Crecimiento del subgrupo de torsión de curvas elípticas

Enrique González Jiménez

enrique.gonzalez.jimenez@uam.es

Seminario Latinoamericano de Teoría de Números

online

20 mayo 2021

Introduction

Let K be a number Field. An elliptic curve over K is:

$$E : Y^2 = X^3 + AX + B, \qquad A, B \in K$$

with $\Delta_E = -16(4A^3 - 27B^2) \neq 0$.

$$E(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

$$\mathcal{O} = [0 : 1 : 0]$$

$$E(K)?$$

Introduction

Let K be a number Field. An elliptic curve over K is:

$$E : Y^2 = X^3 + AX + B, \qquad A, B \in K$$

with $\Delta_E = -16(4A^3 - 27B^2) \neq 0$.

$$E(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

$$\mathcal{O} = [0 : 1 : 0]$$

Mordell-Weil:

$$E(K) = E(K)_{\text{tors}} \bigoplus \mathbb{Z}^r$$

Torsion

$$E(K)_{\text{tors}}?$$

Torsion

$$E(K)_{\text{tors}} = \begin{cases} \mathbb{Z}/n\mathbb{Z} & \overset{\text{notation}}{\longleftrightarrow} \quad (n) \\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \overset{\text{notation}}{\longleftrightarrow} \quad (n,m), \quad n|m \end{cases}$$

$$S(d) = \left\{ p \text{ prime} \ : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists E_{/K} \text{ elliptic curve} \end{array} , \quad p \,|\, \#E(K)_{\text{tors}} \right\}$$

$$\Phi(d) = \left\{ \quad G \quad : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists E_{/K} \text{ elliptic curve} \end{array} , \quad E(K)_{\text{tors}} = G \right\}_{/\sim}$$

$$\Phi^{\infty}(d) = \left\{ \quad G \quad : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists \infty\, E_{/K} \text{ elliptic curve} \end{array} , \quad E(K)_{\text{tors}} = G \right\}_{/\sim}$$

Torsion

$$S(d) = \left\{ p \text{ prime} \ : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists E_{/K} \text{ elliptic curve} \end{array} , \ p \,|\, \#E(K)_{\text{tors}} \right\}$$

$$\Phi(d) = \left\{ G \ : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists E_{/K} \text{ elliptic curve} \end{array} , \ E(K)_{\text{tors}} = G \right\}_{/\sim}$$

$$\Phi^{\infty}(d) = \left\{ G \ : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists\, \infty\, E_{/K} \text{ elliptic curve} \end{array} , \ E(K)_{\text{tors}} = G \right\}_{/\sim}$$

$$\Phi^{\infty}(d) \subseteq \Phi(d)$$

Torsion

$$S(d) = \left\{ p \text{ prime} \ : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists E_{/K} \text{ elliptic curve} \end{array} , \ p \,|\, \#E(K)_{\text{tors}} \right\}$$

$$\Phi(d) = \left\{ \quad G \quad : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists E_{/K} \text{ elliptic curve} \end{array} , \ E(K)_{\text{tors}} = G \right\}_{/\sim}$$

$$\Phi^{\infty}(d) = \left\{ \ G \ : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists\, \infty\, E_{/K} \text{ elliptic curve} \end{array} , \ E(K)_{\text{tors}} = G \right\}_{/\sim}$$

Merel (1996)

$E_{/K}$ elliptic curve, $[K:\mathbb{Q}] = d$. Then $\exists\, B(d) \in \mathbb{Z}$ such that $\#E(K)_{\text{tors}} < B(d)$.

Torsion

$$S(d) = \left\{ p \text{ prime} \ : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists E_{/K} \text{ elliptic curve} \end{array} , \ p \,|\, \#E(K)_{\text{tors}} \right\}$$

$$\Phi(d) = \left\{ \quad G \quad : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists E_{/K} \text{ elliptic curve} \end{array} , \ E(K)_{\text{tors}} = G \right\}_{/\sim}$$

$$\Phi^{\infty}(d) = \left\{ \ G \ : \ \begin{array}{l} \exists K,\, [K:\mathbb{Q}] = d \\ \exists\, \infty\, E_{/K} \text{ elliptic curve} \end{array} , \ E(K)_{\text{tors}} = G \right\}_{/\sim}$$

$$\#\Phi(d) < \infty$$

Torsion over $\mathbb{Q}$

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

Torsion over $\mathbb{Q}$

Mazur (1977):

$$S(1) = \{2, 3, 5, 7\}$$

$$\Phi(1) = \left\{ \begin{array}{ll} (n), & n = 1, \ldots, 10, 12 \\ (2, 2m), & m = 1, 2, 3, 4 \end{array} \right\}$$

$$\Phi^{\infty}(1) = \Phi(1)$$

Torsion over quadratic fields

$$E(K)_{\text{tors}}\ , \quad [K:\mathbb{Q}] = 2?$$

Torsion over quadratic fields

Kamienny (1992), Kenku, Momose (1988))

$$S(2) = \{2, 3, 5, 7, 11, 13\}$$

$$\Phi(2) = \left\{ \begin{array}{ll} (n)\,, & n = 1, \ldots, 11, 12, 13, 14, 15, 16, 18 \\ (2, 2m)\,, & m = 1, 2, 3, 4, 5, 6 \\ (3, 3r)\,, & r = 1, 2 \\ (4, 4) & \end{array} \right\}$$

$$\Phi^{\infty}(2) = \Phi(2)$$

Torsion over cubic fields

$$E(K)_{\text{tors}}\ , \quad [K:\mathbb{Q}]=3?$$

Torsion over cubic fields

Parent (2003)

$$S(3) = \{2, 3, 5, 7, 11, 13\}$$

Jeon, Kim, Schweizer (2004)

$$\Phi^{\infty}(3) = \left\{ \begin{array}{ll} (n), & n = 1, \ldots, 16, 18, 20 \\ (2, 2m), & m = 1, \ldots, 7 \end{array} \right\}$$

Najman (2012)

$$(21) \in \Phi(3) \setminus \Phi^{\infty}(3)$$

Torsion over cubic fields

Parent (2003)

$$S(3) = \{2, 3, 5, 7, 11, 13\}$$

Jeon, Kim, Schweizer (2004)

$$\Phi^{\infty}(3) = \left\{ \begin{array}{ll} (n), & n = 1, \ldots, 16, 18, 20 \\ (2, 2m), & m = 1, \ldots, 7 \end{array} \right\}$$

Najman (2012)

$$E : y^2 + xy + y = x^3 - x^2 - 5x + 5,$$
$$K = \mathbb{Q}(\zeta_9)^+, \ E(K)_{\text{tors}} = (21)$$

Torsion over cubic fields

Parent (2003)

$$S(3) = \{2, 3, 5, 7, 11, 13\}$$

Jeon, Kim, Schweizer (2004)

$$\Phi^{\infty}(3) = \left\{ \begin{array}{ll} (n), & n = 1, \ldots, 16, 18, 20 \\ (2, 2m), & m = 1, \ldots, 7 \end{array} \right\}$$

Najman (2012)

$$E = \texttt{162b1},\ K = \mathbb{Q}(\zeta_9)^+,\ E(K)_{\text{tors}} = (21)$$

Torsion over cubic fields

Parent (2003)

$$S(3) = \{2, 3, 5, 7, 11, 13\}$$

Derickx, Etropolski, van Hoeij, Morrow, Zureick-Brown (2017)

$$\Phi(3) = \left\{ \begin{array}{ll} (n), & n = 1, \ldots, 16, 18, 20, 21 \\ (2, 2m), & m = 1, \ldots, 7 \end{array} \right\}$$

Torsion over cubic fields

Parent (2003)

$$S(3) = \{2, 3, 5, 7, 11, 13\}$$

Derickx, Etropolski, van Hoeij, Morrow, Zureick-Brown (2021)

$$\Phi(3) = \left\{ \begin{array}{ll} (n), & n = 1, \ldots, 16, 18, 20, 21 \\ (2, 2m), & m = 1, \ldots, 7 \end{array} \right\}$$

Torsion over quartic fields

$$E(K)_{\text{tors}}\ , \quad [K:\mathbb{Q}] = 4?$$

Torsion over quartic fields

Kamienny, Stein, Stoll (2010)

$$S(4) = \{2, 3, 5, 7, 11, 13, 17\}$$

Jeon, Kim, Park (2006)

$$\Phi^{\infty}(4) = \left\{ \begin{array}{ll} (n)\,, & n = 1, \ldots, 18, 20, 21, 22, 24 \\ (2, 2m)\,, & m = 1, \ldots, 9 \\ (3, 3r)\,, & r = 1, 2, 3 \\ (4, 4s)\,, & s = 1, 2 \\ (5, 5) & \\ (6, 6) & \end{array} \right\}$$

$\Phi(4)$?

$\Phi^{\infty}(4) \subsetneq \Phi(4)$?

Torsion over number fields

$$E(K)_{\text{tors}}\ , \quad [K:\mathbb{Q}] = d\text{?}$$

Torsion over number fields

Derickx, Kamienny, Stein, Stoll (2017)

$$S(5) = \{2, 3, 5, 7, 11, 13, 17, 19\}$$
$$S(6) = \{2, 3, 5, 7, 11, 13, 17, 19, 37\}$$

Derickx, Sutherland (2017)

$$\Phi^{\infty}(5) = \left\{ \begin{array}{ll} (n), & n = 1, \ldots, 25,\ n \neq 23 \\ (2, 2m), & m = 1, \ldots, 8 \end{array} \right\}$$

$$\Phi^{\infty}(6) = \left\{ \begin{array}{ll} (n), & n = 1, \ldots, 30,\ n \neq 23, 25, 29 \\ (2, 2m), & m = 1, \ldots, 10 \\ (3, 3r), & r = 1, \ldots, 4 \\ (4, 4s), & s = 1, 2 \\ (6, 6) & \end{array} \right\}$$

$$\Phi^{\infty}(d) \subsetneq \Phi(d), \qquad d = 5, 6$$

Torsion over number fields

Derickx, Kamienny, Stein, Stoll (2021)

$$S(5) = \{2, 3, 5, 7, 11, 13, 17, 19\}$$
$$S(6) = \{2, 3, 5, 7, 11, 13, 17, 19, 37\}$$
$$S(7) = \{2, 3, 5, 7, 11, 13, 17, 19, 23\}$$

Torsion over number fields

$$S(d)?\,, \quad d > 6$$

$$\Phi^{\infty}(d)?\,, \quad d > 6$$

$$\Phi(d)?\,, \quad d > 3$$

Growth of torsion upon base change

$$E_{/K}\ , \quad L/K\ , \quad E(L)_{\text{tors}}?$$

We say that there is **torsion growth from** L **to** K if

$$E(K)_{\text{tors}} \subsetneq E(L)_{\text{tors}}$$

Growth of torsion upon base change

$$E_{/\mathbb{Q}}\,, \quad K/\mathbb{Q}\,, \quad E(K)_{\text{tors}}?$$

We say that there is **torsion growth in** $K/\mathbb{Q}$ if

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

Growth of torsion upon base change

$$E_{/\mathbb{Q}}\ , \quad K/\mathbb{Q}\ , \quad E(K)_{\text{tors}}?$$

Problem:

INPUT : $E_{/\mathbb{Q}}$ an elliptic curve, $K/\mathbb{Q}$ number field

OUTPUT : $E(K)_{\text{tors}}$

Solution:

Nagel-Lutz algorithm

Example: 30a7

```
Magma V2.26-3     Thu May  20 2021 20:10:10 on luna
Type ? for help.  Type <Ctrl>-D to quit.
> E:=EllipticCurve("30a7");E;
Elliptic Curve defined by y^2 + x*y + y = x^3 - 5334*x - 150368
over Rational Field

> T:=TorsionSubgroup(E);
> AbelianInvariants(T);
[ 2 ]

> K:=QuadraticField(10);

> EK:=BaseChange(E,K);

> TK:=TorsionSubgroup(EK);
> AbelianInvariants(TK);
[ 2, 2 ]
```

Rational torsion over number fields

$$E_{/\mathbb{Q}}\ , \quad E(K)_{\text{tors}}\ , \quad [K:\mathbb{Q}]=d\,?$$

Problem:

INPUT : $E_{/\mathbb{Q}}$ an elliptic curve

OUTPUT : $E(K)_{\text{tors}}$ for all $K/\mathbb{Q}$ number field, $[K:\mathbb{Q}]=d$

$$\Phi_{\mathbb{Q}}(d,E)=\{H\,:\,\exists K/\mathbb{Q},\,[K:\mathbb{Q}]=d\,,\,E(K)_{\text{tors}}=H\,\}_{/\sim}$$

$$S_{\mathbb{Q}}(d,E)=\{p \text{ prime}\,:\,\exists K\,,\ [K:\mathbb{Q}]=d,\quad p\,|\,\#E(K)_{\text{tors}}\}$$

Rational torsion over number fields

$$\text{All } E_{/\mathbb{Q}}\ , \quad E(K)_{\text{tors}}\ , \quad [K:\mathbb{Q}]=d\text{?}$$

$$\Phi_{\mathbb{Q}}(d)=\left\{ G\ :\ \begin{array}{l}\exists E_{/\mathbb{Q}} \text{ elliptic curve}\\ \exists K,\ [K:\mathbb{Q}]=d\end{array}\ ,\ E(K)_{\text{tors}}=G \right\}_{/\sim}$$

$$S_{\mathbb{Q}}(d)=\left\{ p \text{ prime}\ :\ \begin{array}{l}\exists E_{/\mathbb{Q}} \text{ elliptic curve}\\ \exists K,\ [K:\mathbb{Q}]=d\end{array}\ ,\ p \mid \#E(K)_{\text{tors}} \right\}$$

Rational torsion over number fields

$$\text{All } E_{/\mathbb{Q}} \ , \quad E(K)_{\text{tors}} \ , \quad [K : \mathbb{Q}] = d \text{?}$$

$$\Phi_{\mathbb{Q}}(d) = \bigcup_{E/\mathbb{Q}} \Phi_{\mathbb{Q}}(d, E)$$

$$S_{\mathbb{Q}}(d) = \bigcup_{E/\mathbb{Q}} S_{\mathbb{Q}}(d, E)$$

Rational torsion over number fields

$$E_{/\mathbb{Q}}\ , \quad E(K)_{\text{tors}}\ , \quad [K:\mathbb{Q}]=d\text{?}$$

Problem:

INPUT : $E_{/\mathbb{Q}}$ an elliptic curve

OUTPUT : $E(K)_{\text{tors}}$ for all $K/\mathbb{Q}$ number field, $[K:\mathbb{Q}]=d$

Solution:

Division polynomials + $\Phi_{\mathbb{Q}}(d,E)$ or $S_{\mathbb{Q}}(d,E)$

Rational torsion over number fields

$$E_{/\mathbb{Q}}\ , \quad E(K)_{\text{tors}}\ , \quad [K:\mathbb{Q}]=d\text{?}$$

Problem:

INPUT : $E_{/\mathbb{Q}}$ an elliptic curve

OUTPUT : $E(K)_{\text{tors}}$ for all $K/\mathbb{Q}$ number field, $[K:\mathbb{Q}]=d$

Solution:

Division polynomials + $\Phi_{\mathbb{Q}}(d)$ or $S_{\mathbb{Q}}(d)$

Rational torsion over number fields

$$S_{\mathbb{Q}}(d)?$$

Lozano-Robledo (2013)

$$\bigcup_{k \leq d} S_{\mathbb{Q}}(k)\,, \qquad d \leq 21$$

For example:
$S_{\mathbb{Q}}(2) = \{2, 3, 5, 7\}$
$S_{\mathbb{Q}}(3) = \{2, 3, 5, 7, 13\}$

Goal 1

$$S_{\mathbb{Q}}(d)$$

Rational torsion over number fields

$$\Phi_{\mathbb{Q}}(d)?$$

$$\Phi(2) = \left\{ \begin{array}{ll} (n)\,, & n = 1, \ldots, 10, 11, 12, 13, 14, 15, 16, 18 \\ (2, 2m)\,, & m = 1, 2, 3, 4, 5, 6 \\ (3, 3r)\,, & r = 1, 2 \\ (4, 4) & \end{array} \right\}$$

$$\Phi(3) = \left\{ \begin{array}{ll} (n)\,, & n = 1, \ldots, 10, 11, 12, 13, 14, 15, 16, 18, 20, 21 \\ (2, 2m)\,, & m = 1, 2, 3, 4, 5, 6, 7 \end{array} \right\}$$

Rational torsion over number fields

$$\Phi_{\mathbb{Q}}(d)?$$

$$\Phi(2) = \left\{ \begin{array}{ll} (n)\,, & n = 1,\ldots,10,11,12,13,14,15,16,18 \\ (2,2m)\,, & m = 1,2,3,4,5,6 \\ (3,3r)\,, & r = 1,2 \\ (4,4) & \end{array} \right\}$$

$$\Phi(3) = \left\{ \begin{array}{ll} (n)\,, & n = 1,\ldots,10,11,12,13,14,15,16,18,20,21 \\ (2,2m)\,, & m = 1,2,3,4,5,6,7 \end{array} \right\}$$

Rational torsion over number fields

$$\Phi_{\mathbb{Q}}(d)?$$

Najman (2012)

$$\Phi_{\mathbb{Q}}(2) = \left\{ \begin{array}{ll} (n)\,, & n = 1, \ldots, 10, 12, 15, 16, 18 \\ (2, 2m)\,, & m = 1, 2, 3, 4, 5, 6 \\ (3, 3r)\,, & r = 1, 2 \\ (4, 4) & \end{array} \right\}$$

$$\Phi_{\mathbb{Q}}(3) = \left\{ \begin{array}{ll} (n)\,, & n = 1, \ldots, 10, 12, 13, 14, 18, 21 \\ (2, 2m)\,, & m = 1, 2, 3, 4, 7 \end{array} \right\}$$

$$(21) \in \Phi(3) \setminus \Phi^{\infty}(3), \qquad (21) \in \Phi_{\mathbb{Q}}(3)$$

Rational torsion over number fields

$$\Phi_{\mathbb{Q}}(d)?$$

Goal 2

$$\Phi_{\mathbb{Q}}(d)\,, \quad d > 3$$

On the division polynomials

$$E : y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Q}$$

$$\begin{aligned}
&\psi_1 = 1,\\
&\psi_2 = x^3 + ax + b\\
&\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,\\
&\psi_4 = (2x^6 + 10ax^4 + 40bx^3 - 10a^2x^2 - 8bax - 2a^3 - 16b^2)\Psi_2\\
&\psi_{2k+1} = \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3, \ k \geq 2\\
&\psi_{2k} = \psi_k(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2)/\psi_2, \ k \geq 2.
\end{aligned}$$

$$\Psi_2 = \psi_2 \quad , \quad \Psi_m = \begin{cases} \psi_m & m \text{ odd} \\ \psi_m/\psi_2 & m \text{ even.} \end{cases}$$

- $\Psi_m \in \mathbb{Q}[x]$.
- $P \in E[m]$ if and only if $\Psi_m(x(P)) = 0$.
- $P \in E(K)[m]$ if and only if $\Psi_m(x(P)) = 0$ and $P \in E(K)$.

Example: $\Phi_{\mathbb{Q}}(2, 30a7)$

$$E : y^2 + xy + y = x^3 - 5334x - 150368 \qquad E(\mathbb{Q})_{\text{tors}} = (2)$$

[1] Weierstrass Model: $E : y^2 = x^3 - 6912243x - 6994821042$
[2] Factorization of Ψ_m for $m \in \{2, 3, 4, 8, 5, 12, 16\}$:

m=3

$$\begin{aligned} \Psi_3 &= 3x^4 - 41473458x^2 - 83937852504x - 47779103291049 \\ &= 3(x + 1521)(x^3 - 1521x^2 - 11511045x - 10470984723) \end{aligned}$$

$$(-1521)^3 - 6912243(-1521) - 6994821042 = -2^6 3^3 5^2 = -3\square$$

$$E(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} = (6)$$

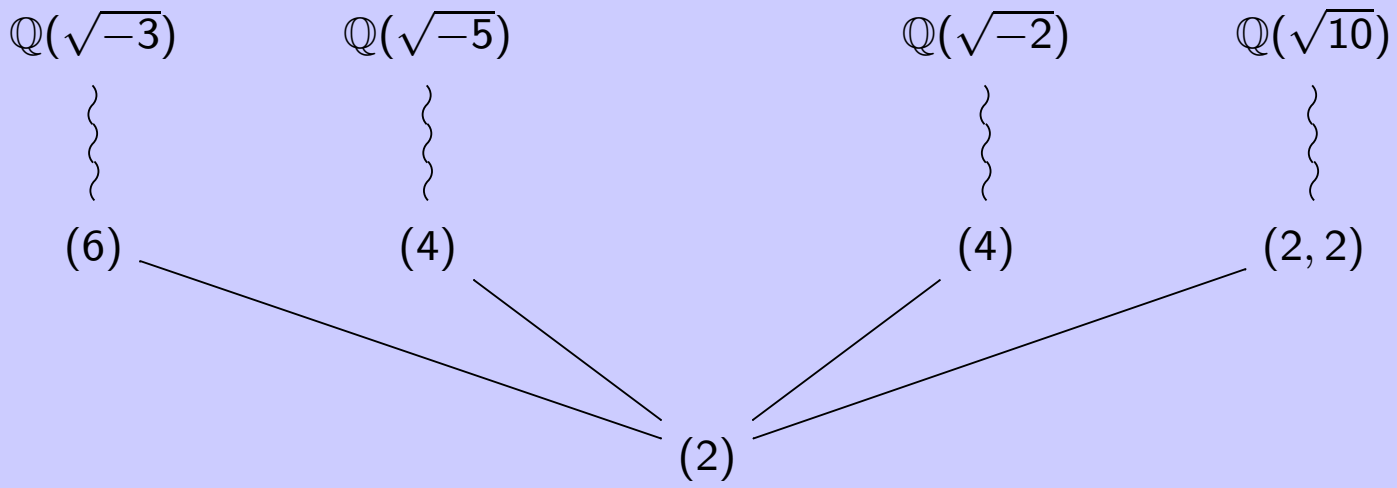
Example: $\Phi_{\mathbb{Q}}(2, 30a7)$

$$E : y^2 + xy + y = x^3 - 5334x - 150368$$

$$E(\mathbb{Q})_{\text{tors}} = (2)$$

$$E(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} = (6) \qquad E(\mathbb{Q}(\sqrt{-5}))_{\text{tors}} = (4)$$

$$E(\mathbb{Q}(\sqrt{10}))_{\text{tors}} = (2,2) \qquad E(\mathbb{Q}(\sqrt{-2}))_{\text{tors}} = (4)$$



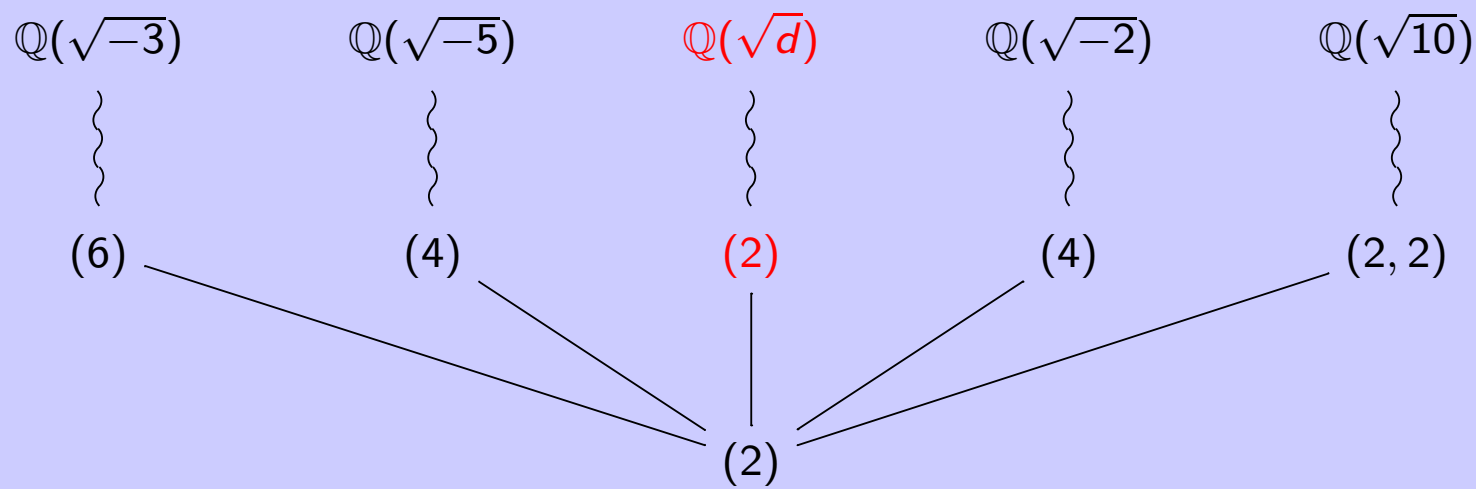
Example: $\Phi_{\mathbb{Q}}(2, 30a7)$

$$E : y^2 + xy + y = x^3 - 5334x - 150368$$

$$E(\mathbb{Q})_{\text{tors}} = (2)$$

$$E(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} = (6) \qquad E(\mathbb{Q}(\sqrt{-5}))_{\text{tors}} = (4)$$

$$E(\mathbb{Q}(\sqrt{10}))_{\text{tors}} = (2,2) \qquad E(\mathbb{Q}(\sqrt{-2}))_{\text{tors}} = (4)$$



Growth of torsion upon base change

$G \in \Phi(1)$

$$E_{/\mathbb{Q}} \ , \quad E(\mathbb{Q})_{\text{tors}} = G \ , \quad E(K)_{\text{tors}} \ , \quad [K : \mathbb{Q}] = d \text{?}$$

$G \in \Phi(1)$

$$\Phi_{\mathbb{Q}}(d,G) = \left\{ H : \begin{array}{ll} \exists E_{/\mathbb{Q}} \text{ elliptic curve}, & E(\mathbb{Q})_{\text{tors}} = G \\ \exists K,\ [K:\mathbb{Q}] = d, & E(K)_{\text{tors}} = H \end{array} \right\}_{/\sim}$$

$$\Phi_{\mathbb{Q}}(d,G) = \bigcup_{E(\mathbb{Q})_{\text{tors}} = G} \Phi_{\mathbb{Q}}(d,E)$$

Goal 3

$$\Phi_{\mathbb{Q}}(d,G)$$

Torsion configurations

We say that the torsion growth in K is **primitive** if

$$E(K')_{\text{tors}} \subsetneq E(K)_{\text{tors}} \qquad \text{for all subfields } K \subsetneq K.$$

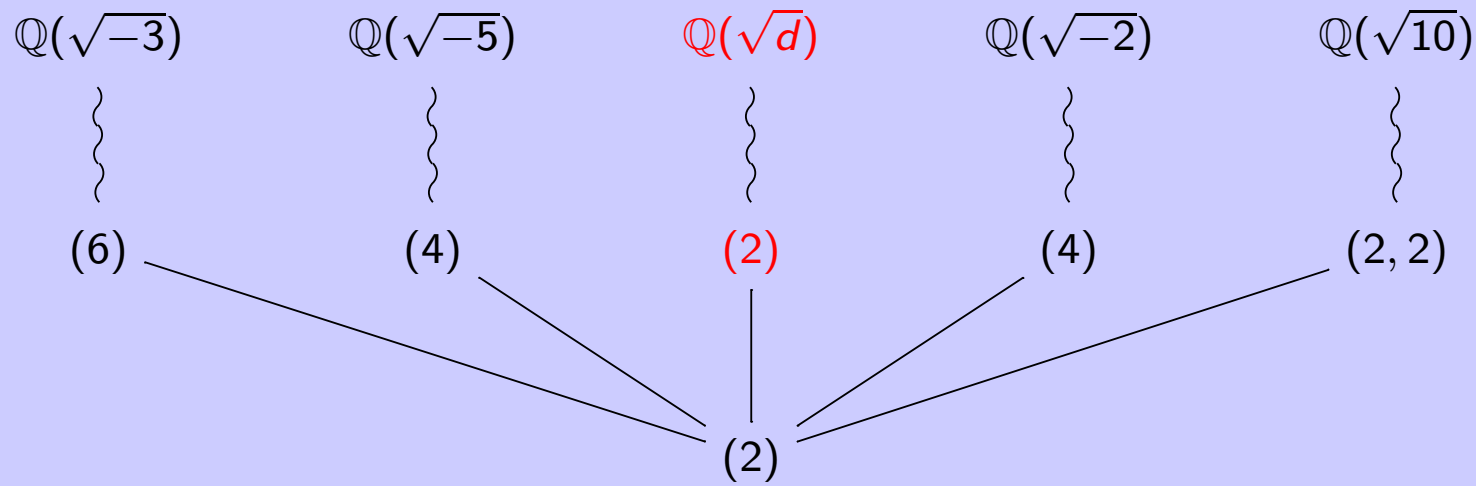
Given $E_{/\mathbb{Q}}$ and d,
how many primitive degree d extension can appear?

Torsion configurations

Given $E_{/\mathbb{Q}}$ and d,
how many primitive degree d extension can appear?

$$\mathcal{H}_{\mathbb{Q}}(d, E) = \left\{ H \ : \ \begin{array}{l} \exists K/\mathbb{Q} \text{ primitive}, \quad [K : \mathbb{Q}] \mid d \, , \\ E(K)_{\text{tors}} = H \neq E(\mathbb{Q})_{\text{tors}} \end{array} \right\}$$

Example: 30a7



$$\Phi_{\mathbb{Q}}(2, 30a7) = \{(2), (4), (6), (2, 2)\}$$

$$\mathcal{H}_{\mathbb{Q}}(2, 30a7) = \{(4), (4), (6), (2, 2)\}$$

Torsion configurations

$$\mathcal{H}_{\mathbb{Q}}(d, E) = \left\{ H : \begin{array}{l} \exists K/\mathbb{Q} \text{ primitive} \quad [K:\mathbb{Q}] \mid d \\ E(K)_{\text{tors}} = H \neq E(\mathbb{Q})_{\text{tors}} \end{array} \right\}$$

$G \in \Phi(1)$:

$$\mathcal{H}_{\mathbb{Q}}(d, G) = \bigcup_{E(\mathbb{Q})_{\text{tors}} = G} \mathcal{H}_{\mathbb{Q}}(d, E)$$

$$\mathcal{H}_{\mathbb{Q}}(d) = \bigcup_{G \in \Phi(1)} \mathcal{H}_{\mathbb{Q}}(d, G)$$

$$h_{\mathbb{Q}}(d) = \max \{ \#S \mid S \in \mathcal{H}_{\mathbb{Q}}(d) \}$$

Goal 4 $\mathcal{H}_{\mathbb{Q}}(d) = \left\{ H : \begin{array}{l} \exists K/\mathbb{Q} \text{ primitive}, \quad [K:\mathbb{Q}] \mid d \\ \exists E(K)_{\text{tors}} = H \neq E(\mathbb{Q})_{\text{tors}} \end{array} \right\}$

Goals:

Goal 1

$$S_{\mathbb{Q}}(d) = \left\{ p \text{ prime} : \begin{array}{l} \exists E_{/\mathbb{Q}} \text{ elliptic curve} \\ \exists K,\ [K:\mathbb{Q}] = d \end{array} ,\ p \mid \#E(K)_{\text{tors}} \right\}$$

Goal 2

$$\Phi_{\mathbb{Q}}(d) = \left\{ G : \begin{array}{l} \exists E_{/\mathbb{Q}} \text{ elliptic curve} \\ \exists K,\ [K:\mathbb{Q}] = d \end{array} ,\ E(K)_{\text{tors}} = G \right\}_{/\sim}$$

Goal 3

$$\Phi_{\mathbb{Q}}(d, G) = \left\{ H : \begin{array}{ll} \exists E_{/\mathbb{Q}} \text{ elliptic curve}, & E(\mathbb{Q})_{\text{tors}} = G \\ \exists K,\ [K:\mathbb{Q}] = d, & E(K)_{\text{tors}} = H \end{array} \right\}_{/\sim}$$

Goal 4

$$\mathcal{H}_{\mathbb{Q}}(d) = \left\{ H : \begin{array}{ll} \exists K/\mathbb{Q} \text{ primitive}, & [K:\mathbb{Q}] \mid d \\ \exists E(K)_{\text{tors}} = H \neq E(\mathbb{Q})_{\text{tors}} & \end{array} \right\}$$

E.-Tornero (2014)

$d = 2$

G	$\Phi_{\mathbb{Q}}(2, G) \setminus \{G\}$
(1)	$\{(3), (5), (7), (9)\}$
(2)	$\{(4), (6), (8), (10), (12), (16), (2,2), (2,6), (2,10)\}$
(3)	$\{(15), (3,3)\}$
(4)	$\{(8), (12), (2,4), (2,8), (2,12), (4,4)\}$
(5)	$\{(15)\}$
(6)	$\{(12), (2,6), (3,6)\}$
(7)	$\{\}$
(8)	$\{(16), (2,8)\}$
(9)	$\{\}$
(10)	$\{(2,10)\}$
(12)	$\{(2,12)\}$
$(2,2)$	$\{(2,4), (2,6), (2,8), (2,12)\}$
$(2,4)$	$\{(2,8), (4,4)\}$
$(2,6)$	$\{(2,12)\}$
$(2,8)$	$\{\}$

E.-Tornero (2014)

$d = 2$

G	$\mathcal{H}_{\mathbb{Q}}(2, G)$
(1)	(3)
	(5)
	(7)
	(9)
	(3), (3)
	(3), (5)
(2)	(2, 2)
	(2, 6)
	(2, 10)
	(2, 2), (6)
	(2, 2), (10)
	(2, 6), (6)
	(2, 2), (4), (4)
	(2, 2), (6), (6)
	((2, 2), (8), (8)
	((2, 2), (4), (8)
	(2, 2), (4), (12)
	(2, 2), (4), (16)
	(2, 6), (4), (4)
	(2, 2), (4), (4), (6)

G	$\mathcal{H}_{\mathbb{Q}}(2, G)$
(3)	(15)
	(3, 3)
(4)	(2, 4)
	(2, 8)
	(2, 12)
	(4, 4)
	(2, 4), (12)
	(2, 4), (8), (8)
	(2, 8), (8), (8)
(5)	(15)
(6)	(2, 6)
	(2, 6), (3, 6)
	(2, 6), (12), (12)
(8)	(2, 8)
	(2, 8), (16), (16)
(10)	(2, 10)
(12)	(2, 12)

G	$\mathcal{H}_{\mathbb{Q}}(2, G)$
(2, 2)	(2, 4)
	(2, 6)
	(2, 8)
	(2, 12)
	(2, 4), (2, 4)
	(2, 4), (2, 6)
	(2, 4), (2, 8)
	(2, 4), (2, 4), (2, 4)
	(2, 4), (2, 4), (2, 8)
(2, 4)	(2, 8)
	(4, 4)
	(2, 8), (4, 4)
	(2, 8), (2, 8)
	(2, 8), (2, 8), (4, 4)
(2, 6)	(2, 12)

$$h_{\mathbb{Q}}(2) = 4$$

Najman (2013):

$$h_{\mathbb{Q}}(2) = 4$$


F. Najman.
The number of twists with large torsion of an elliptic curve.
Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM, **109** (2015), 535–547.

E.-Najman-Tornero (2016)

$d = 3$

G	$\Phi_{\mathbb{Q}}(3, G) \setminus \{G\}$
(1)	$\{(2), (3), (4), (6), (7), (13), (2,2), (2,14)\}$
(2)	$\{(6), (14)\}$
(3)	$\{(6), (9), (12), (21), (2,6)\}$
(4)	$\{(12)\}$
(5)	$\{(10)\}$
(6)	$\{(18)\}$
(7)	$\{(14)\}$
(8)	$\{()\}$
(9)	$\{(18)\}$
(10)	$\{\}$
(12)	$\{\}$
(2, 2)	$\{(2,6)\}$
(2, 4)	$\{\}$
(2, 6)	$\{\}$
(2, 8)	$\{\}$

E.-Najman-Tornero (2016)

$d = 3$

G	$\mathcal{H}_{\mathbb{Q}}(3, G)$
(1)	(2)
	(4)
	(6)
	(2, 2)
	(2, 14)
	(2), (3)
	(2), (7)
	(2), (13)
	(3), (4)
	(3), (2, 2)
	(4), (7)
	(7), (2, 2)
	(2), (3), (7)

G	$\mathcal{H}_{\mathbb{Q}}(3, G)$
(2)	(6)
	(14)
(3)	(6)
	(12)
	(2, 6)
	(6), (9)
	(6), (21)
(4)	(12)
(5)	(10)
(6)	(18)
(7)	(14)
(9)	(18)
(2, 2)	(2, 6)

$$h_{\mathbb{Q}}(3) = 3$$

Chou (2016), E.-Najman (2017)

$d = 4$

$$\Phi_{\mathbb{Q}}(4) = \left\{ \begin{array}{ll} (n)\,, & n = 1, \ldots, 10, 12, 13, 15, 16, 20, 24 \\ (2, 2m)\,, & m = 1, 2, 3, 4, 5, 6, 8 \\ (3, 3r)\,, & r = 1, 2 \\ (4, 4s)\,, & s = 1, 2 \\ (5, 5) & \\ (6, 6) & \end{array} \right\}$$

Remark: $K/\mathbb{Q}$ quartic
Chou: Galois case: $\mathrm{Gal}(K/\mathbb{Q}) = 4, V_4$
E.-Najman: $\mathrm{Gal}(K/\mathbb{Q}) = D_4, \mathbb{A}_4, \mathbb{S}_4$

E.-Lozano-Robledo (2017)

$d = 4$

G	$\Phi_{\mathbb{Q}}(4, G) \setminus \{G\}$
(1)	$\{(3), (5), (7), (9), (13), (15), (3,3), (5,5)\}$
(2)	$\{(4), (6), (8), (10), (12), (16), (20), (24), (2,2), (2,4), (2,6), (2,8), (2,10), (2,12), (2,16), (3,6), (4,4), (4,8), (6,6)\}$
(3)	$\{(15), (3,3)\}$
(4)	$\{(8), (12), (16), (24), (2,4), (2,8), (2,12), (2,16), (4,4), (4,8)\}$
(5)	$\{(15), (5,5)\}$
(6)	$\{(12), (24), (2,6), (2,12), (3,6), (6,6)\}$
(7)	$\{\}$
(8)	$\{(16), (2,8), (2,16), (4,8)\}$
(9)	$\{\}$
(10)	$\{(20), (2,10)\}$
(12)	$\{(24), (2,12)\}$
$(2,2)$	$\{(2,4), (2,6), (2,8), (2,12), (2,16), (4,4), (4,8)\}$
$(2,4)$	$\{(2,8), (2,16), (4,4), (4,8)\}$
$(2,6)$	$\{(2,12)\}$
$(2,8)$	$\{(2,8), (2,16), (4,8)\}$

E.-Lozano-Robledo (2017)

$d = 4$

G	$\mathcal{H}_{\mathbb{Q}}(4, E)$	E
(1)	(3)	19a2
	(5)	11a2
	(7)	208d1
	(9)	54a2
	(13)	2890d1
	$(3)^2$	121b1
	(3), (5)	50a2
	(3), (15)	50b3
	$(5)^2$	99d2
	(5), (5, 5)	275b2
	$(3)^2$, (5)	338d1
	(3), (5), (15)	50a4
	$(3)^2$, (3, 3)	175b2
(2)	(4), (2, 2)	46a1
	(4), (2, 6)	36a3
	(4), (2, 10)	450a3
	(2, 2), (2, 4)	200b1
	(4), (10), (2, 2)	66c3
	(4), (2, 2), (2, 4)	49a1
	(4), (2, 2), (2, 10)	1014c2
	(4), (2, 6), (2, 12)	1040g2
	(8), (2, 2), (2, 4)	294f1
	$(4)^2$, (2, 2), (2, 4)	120b1
	$(4)^2$, (2, 2), (4, 4)	320a4
	$(4)^2$, (2, 6), (2, 12)	450g1
	(4), $(6)^2$, (2, 2)	726a2
	(4), (6), (2, 2), (2, 6)	14a3
	(4), (6), (2, 6), (6, 6)	98a3
	(4), (8), (2, 2), (2, 8)	45a1
	(4), (10), (2, 2), (2, 10)	150b3
	(4), (12), (2, 2), (2, 12)	30a3
	(4), (16), (2, 2), (2, 16)	3150bk1

G	$\mathcal{H}_{\mathbb{Q}}(4, E)$	E
(2)	$(6)^2$, (2, 2), (2, 4)	256a1
	(6), (12), (2, 2), (2, 6)	36a4
	$(8)^2$, (2, 2), (4, 8)	2880r6
	(10), (20), (2, 2), (2, 10)	450a4
	$(4)^2$, (8), (2, 2), (2, 4)	33a2
	(4), (4), (8), (2, 2), (4, 4)	64a4
	$(4)^2$, (2, 2), $(2, 4)^2$	33a4
	$(4)^2$, (2, 6), $(2, 12)^2$	960o7
	(4), (6), (2, 2), (2, 4), (2, 6)	130a4
	(4), (8), (12), (2, 2), (2, 12)	960e3
	(4), (8), (16), (2, 2), (2, 8)	63a1
	(4), (8), (2, 2), (2, 4), (2, 8)	24a6
	(4), (12), (24), (2, 2), (2, 12)	960o3
	(4), (12), (2, 2), (2, 4), (2, 12)	720j3
	$(4)^2$, $(8)^2$, (2, 2), (2, 4)	45a3
	$(4)^2$, (8), (2, 2), $(2, 4)^2$	17a3
	(4), (8), $(16)^2$, (2, 2), (2, 8)	75b1
	(4), (8), (16), (2, 2), (2, 4), (2, 8)	510e7
	$(4)^2$, $(8)^2$, (2, 2), $(2, 4)^2$	63a6
	(4), $(6)^2$, (2, 2), $(2, 6)^2$, (3, 6)	112c3
	(4), (8), $(16)^2$, (2, 2), (2, 4), (2, 8)	1470k3
	$(6)^2$, (12), (2, 2), $(2, 6)^2$, (3, 6)	98a4
	$(4)^2$, (6), $(12)^2$, (2, 2), (2, 4), (2, 6)	30a7
	$(4)^2$, $(8)^4$, (2, 2), (2, 4)	630c6
	$(4)^2$, $(8)^4$, (2, 2), (4, 4)	4410r6
	$(4)^2$, $(8)^3$, (2, 2), $(2, 4)^2$	15a5
	$(4)^2$, (6), (8), $(12)^2$, (2, 2), (2, 4), (2, 6)	90c5
	$(4)^2$, (6), $(12)^2$, (2, 2), $(2, 4)^2$, (2, 6)	90c4
(3)	(15)	50a1
	(3, 3)	19a1

(4)	$(8), (2, 8)$	192c6
	$(8), (2, 12)$	150c3
	$(8), (4, 4)$	40a4
	$(2, 4), (2, 8)$	64a3
	$(8), (2, 4), (2, 8)$	17a4
	$(8), (2, 4), (4, 4)$	17a1
	$(8), (2, 8), (2, 16)$	1470k1
	$(8)^2, (2, 4), (2, 8)$	24a3
	$(8)^2, (2, 8), (4, 8)$	240d6
	$(8), (12), (2, 4), (2, 12)$	90c1
	$(12), (24), (2, 4), (2, 12)$	960o8
	$(8), (8), (16), (2, 4), (2, 8)$	21a4
	$(8)^2, (16)^2, (2, 4), (2, 8)$	15a7
	$(8)^2, (2, 4), (2, 8)^2, (4, 4)$	195a6
	$(8)^2, (16)^3, (2, 4), (2, 8)$	1230f4
	$(8)^2, (16)^2, (2, 4), (2, 8)^2, (4, 4)$	210e6
(5)	(15)	50b1
	$(5, 5)$	11a1
(6)	$(12), (2, 6)$	14a4
	$(12), (2, 6), (2, 12)$	130a2
	$(12)^2, (2, 6), (2, 12)$	30a1
	$(12), (2, 6), (3, 6), (6, 6)$	14a1
	$(12)^2, (24), (2, 6), (2, 12)$	90c8
	$(12)^2, (2, 6), (2, 12)^2$	90c7
(8)	$(16), (2, 8)$	21a3
	$(16), (2, 8), (2, 16)$	1230f1
	$(16), (2, 8), (4, 8)$	15a4
	$(16)^2, (2, 8), (2, 16)$	210e1
(10)	$(20), (2, 10)$	66c1
(12)	$(24), (2, 12)$	90c3

(2, 2)	$(2, 4), (2, 8)$	45a5
	$(2, 4), (4, 4)$	64a1
	$(2, 4)^3$	120b2
	$(2, 4)^2, (2, 8)$	63a2
	$(2, 4)^2, (2, 12)$	960o6
	$(2, 4)^2, (4, 4)$	17a2
	$(2, 4)^2, (4, 8)$	1200j4
	$(2, 4), (2, 6), (2, 12)$	90c2
	$(2, 4), (2, 8)^2$	45a2
	$(2, 4), (2, 8), (4, 8)$	75b3
	$(2, 4)^3, (2, 6)$	210a6
	$(2, 4)^3, (4, 4)$	231a3
	$(2, 4)^2, (2, 6), (2, 12)$	30a6
	$(2, 4)^2, (2, 8), (2, 16)$	75b2
	$(2, 4)^2, (2, 8), (4, 4)$	40a1
	$(2, 4)^2, (2, 8), (4, 8)$	510e5
	$(2, 4), (2, 6), (2, 12)^2$	14400bo6
	$(2, 4)^3, (2, 8), (4, 4)$	21a2
	$(2, 4)^2, (2, 8)^2, (4, 4)$	75b5
	$(2, 4), (2, 6), (2, 12)^3$	150c6
	$(2, 4)^3, (2, 8)^2, (4, 4)$	42a3
	$(2, 4)^2, (2, 8)^3, (4, 4)$	294c2
	$(2, 4)^3, (2, 8)^3, (4, 4)$	15a2
	$(2, 4)^2, (2, 8)^4, (4, 4)$	6720cd4
	$(2, 4)^3, (2, 8)^4, (4, 4)$	210e5
(2, 4)	$(2, 8), (4, 4)$	21a1
	$(2, 8)^2, (4, 4)$	24a1
	$(2, 8)^2, (4, 8)$	1230f2
	$(2, 8), (2, 16), (4, 4)$	15a3
	$(2, 8), (4, 4), (4, 8)$	15a1
	$(2, 8)^2, (4, 4), (4, 8)$	210e3
(2, 6)	$(2, 12)$	90c6
	$(2, 12)^3$	30a2
(2, 8)	$(2, 16)^2, (4, 8)$	210e2

$$h_{\mathbb{Q}}(4) \geq 9$$

130 configurations
Conductor < 400.000
largest conductor to obtain all the torsion configurations: 14.400

E. (2017) $d = 5$

$$\Phi_{\mathbb{Q}}(5) = \left\{ \begin{array}{ll} (n) & n = 1, \ldots, 11, 12, 25 \\ (2, 2m) & m = 1, 2, 3, 4 \end{array} \right\}$$

For $G \in \Phi(1) \setminus \{(1), (2), (5)\}$:

$$\Phi_{\mathbb{Q}}(5, G) = \{G\} \qquad \& \qquad \mathcal{H}_{\mathbb{Q}}(5, G) = \emptyset$$

Otherwise

G	$\Phi_{\mathbb{Q}}(5, G)$
(1)	$\{(1), (5), (11)\}$
(2)	$\{(2), (10)\}$
(5)	$\{(5), (25)\}$

G	$\mathcal{H}_{\mathbb{Q}}(5, G)$
(1)	(5)
	(11)
(2)	(10)
(5)	(25)

$$h_{\mathbb{Q}}(5) = 1$$

Daniels-E. (2020)

$d = 6$

$$\Phi^{\star}_{\mathbb{Q}}(6) = \Phi_{\mathbb{Q}}(6) \cap \Phi^{\infty}(6)$$

$$\Phi^{\star}_{\mathbb{Q}}(6) = \left\{ \begin{array}{ll} (n)\,, & n = 1, \ldots, 10, 12, \ldots, 16, 18, 21, 30 \\ (2, 2m)\,, & m = 1, 2, 3, 4, 5, 6, 7, 9 \\ (3, 3r)\,, & r = 1, 2, 3, 4 \\ (4, 4)\,, & \\ (6, 6) & \end{array} \right\}$$

Daniels-E. (2020)

$d = 6$

G	$\Phi^{\star}_{\mathbb{Q}}(6, G) \setminus \{G\}$
(1)	$\{(2), (3), (4), (5), (6), (7), (9), (10), (12), (13), (14), (15), (18)$ $(21), (2,2), (2,6), (2,10), (2,14), (2,18), (3,3), (3,9), (4,4), (6,6)\}$
(2)	$\{(4), (6), (8), (10), (12), (14), (16), (18), (2,2),$ $(2,6), (2,10), (2,14), (2,18), (3,6), (3,12), (6,6)\}$
(3)	$\{(6), (9), (12), (15), (21), (30), (2,6),$ $(3,3), (3,6), (3,9), (6,6)\}$
(4)	$\{(8), (12), (2,4), (2,8), (2,12), (3,12), (4,4)\}$
(5)	$\{(10), (15), (30), (2,10)\}$
(6)	$\{(12), (18), (2,6), (2,18), (3,6), (3,12), (6,6)\}$
(7)	$\{(14), (2,14)\}$
(8)	$\{(16), (2,8)\}$
(9)	$\{(18), (2,18), (3,9)\}$
(10)	$\{(2,10)\}$
(12)	$\{(2,12), (3,12)\}$
(2,2)	$\{(2,4), (2,6), (2,8), (2,12), (6,6)\}$
(2,4)	$\{(2,8), (4,4)\}$
(2,6)	$\{(2,12), (6,6)\}$
(2,8)	$\{\}$

Daniels-E. (2020)

$d = 6$

$$h_{\mathbb{Q}}(6) \geq 9$$

137 configurations
Conductor < 400.000
largest conductor to obtain all the torsion configurations: 10.816

Daniels-E. (2020)

$d = 6$

E.-Najman (2019)

$$(4, 12) \in \Phi_{\mathbb{Q}}(6) \setminus \Phi^{\star}_{\mathbb{Q}}(6) \Longrightarrow (4, 12) \in \Phi(6) \setminus \Phi^{\infty}(6)$$

$$\Phi^{\star}_{\mathbb{Q}}(6) \cup \{(4, 12)\} \subseteq \Phi_{\mathbb{Q}}(6)$$

Conjecture:

$$\Phi_{\mathbb{Q}}(6) = \Phi^{\star}_{\mathbb{Q}}(6) \cup \{(4, 12)\}$$

Gužvić (2021):

$$\Phi_{\mathbb{Q}}(6) \subseteq \Phi^{\star}_{\mathbb{Q}}(6) \cup \{(4, 12), (3, 18)\}$$


T. Gužvić,
Torsion growth of rational elliptic curves in sextic number fields.
J. Number Theory **220** (2021), 330–345.

E.-Najman (2017)

$d = 7$

$$\Phi_{\mathbb{Q}}(7) = \left\{ \begin{array}{ll} (n) & n = 1, \ldots, 10, 12 \\ (2, 2m) & m = 1, 2, 3, 4 \end{array} \right\} = \Phi(1)$$

For $G \in \Phi(1) \setminus \{(1)\}$:

$$\Phi_{\mathbb{Q}}(7, G) = \{G\} \qquad \& \qquad \mathcal{H}_{\mathbb{Q}}(7, G) = \emptyset$$

Otherwise

G	$\Phi_{\mathbb{Q}}(7, G)$
(1)	$\{(1), (7)\}$

G	$\mathcal{H}_{\mathbb{Q}}(7, G)$
(1)	(7)

$$h_{\mathbb{Q}}(7) = 1$$

E.-Najman (2017)

$2, 3, 5, 7 \nmid d$

$$\Phi_{\mathbb{Q}}(d) = \left\{ \begin{array}{ll} (n) & n = 1, \ldots, 10, 12 \\ (2, 2m) & m = 1, 2, 3, 4 \end{array} \right\} = \Phi(1)$$

For $G \in \Phi(1)$:

$$\Phi_{\mathbb{Q}}(d, G) = \{G\} \qquad \& \qquad \mathcal{H}_{\mathbb{Q}}(d, G) = \emptyset$$

$$h_{\mathbb{Q}}(d) = 0$$

$$E_{/\mathbb{Q}}\,,\ 2, 3, 5, 7 \nmid [K : \mathbb{Q}] \Longrightarrow E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$$

d	2	3	4	5	6	7	$2,3,5,7 \nmid d$
$h_{\mathbb{Q}}(d)$	4	3	≥ 9	≥ 9	1	1	0

E.-Najman (2017)

$S_{\mathbb{Q}}(d)$

Let $E/\mathbb{Q}$ be an elliptic curve, p a prime and P a point of order p in E. Then all of the cases in the table below occur for $p \leq 13$ or $p = 37$, and they are the only ones possible.

p	$[\mathbb{Q}(P) : \mathbb{Q}]$
2	$1, 2, 3$
3	$1, 2, 3, 4, 6, 8$
5	$1, 2, 4, 5, 8, 10, 16, 20, 24$
7	$1, 2, 3, 6, 7, 9, 12, 14, 18, 21, 24, 36, 42, 48$
11	$5, 10, 20, 40, 55, 80, 100, 110, 120$
13	$3, 4, 6, 12, 24, 39, 48, 52, 72, 78, 96, 144, 156, 168$
37	$12, 36, 72, 444, 1296, 1332, 1368$

E.-Najman (2017)

$S_{\mathbb{Q}}(d)$

For all other p, we have $[\mathbb{Q}(P):\mathbb{Q}]$ the following cases do occur:

p^2-1	for all p,
$8, 16, 32, 136, 256, 272, 288$	for $p = 17$
$(p-1)/2,\ p-1,\ p(p-1)/2,\ p(p-1)$	if $p \in \{19, 43, 67, 163\}$,
$2(p-1),\ (p-1)^2$ if $p \equiv 1 \pmod 3$ or	$\left(\frac{-D}{p}\right) = 1\,, D \in \mathcal{CM}$,
$(p-1)^2/3,\ 2(p-1)^2/3$	if $p \equiv 4, 7 \pmod 9$,
$(p^2-1)/3,\ 2(p^2-1)/3$	if $p \equiv 2, 5 \pmod 9$,

where $\mathcal{CM} = \{1, 2, 7, 11, 19, 43, 67, 163\}$.
Apart from the cases above that have been proven to appear, the only other options that might be possible are:

$$(p^2-1)/3,\ \ 2(p^2-1)/3 \qquad \text{if } p \equiv 8 \pmod 9.$$

E.-Najman (2017)

$S_{\mathbb{Q}}(d)$

Let $p = 2$ or $p > 5$ be a prime.

$$S_{\mathbb{Q}}(p) = S_{\mathbb{Q}}(1) = \{2, 3, 5, 7\}$$

$$S^*_{\mathbb{Q}}(d) = S_{\mathbb{Q}}(d) \setminus \bigcup_{\substack{d' \mid d \\ d' \neq d}} S_{\mathbb{Q}}(d')$$

d	1	3, 4	5	8	9	12	21	33	44	other $d \leq 50$
$S^*_{\mathbb{Q}}(d)$	2, 3, 5, 7	13	11	17	19	37	43	67	23	$\emptyset$

E.-Najman (2017) $S_{\mathbb{Q}}(d)$

Smallest "bad" prime is $p = 3167$

We determine $S_{\mathbb{Q}}(d)$, $d < 3.343.296$

If Serre's uniformity problem is answered positively, then we determine $S_{\mathbb{Q}}(d)$, for all d.

Serre's uniformity problem (1981): Let $E_{/\mathbb{Q}}$ be a non-CM elliptic curve, then

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p),$$

is surjective for $p > 37$ prime.

Mod n Galois representations associated to elliptic curves

- $E[n] = \{P \in E(\overline{\mathbb{Q}}) | n\,P = \mathcal{O}\} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
- $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$P = (x, y) \in E[n] \Longrightarrow {}^{\sigma}P = (\sigma(x), \sigma(y)) \in E[n]$$

$$\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

- $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \simeq \rho_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) =: G_E(n) \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$
- $\mathbb{Q}(P) = \mathbb{Q}(E[n])^{\mathcal{H}_P}$, $\mathcal{H}_P < \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$
- $[\mathbb{Q}(P) : \mathbb{Q}] = [\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) : \mathcal{H}_P]$
- $E[n] = \langle P_1, P_2 \rangle$, $P = aP_1 + bP_2$, $a, b \in \mathbb{Z}/n\mathbb{Z}$:

$$P \in E[n] \longleftrightarrow v = (a, b) \in (\mathbb{Z}/n\mathbb{Z})^2$$
$${}^{\sigma}P \longleftrightarrow M.v, \ M \in G_E(n)$$
$$[\mathbb{Q}(P) : \mathbb{Q}] = [G_E(n) : G_E(n)_v] = |G_E(n) \cdot v|,$$

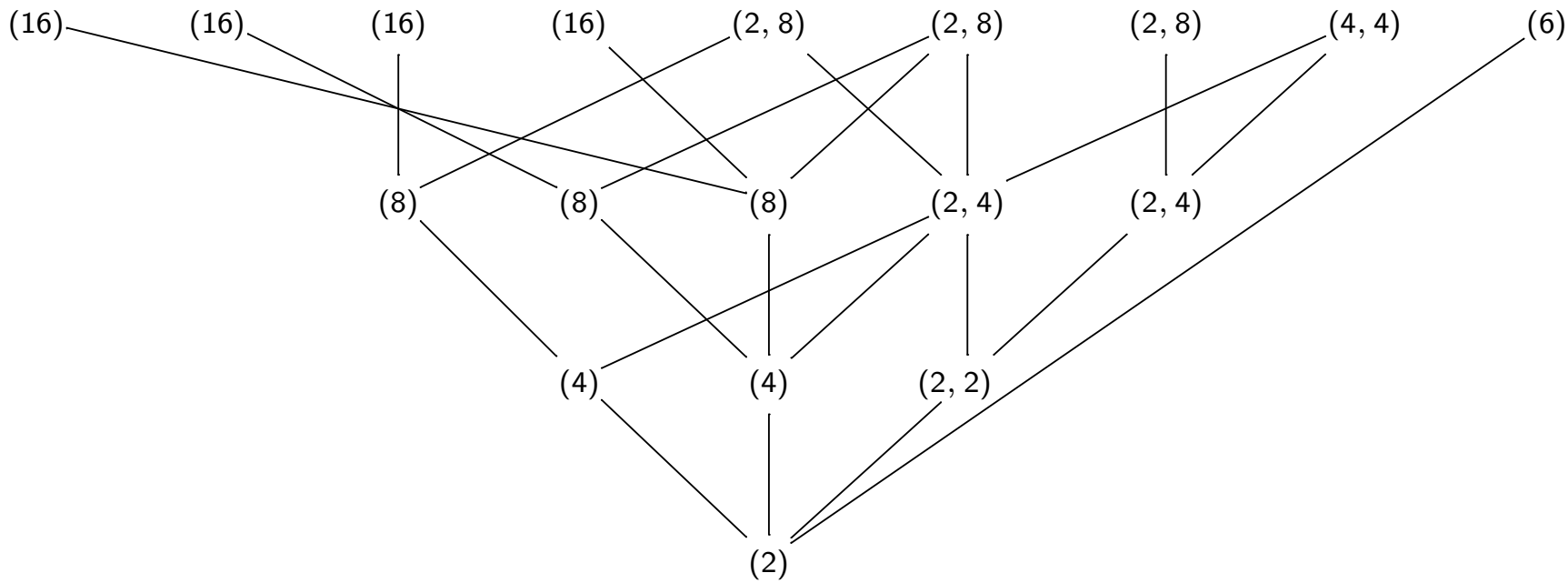
where $G_E(n)_v$ (resp. $G_E(n) \cdot v$) denotes the stabilizer (resp. orbit) of v by the action of $G_E(n)$ on $(\mathbb{Z}/n\mathbb{Z})^2$.

E.-Najman (2019) New algorithm GrowthTorsion

```
Magma V2.26-3     Thu May  20 2021 20:40:10 on luna
Type ? for help.  Type <Ctrl>-D to quit.

> E:=EllipticCurve("210e7");

> time G8:=GrowthTorsion(E,8);
 Has CM? false
 Torsion over Q : [ 2 ]
Computing for degree 2 ...
 Primes : [ 2 ]
 Torsion Growth over degree 2 : <[ 4 ], [ 4 ], [ 2, 2 ]>
Computing for degree 4 ...
 Primes : [ 2 ]
 Torsion Growth over degree 4 : <[ 8 ], [ 8 ], [ 8 ], [ 2, 4 ],[ 2, 4 ]>
Computing for degree 8 ...
 Primes : [ 3, 2 ]
 Torsion Growth over degree 8 : <[ 6 ], [ 16 ], [ 16 ], [ 16 ], [ 16 ],
 [ 2, 8 ], [ 2, 8 ], [ 2, 8 ], [ 4, 4 ]>
Time: 30.050
```


(16)
(16)
(16)
(16)
(2, 8)
(2, 8)
(2, 8)
(4, 4)
(6)
(8)
(8)
(8)
(2, 4)
(2, 4)
(4)
(4)
(2, 2)
(2)

E.-Najman (2019) New algorithm GrowthTorsion

d	$\Phi_{\mathbb{Q}}(d) \setminus \cup_{d' \mid d, d' < d} \Phi_{\mathbb{Q}}(d') \supseteq$	$h_{\mathbb{Q}}(d)$	$N_{\mathbb{Q}}(d)$	$\#\mathcal{H}_{\mathbb{Q}}(d)$
1	(1), (2), (3), (4), (5), (6), (7), (8), (9), (10), (12), (2, 2), (2, 4), (2, 6), (2, 8)	1	210	15
2	(15), (16), (2, 10), (2, 12), (3, 3), (3, 6), (4, 4)	4	3150	52
3	(13), (14), (18), (21), (2, 14)	3	3969	26
4	(13), (20), (24), (2, 16), (4, 8), (5, 5), (6, 6)	≥ 9	≥ 14400	≥ 130
5	(11), (25)	1	121	4
6	(30), (2, 18), (3, 9), (3, 12), (4, 12), (6, 6)	≥ 9	≥ 10816	≥ 137
7	–	1	26	1
8	(17), (21), (30), (32), (2, 20), (2, 24), (3, 12), (4, 12)	≥ 17	≥ 277440	≥ 275
9	(19), (26), (27), (28), (36), (42), (2, 18)	≥ 6	≥ 3969	≥ 34
10	–	≥ 4	≥ 3150	≥ 58
12	(26), (28), (36), (37), (42), (2, 28), (2, 30), (2, 42), (3, 15), (3, 21), (5, 10), (6, 12)	≥ 19	≥ 18176	≥ 268
14	–	≥ 4	≥ 3150	≥ 52
15	(22), (50)	≥ 3	≥ 3969	≥ 30
16	(40), (48), (2, 30), (2, 32), (3, 15), (4, 16), (4, 20), (5, 15), (6, 12), (8, 8)	≥ 25	≥ 277440	≥ 480
18	(45), (2, 26), (2, 36), (2, 42), (3, 18), (3, 21), (4, 28), (6, 18), (7, 7), (9, 9)	≥ 17	≥ 254016	≥ 192
20	(22), (33), (2, 22), (5, 10), (5, 15)	≥ 9	≥ 14400	≥ 149
21	(43)	≥ 3	≥ 3969	≥ 29

Tiempo para la publicidad:

E. González–Jiménez, J.M. Tornero.
Torsion of rational elliptic curves over quadratic fields.
Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. **108** (2014), 923–934.

E. González–Jiménez, J.M. Tornero.
Torsion of rational elliptic curves over quadratic fields II.
Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. **110** (2016), 121–143.

E. González–Jiménez, F. Najman, J.M. Tornero.
Torsion of rational elliptic curves over cubic fields.
Rocky Mountain J. Math. **46** (2016), no. 6, 1899–1917.

E. González–Jiménez.
Complete classification of the torsion structures of rational elliptic curves over quintic number fields.
Journal of Algebra **478** (2017), 484–505.

E. González–Jiménez, Á. Lozano–Robledo.
On torsion of rational elliptic curves over quartic fields.
Math. Comp. 87 (2018) 1457–1478.

Tiempo para la publicidad (continuación):


E. González–Jiménez, F. Najman.
Growth of torsion groups of elliptic curves upon base change.
Math. Comp. 89 (2020) 1457–1485.


H. Daniels, E. González–Jiménez.
On torsion of rational elliptic curves over sextics fields.
Math. Comp. 89 (2020) 411–439.

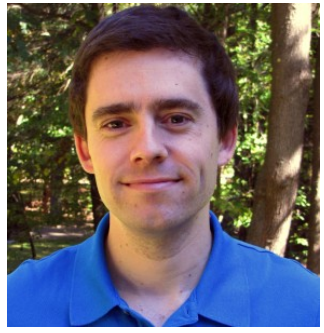

E. González–Jiménez, F. Najman.
An algorithm for determining torsion growth of elliptic curves.
A aparecer en Exp. Math.


E. González–Jiménez.
Explicit characterization of the torsion growth of rational elliptic curves with complex multiplication over quadratic fields.
Glas. Mat. Ser. III 56(76)(2021) 47–61


E. González–Jiménez.
Torsion growth over cubic fields of rational elliptic curves with complex multiplication.
Publ. Math. Debrecen 97/1-2 (2020) 63-76.

J.M. Tornero

F. Najman



Á. Lozano Robledo

H. Daniels

GRACIAS