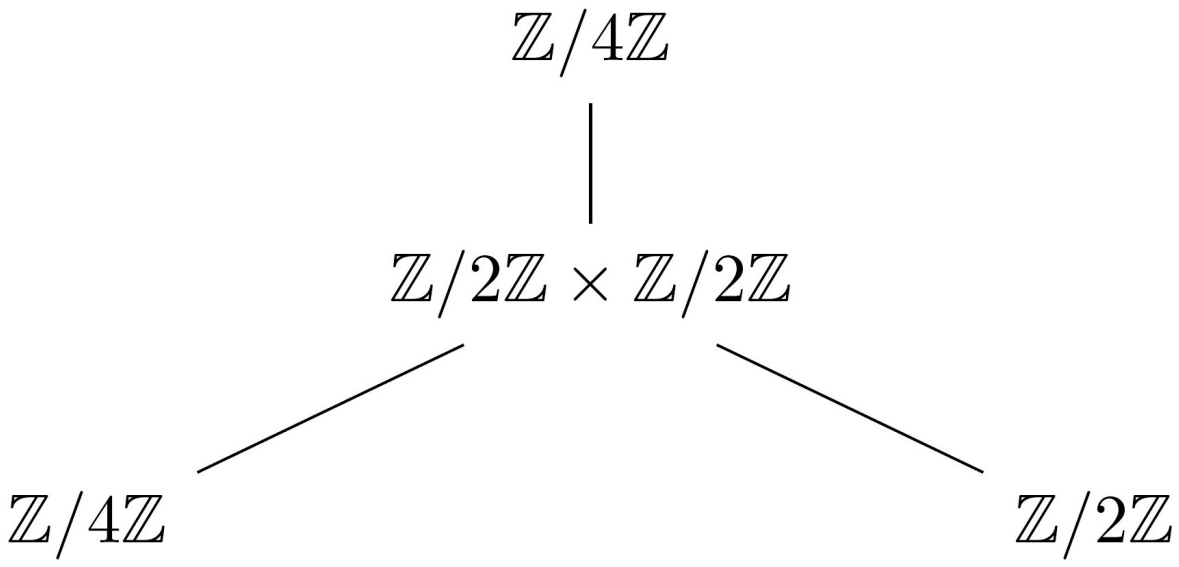
En ambos casos, dos cosas occurren:

Pregunta

¿Son las configuraciones $([2,2],[2,2],[4],[4],[4],[4],[2],[2])$ ó $([2,6],[2,2],[12],[4],[12],[4],[6],[2])$ posibles?

En ambos casos, dos cosas occurren:

1. El grafo de 2-isogenias es de tipo T_4, y el grafo de 2-isogenia-torsión es de tipo $([2,2],[4],[4],[2])$.

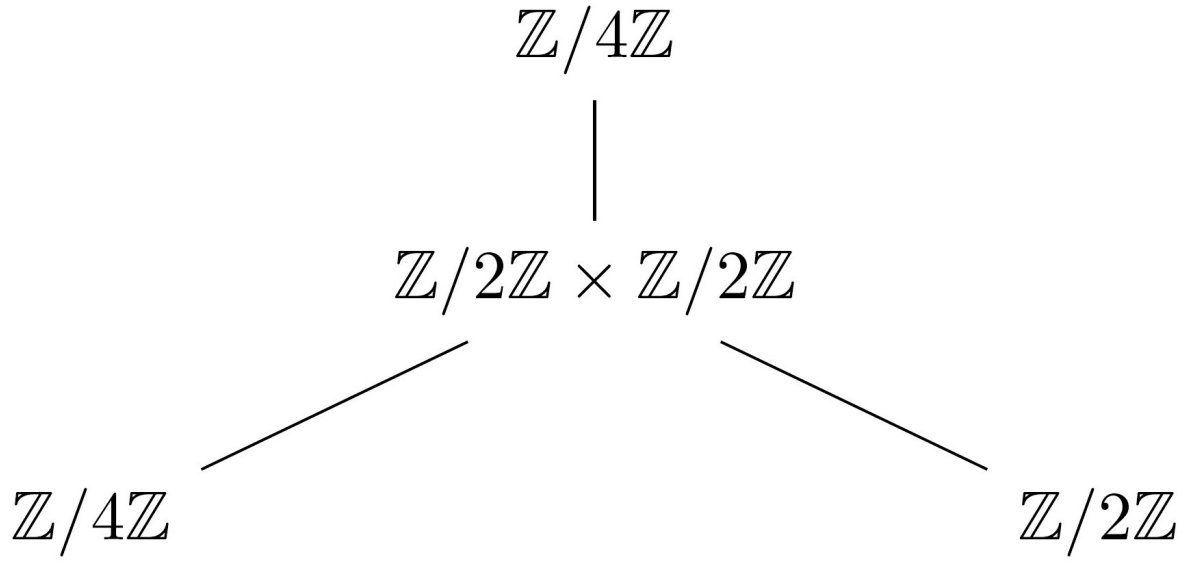


Pregunta

¿Son las configuraciones $([2,2],[2,2],[4],[4],[4],[4],[2],[2])$ ó $([2,6],[2,2],[12],[4],[12],[4],[6],[2])$ posibles?

En ambos casos, dos cosas occurren:

1. El grafo de 2-isogenias es de tipo T_4, y el grafo de 2-isogenia-torsión es de tipo $([2,2],[4],[4],[2])$.



2. Toda curva en el grafo tiene una 3-isogenia.

Primero, clasificamos curvas cuyo grafo de 2-isogenia-torsión es de tipo T_4 con grupos de torsión $([2,2],[4],[4],[2])$:

Primero, clasificamos curvas cuyo grafo de 2-isogenia-torsión es de tipo T_4 con grupos de torsión $([2,2],[4],[4],[2])$:

Esta condición determina la imagen de la representación de Galois

$$\rho_{E,4}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[4]) \cong \mathrm{GL}(2,\mathbb{Z}/4\mathbb{Z})$$

Primero, clasificamos curvas cuyo grafo de 2-isogenia-torsión es de tipo T_4 con grupos de torsión $([2,2],[4],[4],[2])$:

Esta condición determina la imagen de la representación de Galois

$$\rho_{E,4}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[4]) \cong \mathrm{GL}(2,\mathbb{Z}/4\mathbb{Z})$$

La imagen es un subgrupo de $\mathrm{GL}(2,\mathbb{Z}/4\mathbb{Z})$ que es conjugado de

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

Sea $E/\mathbb{Q}$ una curva elíptica, y sea $T_2(E) = \varprojlim E[2^n]$ el módulo de Tate. La acción de Galois de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sobre $T_2(E)$ induce

$$\rho_{E,2^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_2(E)) \cong \mathrm{GL}(2, \mathbb{Z}_2).$$

Sea $E/\mathbb{Q}$ una curva elíptica, y sea $T_2(E) = \varprojlim E[2^n]$ el módulo de Tate. La acción de Galois de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sobre $T_2(E)$ induce

$$\rho_{E,2^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_2(E)) \cong \mathrm{GL}(2, \mathbb{Z}_2).$$

Teorema (Rouse y Zureick-Brown, 2014)

Sea $E/\mathbb{Q}$ una curva elíptica sin CM. Entonces, hay precisamente 1208 posibilidades para la imágen $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, hasta conjugación. Además, la representación $\rho_{E,2^\infty}$ está definida (cómo mucho) módulo 32.


$\mathbf{F}_p(t)$
|
$\mathbf{F}_p(t^p)$
We're inseparable


$\mathbb{F}_p(t)$
|
$\mathbb{F}_p(t^p)$
We're inseparable

Primero, clasificamos curvas cuyo grafo de 2-isogenias es de tipo T_4, y el grafo de 2-isogenia-torsión es de tipo $([2,2],[4],[4],[2])$:

Esta condición determina la imagen de

$$\rho_{E,4}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[4]) \cong \mathrm{GL}(2,\mathbb{Z}/4\mathbb{Z})$$

La imagen es un subgrupo de $\mathrm{GL}(2,\mathbb{Z}/4\mathbb{Z})$ que es conjugado de

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

Primero, clasificamos curvas cuyo grafo de 2-isogenias es de tipo T_4, y el grafo de 2-isogenia-torsión es de tipo $([2,2],[4],[4],[2])$:

Esta condición determina la imagen de

$$\rho_{E,4}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[4]) \cong \mathrm{GL}(2,\mathbb{Z}/4\mathbb{Z})$$

La imagen es un subgrupo de $\mathrm{GL}(2,\mathbb{Z}/4\mathbb{Z})$ que es conjugado de

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

Sea $\widehat{H} \subseteq \mathrm{GL}(2,\mathbb{Z}_2)$ el mayor subgrupo tal que $\widehat{H} \equiv H \bmod 4$. Usamos la base de datos de imágenes 2-ádicas de Rouse–Zureick-Brown, y encontramos que las curvas elípticas con imágen 2-ádica contenida en $\widehat{H}$ vienen parametrizadas por una curva modular, X_{24e} en la nomenclatura de R–Z-B.

La curva modular X_{24e} es de género 0, y podemos parametrizar las curvas elípticas como una familia sobre $\mathbb{Q}(t)$:

$$E_{X24e} : y^2 = x^3 - (27t^4 + 27t^2 + 27)x + (54t^6 + 81t^4 - 81t^2 - 54),$$

con j-invariante igual a $j_{E_{X24e}}(t) = \dfrac{(t^4 + t^2 + 1)^3}{t^4(t^2 + 1)^2}$.

La curva modular X_{24e} es de género 0, y podemos parametrizar las curvas elípticas como una familia sobre $\mathbb{Q}(t)$:

$$E_{X24e} : y^2 = x^3 - (27t^4 + 27t^2 + 27)x + (54t^6 + 81t^4 - 81t^2 - 54),$$

con j-invariante igual a $j_{E_{X24e}}(t) = \dfrac{(t^4 + t^2 + 1)^3}{t^4(t^2 + 1)^2}$.

Segundo, parametrizamos las curvas con una 3-isogenia.

La curva modular X_{24e} es de género 0, y podemos parametrizar las curvas elípticas como una familia sobre $\mathbb{Q}(t)$:

$$E_{X24e} : y^2 = x^3 - (27t^4 + 27t^2 + 27)x + (54t^6 + 81t^4 - 81t^2 - 54),$$

con j-invariante igual a $j_{E_{X24e}}(t) = \dfrac{(t^4 + t^2 + 1)^3}{t^4(t^2 + 1)^2}$.

Segundo, parametrizamos las curvas con una 3-isogenia. Estas vienen parametrizadas por la curva modular $X_0(3)$, y son curvas con j-invariante dado por

$$j(s) = \frac{(s + 27)(s + 243)^3}{s^3}.$$

La curva modular X_{24e} es de género 0, y podemos parametrizar las curvas elípticas como una familia sobre $\mathbb{Q}(t)$:

$$E_{X24e} : y^2 = x^3 - (27t^4 + 27t^2 + 27)x + (54t^6 + 81t^4 - 81t^2 - 54),$$

con j-invariante igual a $j_{E_{X24e}}(t) = \dfrac{(t^4 + t^2 + 1)^3}{t^4(t^2 + 1)^2}$.

Segundo, parametrizamos las curvas con una 3-isogenia. Estas vienen parametrizadas por la curva modular $X_0(3)$, y son curvas con j-invariante dado por

$$j(s) = \frac{(s + 27)(s + 243)^3}{s^3}.$$

Por tanto, existen números racionales s y t ($\neq 0$) tales que

$$\frac{(t^4 + t^2 + 1)^3}{t^4(t^2 + 1)^2} = \frac{(s + 27)(s + 243)^3}{s^3}.$$

Definamos una curva:

$$C : (t^4 + t^2 + 1)^3 s^3 - t^4 (t^2 + 1)^2 (s + 27)(s + 243)^3 = 0$$

...

Definamos una curva:

$$C : (t^4 + t^2 + 1)^3 s^3 - t^4 (t^2 + 1)^2 (s + 27)(s + 243)^3 = 0$$

... y Magma nos dice que tiene género 13!

Definamos una curva:

$$C : (t^4 + t^2 + 1)^3 s^3 - t^4 (t^2 + 1)^2 (s + 27)(s + 243)^3 = 0$$

... y Magma nos dice que tiene género 13!

Si en vez definimos

$$C' : (t^2 + t + 1)^3 s^3 - t^2 (t + 1)^2 (s + 27)(s + 243)^3 = 0$$

entonces hay una función $\phi \colon C \to C'$ tal que $(s, t) \mapsto (s, t^2)$. La curva C' es de género 6.

Definamos una curva:

$$C : (t^4 + t^2 + 1)^3 s^3 - t^4 (t^2 + 1)^2 (s + 27)(s + 243)^3 = 0$$

... y Magma nos dice que tiene género 13!

Si en vez definimos

$$C' : (t^2 + t + 1)^3 s^3 - t^2 (t + 1)^2 (s + 27)(s + 243)^3 = 0$$

entonces hay una función $\phi \colon C \to C'$ tal que $(s, t) \mapsto (s, t^2)$. La curva C' es de género 6.

La curva C' tiene un automorfismo

$$\psi \colon (t, s, z) \mapsto (-tz - z^2, ts, tz),$$

Definamos una curva:

$$C : (t^4 + t^2 + 1)^3 s^3 - t^4 (t^2 + 1)^2 (s + 27)(s + 243)^3 = 0$$

... y Magma nos dice que tiene género 13!

Si en vez definimos

$$C' : (t^2 + t + 1)^3 s^3 - t^2 (t + 1)^2 (s + 27)(s + 243)^3 = 0$$

entonces hay una función $\phi \colon C \to C'$ tal que $(s, t) \mapsto (s, t^2)$. La curva C' es de género 6.

La curva C' tiene un automorfismo

$$\psi \colon (t, s, z) \mapsto (-tz - z^2, ts, tz),$$

y la curva cociente $C'' = C'/\langle \psi \rangle$ tiene género 2, con ecuación:

$$C'' : y^2 + x^2 y = -x^5 - x^4 + 4x^3 - 2x^2 - 9x + 2.$$

$$C : (t^4 + t^2 + 1)^3 s^3 - t^4 (t^2 + 1)^2 (s + 27)(s + 243)^3 = 0$$

$$C' : (t^2 + t + 1)^3 s^3 - t^2 (t + 1)^2 (s + 27)(s + 243)^3 = 0$$

$$C'' : y^2 + x^2 y = -x^5 - x^4 + 4x^3 - 2x^2 - 9x + 2.$$

$$C : (t^4 + t^2 + 1)^3 s^3 - t^4 (t^2 + 1)^2 (s + 27)(s + 243)^3 = 0$$

$$C' : (t^2 + t + 1)^3 s^3 - t^2 (t + 1)^2 (s + 27)(s + 243)^3 = 0$$

$$C'' : y^2 + x^2 y = -x^5 - x^4 + 4x^3 - 2x^2 - 9x + 2.$$

Un descenso demuestra que la variedad jacobiana $J(C'')/\mathbb{Q}$ es de rango 0, y por tanto podemos usar el método de Chabauty para calcular los puntos racionales de C''.

$$C : (t^4 + t^2 + 1)^3 s^3 - t^4 (t^2 + 1)^2 (s + 27)(s + 243)^3 = 0$$

$$C' : (t^2 + t + 1)^3 s^3 - t^2 (t + 1)^2 (s + 27)(s + 243)^3 = 0$$

$$C'' : y^2 + x^2 y = -x^5 - x^4 + 4x^3 - 2x^2 - 9x + 2.$$

Un descenso demuestra que la variedad jacobiana $J(C'')/\mathbb{Q}$ es de rango 0, y por tanto podemos usar el método de Chabauty para calcular los puntos racionales de C''. Estos son $[-2, -2, 1]$ and $[1, 0, 0]$ en coordenadas proyectivas.

$$C : (t^4 + t^2 + 1)^3 s^3 - t^4 (t^2 + 1)^2 (s + 27)(s + 243)^3 = 0$$

$$C' : (t^2 + t + 1)^3 s^3 - t^2 (t + 1)^2 (s + 27)(s + 243)^3 = 0$$

$$C'' : y^2 + x^2 y = -x^5 - x^4 + 4x^3 - 2x^2 - 9x + 2.$$

Un descenso demuestra que la variedad jacobiana $J(C'')/\mathbb{Q}$ es de rango 0, y por tanto podemos usar el método de Chabauty para calcular los puntos racionales de C''. Estos son $[-2, -2, 1]$ and $[1, 0, 0]$ en coordenadas proyectivas.

A través de la función $C' \to C'/\langle\psi\rangle = C''$ obtenemos los puntos racionales de C':

$$[t, s, z] \in \{[-1, 0, 1], [0, 0, 1], [0, 1, 0], [1, 0, 0]\}.$$

$$C : (t^4 + t^2 + 1)^3 s^3 - t^4 (t^2 + 1)^2 (s + 27)(s + 243)^3 = 0$$

$$C' : (t^2 + t + 1)^3 s^3 - t^2 (t + 1)^2 (s + 27)(s + 243)^3 = 0$$

$$C'' : y^2 + x^2 y = -x^5 - x^4 + 4x^3 - 2x^2 - 9x + 2.$$

Un descenso demuestra que la variedad jacobiana $J(C'')/\mathbb{Q}$ es de rango 0, y por tanto podemos usar el método de Chabauty para calcular los puntos racionales de C''. Estos son $[-2, -2, 1]$ and $[1, 0, 0]$ en coordenadas proyectivas.

A través de la función $C' \to C'/\langle\psi\rangle = C''$ obtenemos los puntos racionales de C':

$$[t, s, z] \in \{[-1, 0, 1], [0, 0, 1], [0, 1, 0], [1, 0, 0]\}.$$

Todos estos puntos tienen $t = 0$ ó $s = 0$, y por lo tanto corresponden a cúspides de la curva C.

$$C : (t^4 + t^2 + 1)^3 s^3 - t^4 (t^2 + 1)^2 (s + 27)(s + 243)^3 = 0$$

$$C' : (t^2 + t + 1)^3 s^3 - t^2 (t + 1)^2 (s + 27)(s + 243)^3 = 0$$

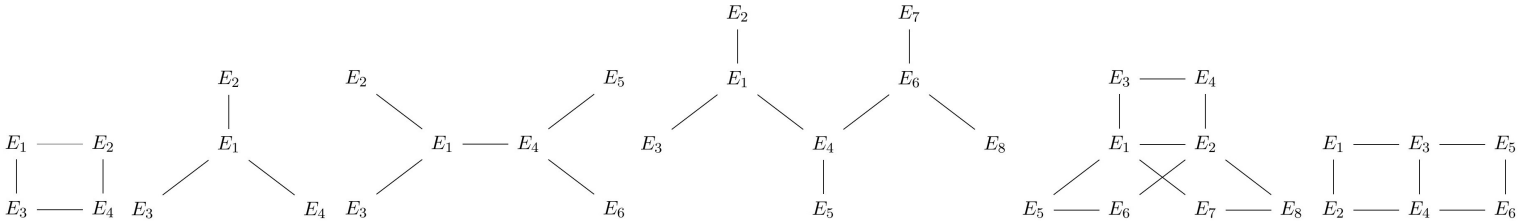
$$C'' : y^2 + x^2 y = -x^5 - x^4 + 4x^3 - 2x^2 - 9x + 2.$$

Un descenso demuestra que la variedad jacobiana $J(C'')/\mathbb{Q}$ es de rango 0, y por tanto podemos usar el método de Chabauty para calcular los puntos racionales de C''. Estos son $[-2, -2, 1]$ and $[1, 0, 0]$ en coordenadas proyectivas.

A través de la función $C' \to C'/\langle\psi\rangle = C''$ obtenemos los puntos racionales de C':

$$[t, s, z] \in \{[-1, 0, 1], [0, 0, 1], [0, 1, 0], [1, 0, 0]\}.$$

Todos estos puntos tienen $t = 0$ ó $s = 0$, y por lo tanto corresponden a cúspides de la curva C. **Esto demuestra que las configuraciones de tipo S que buscabamos no existen** (sobre $\mathbb{Q}$!).



GRACIAS

alvaro.lozano-robledo@uconn.edu

"Si por casualidad he omitido algo
más o menos apropiado o necesario,
Le ruego perdón,
ya que no hay nadie sin culpa
ni circunspecto en todos los asuntos."

Leonardo Pisano (Fibonacci), *Liber Abaci*.