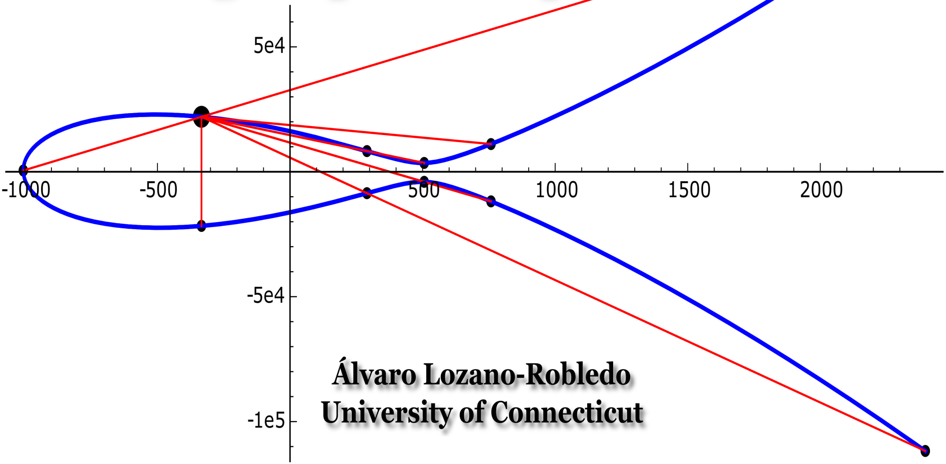
Recent progress in the classification of torsion subgroups of elliptic curves



Álvaro Lozano-Robledo
University of Connecticut

Recent progress in the classification of torsion subgroups of elliptic curves

Álvaro Lozano-Robledo

Department of Mathematics
University of Connecticut

September 29^{th}
Front Range Number Theory Day
Colorado State University

Definition

An elliptic curve E over a field F is a projective smooth curve of genus one, with at least one point defined over F.

Definition

An elliptic curve E over a field F is a projective smooth curve of genus one, with at least one point defined over F.

- Every elliptic curve has a (Weierstrass) model of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ for some } a_i \in F.$$

- We are interested in determining all F-rational points on E:

$$E(F) = \{(x_0, y_0) \in E : x_0, y_0 \in F\} \cup \{\mathcal{O} = [0 : 1 : 0]\}.$$

Definition

An elliptic curve E over a field F is a projective smooth curve of genus one, with at least one point defined over F.

- Every elliptic curve has a (Weierstrass) model of the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \text{ for some } a_i \in F.$$

- We are interested in determining all F-rational points on E:

$$E(F) = \{(x_0, y_0) \in E : x_0, y_0 \in F\} \cup \{\mathcal{O} = [0 : 1 : 0]\}.$$

Example

Let $E/\mathbb{Q}$ be the curve $y^2 = x^3 + 13x - 34$, with Cremona label "40a4".

Definition

An elliptic curve E over a field F is a projective smooth curve of genus one, with at least one point defined over F.

- Every elliptic curve has a (Weierstrass) model of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ for some } a_i \in F.$$

- We are interested in determining all F-rational points on E:

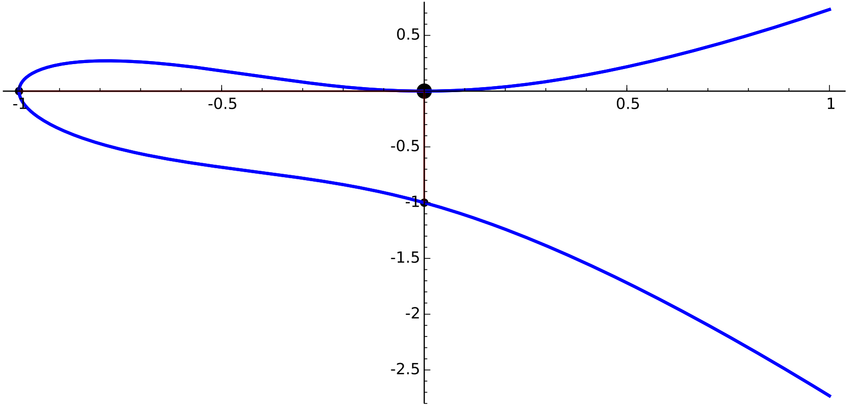
$$E(F) = \{(x_0, y_0) \in E : x_0, y_0 \in F\} \cup \{\mathcal{O} = [0 : 1 : 0]\}.$$

Example

Let $E/\mathbb{Q}$ be the curve $y^2 = x^3 + 13x - 34$, with Cremona label "40a4". Then:

$$E(\mathbb{Q}) = \{\mathcal{O}, (7, -20), (2, 0), (7, 20)\} \cong \mathbb{Z}/4\mathbb{Z},$$

where $\mathcal{O} = [0 : 1 : 0]$, in projective coordinates.



The elliptic curve $E/\mathbb{Q} : y^2 + xy + y = x^3 + x^2$
has a point $P = (0, 0)$ of order 4.

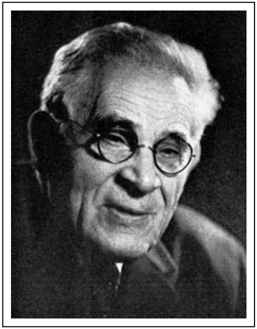
Example

Let $E/\mathbb{Q}(i)$ be the curve $y^2 = x^3 + 13x - 34$.

Example

Let $E/\mathbb{Q}(i)$ be the curve $y^2 = x^3 + 13x - 34$. Then:

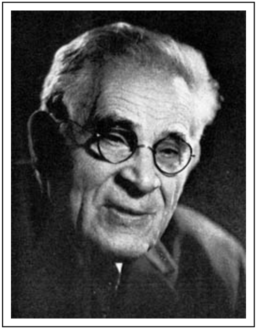
$$E(\mathbb{Q}(i)) = \langle (1+2i, -2-6i), (-3, -10i) \rangle \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$



Louis Mordell
1888 – 1972

Theorem (Mordell, 1922)

Let $E/\mathbb{Q}$ be an elliptic curve. Then, the group of $\mathbb{Q}$-rational points on E, denoted by $E(\mathbb{Q})$, is a finitely generated abelian group. In particular, $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$ where $E(\mathbb{Q})_{tors}$ is a finite subgroup, and $R_{E/\mathbb{Q}} \geq 0$.

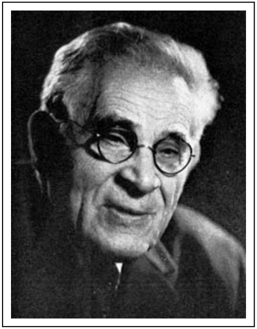


Louis Mordell
1888 – 1972

André Weil
1906 – 1998

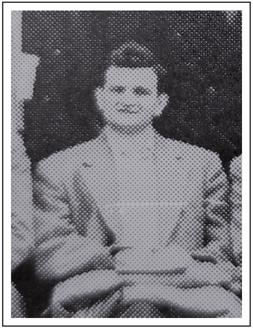
Theorem (Mordell–Weil, 1928)

Let F be a number field, and let A/F be an abelian variety. Then, the group of F-rational points on A, denoted by $A(F)$, is a finitely generated abelian group. In particular, $A(F) \cong A(F)_{tors} \oplus \mathbb{Z}^{R_{A/F}}$ where $A(F)_{tors}$ is a finite subgroup, and $R_{A/F} \geq 0$.



Louis Mordell
1888 – 1972

André Weil
1906 – 1998



André Néron
1922 – 1985

Theorem (Mordell–Weil–Néron, 1952)

Let F be a field that is finitely generated over its prime field, and let A/F be an abelian variety. Then, the group of F-rational points on A, denoted by $A(F)$, is a finitely generated abelian group. In particular, $A(F) \cong A(F)_{tors} \oplus \mathbb{Z}^{R_{A/F}}$ where $A(F)_{tors}$ is a finite subgroup, and $R_{A/F} \geq 0$.

Theorem (Mordell–Weil–Néron, 1952)

Let F be a field that is finitely generated over its prime field (e.g., a global field), and let A/F be an abelian variety. Then, the group of F-rational points on A, denoted by $A(F)$, is a finitely generated abelian group. In particular, $A(F) \cong A(F)_{tors} \oplus \mathbb{Z}^{R_{A/F}}$ where $A(F)_{tors}$ is a finite subgroup, and $R_{A/F} \geq 0$.

... leads to ...

Theorem (Mordell–Weil–Néron, 1952)

Let F be a field that is finitely generated over its prime field (e.g., a global field), and let A/F be an abelian variety. Then, the group of F-rational points on A, denoted by $A(F)$, is a finitely generated abelian group. In particular, $A(F) \cong A(F)_{tors} \oplus \mathbb{Z}^{R_{A/F}}$ where $A(F)_{tors}$ is a finite subgroup, and $R_{A/F} \geq 0$.

... leads to ...

Natural Question

What finitely generated abelian groups arise from abelian varieties over global fields?

There are a number of ways to study this question, depending on what we allow to **vary.**

Natural Question

What finitely generated abelian groups arise from abelian varieties over global fields?

Variations: **Mordell–Weil groups of elliptic curves for a fixed field F**

Fix a field F, and vary over 1-dimensional abelian varieties over F.

$$\begin{tikzcd}[column sep=small]
E_1(F) & E_2(F) & \dots & E_k(F) & \dots \\
 & & F \arrow[ull, no head] \arrow[ul, no head] \arrow[u, no head] \arrow[ur, no head] \arrow[urr, no head] & &
\end{tikzcd}$$

where $E_1, E_2, \dots, E_k, \dots$ is some family of (perhaps all) elliptic curves over a fixed field F.

Natural Question

What finitely generated abelian groups arise from abelian varieties over global fields?

Variations: **Mordell–Weil groups for a fixed curve E/F and vary L/F**

Fix an elliptic curve E/F, and vary over finite extensions of F.

$$\begin{tikzcd}
E(L_1) \arrow[ddrr, dash] & E(L_2) \arrow[ddr, dash] & \dots \arrow[dd, dash] & E(L_2) \arrow[ddl, dash] & \dots \arrow[ddll, dash] \\
& & & & \\
& & E/F & &
\end{tikzcd}$$

where $L_1, L_2, \dots, L_k, \dots$ is some family of (perhaps all) finite extensions of the base field F, contained in some fixed algebraic closure $\overline{F}$.

Natural Question

What finitely generated abelian groups arise from abelian varieties over global fields?

Variations: **ranks in a family of elliptic curves over a fixed** F

$$\begin{tikzcd}
R_{E_1/F} \arrow[drr, dash] & R_{E_2/F} \arrow[dr, dash] & \cdots \arrow[d, dash] & R_{E_k/F} \arrow[dl, dash] & \cdots \arrow[dll, dash] \\
 & & F & &
\end{tikzcd}$$

where $E_1, E_2, \ldots, E_k, \ldots$ is some family of (perhaps all) elliptic curves over a fixed field F.

Natural Question

What finitely generated abelian groups arise from abelian varieties over global fields?

Variations: **ranks for a fixed curve E/F under field extensions L/F**

$$
\begin{tikzcd}
R_{E/L_1} \arrow[drr, dash] & R_{E/L_2} \arrow[dr, dash] & \dots \arrow[d, dash] & R_{E/L_k} \arrow[dl, dash] & \dots \arrow[dll, dash] \\
 & & E/F & &
\end{tikzcd}
$$

where $L_1, L_2, \dots, L_k, \dots$ is some family of (perhaps all) finite extensions of a fixed field F, contained in some fixed algebraic closure $\overline{F}$.

Natural Question

What finitely generated abelian groups arise from abelian varieties over global fields?

Variations: **torsion subgroups in a family of curves over a fixed** F

$$\begin{tikzcd}
E_1(F)_{\mathrm{tors}} \arrow[drr, dash] & E_2(F)_{\mathrm{tors}} \arrow[dr, dash] & \cdots \arrow[d, dash] & E_k(F)_{\mathrm{tors}} \arrow[dl, dash] & \cdots \arrow[dll, dash] \\
 & & F & &
\end{tikzcd}$$

where $E_1, E_2, \ldots, E_k, \ldots$ is some family of (perhaps all) elliptic curves over a fixed field F.

Natural Question

What finitely generated abelian groups arise from abelian varieties over global fields?

Variations: **torsion for a fixed curve E/F over extensions L/F**

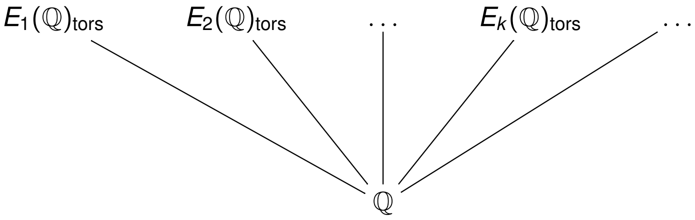
$$\begin{tikzcd}[column sep=small]
E(L_1)_{\text{tors}} \arrow[drr, dash] & E(L_2)_{\text{tors}} \arrow[dr, dash] & \cdots \arrow[d, dash] & E(L_k)_{\text{tors}} \arrow[dl, dash] & \cdots \arrow[dll, dash] \\
 & & E/F & &
\end{tikzcd}$$

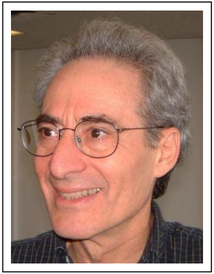
where $L_1, L_2, \ldots, L_k, \ldots$ is some family of (perhaps all) finite extensions of a fixed field F, contained in some fixed algebraic closure $\overline{F}$.

Torsion subgroups of elliptic curves over $\mathbb{Q}$

$$\begin{tikzcd}
E_1(\mathbb{Q})_{\text{tors}} & E_2(\mathbb{Q})_{\text{tors}} & \cdots & E_k(\mathbb{Q})_{\text{tors}} & \cdots \\
 & & \mathbb{Q} \arrow[ull, dash] \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] \arrow[urr, dash] & &
\end{tikzcd}$$

Torsion subgroups of elliptic curves over $\mathbb{Q}$





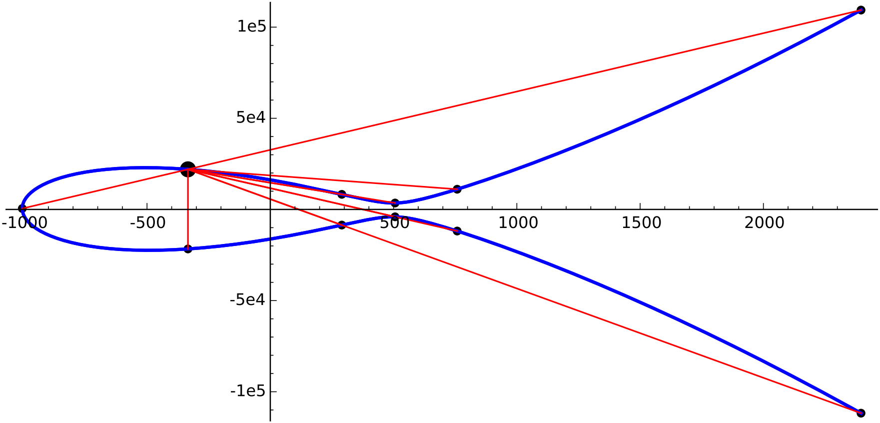
Barry Mazur

Theorem (Levi–Ogg Conjecture; Mazur, 1977)

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

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

Moreover, each possible group appears infinitely many times.



The elliptic curve `30030bt1` has a point of order 12.

All elliptic curves with given torsion

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

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

Torsion subgroups of elliptic curves over $\mathbb{F}_q(T)$

Fix a prime p, let $q = p^n$, and $K = \mathbb{F}_q(T)$.

$$\begin{tikzcd}[column sep=small]
E_1(\mathbb{F}_q(T))_{\text{tors}} \arrow[drr, dash] & E_2(\mathbb{F}_q(T))_{\text{tors}} \arrow[dr, dash] & \cdots \arrow[d, dash] & E_k(\mathbb{F}_q(T))_{\text{tors}} \arrow[dl, dash] & \cdots \arrow[dll, dash] \\
 & & \mathbb{F}_q(T) & &
\end{tikzcd}$$

Torsion subgroups of elliptic curves over $\mathbb{F}_q(T)$

Fix a prime p, let $q = p^n$, and $K = \mathbb{F}_q(T)$.

$$\begin{tikzcd}
E_1(\mathbb{F}_q(T))_{\mathrm{tors}} \arrow[drr, dash] & E_2(\mathbb{F}_q(T))_{\mathrm{tors}} \arrow[dr, dash] & \cdots \arrow[d, dash] & E_k(\mathbb{F}_q(T))_{\mathrm{tors}} \arrow[dl, dash] & \cdots \arrow[dll, dash] \\
 & & \mathbb{F}_q(T) & &
\end{tikzcd}$$

Building on work of Cox and Parry (1980), and Levin (1968):

Theorem (McDonald, 2017)

Let $K = \mathbb{F}_q(T)$ for q a power of p. Let E/K be non-isotrivial. If $p \nmid E(K)_{\mathrm{tors}}$, then $E(K)_{\mathrm{tors}}$ is one of

$$0,\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \ldots,\ \mathbb{Z}/10\mathbb{Z},\ \mathbb{Z}/12\mathbb{Z},$$
$$(\mathbb{Z}/2\mathbb{Z})^2,\ \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},$$
$$(\mathbb{Z}/3\mathbb{Z})^2,\ \mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z},\ (\mathbb{Z}/4\mathbb{Z})^2,\ (\mathbb{Z}/5\mathbb{Z})^2.$$

If $p \mid \#E(K)_{\mathrm{tors}}$, then $p \leq 11$, and $E(K)_{\mathrm{tors}}$ is one of

$$\begin{array}{cl}
\mathbb{Z}/p\mathbb{Z} & \text{if } p = 2, 3, 5, 7, 11, \\
\mathbb{Z}/2p\mathbb{Z} & \text{if } p = 2, 3, 5, 7, \\
\mathbb{Z}/3p\mathbb{Z} & \text{if } p = 2, 3, 5, \\
\mathbb{Z}/4p\mathbb{Z}, \mathbb{Z}/5p\mathbb{Z}, & \text{if } p = 2, 3, \\
\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/14\mathbb{Z}, \mathbb{Z}/18\mathbb{Z} & \text{if } p = 2, \\
\mathbb{Z}/10\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z} & \text{if } p = 2, \\
\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} & \text{if } p = 3, \\
\mathbb{Z}/10\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} & \text{if } p = 5.
\end{array}$$

Characteristic	$E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2,\ f \in K$		G
$p = 11$	$a = \frac{(f+3)(f+5)^2(f+9)^2}{3(f+1)(f+4)^4}$	$b = a\frac{(f+1)^2(f+9)}{2(f+4)^3}$	$\mathbb{Z}/11\mathbb{Z}$
$p = 2$	$a = \frac{f(f+1)^3}{f^3+f+1}$	$b = a\frac{1}{f^3+f+1}$	$\mathbb{Z}/14\mathbb{Z}$
$p = 7$	$a = \frac{(f+1)(f+3)^3(f+4)(f+6)}{f(f+2)^2(f+5)}$	$b = a\frac{(f+1)(f+5)^3}{4f(f+2)}$	
$p = 3$	$a = \frac{f^3(f+1)^2}{(f+2)^6}$	$b = a\frac{f(f^4+2f^3+f+1)}{(f+2)^5}$	$\mathbb{Z}/15\mathbb{Z}$
$p = 5$	$a = \frac{(f+1)(f+2)^2(f+4)^3(f^2+2)}{(f+3)^6(f^2+3)}$	$b = a\frac{f(f+4)}{(f+3)^5}$	
$p = 2$	$a = \frac{f(f+1)^2(f^2+f+1)}{f^3+f+1}$	$b = a\frac{(f+1)^2}{f^3+f+1}$	$\mathbb{Z}/18\mathbb{Z}$
$p = 5$	$a = \frac{f(f+1)(f+2)^2(f+3)(f+4)}{(f^2+4f+1)^2}$	$b = a\frac{(f+1)^2(f+3)^2}{4(f^2+4f+1)^2}$	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p = 3,\ \zeta_4 \in k$	$a = \frac{f(f+1)(f+2)(f^2+2f+2)}{(f^2+f+2)^3}$	$b = a\frac{(f^2+1)^2}{f(f^2+f+2)}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p = 2,\ \zeta_4 \in k$	$a = \frac{f(f^4+f+1)(f^4+f^3+1)}{(f^2+f+1)^5}$	$b = a\frac{f^2(f^4+f^3+1)^2}{(f^2+f+1)^5}$	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Table: families of elliptic curves such that $G \subset E_{a,b}(K)_{\mathrm{tors}}$.

Theorem (McDonald, 2018)

Let C be a curve of genus 1 over $\mathbb{F}_q$, for $q = p^n$, and let $K = \mathbb{F}_q(C)$. Let E/K be non-isotrivial. If $p \nmid \#E(K)_{\mathrm{tors}}$, then $E(K)_{\mathrm{tors}}$ is one of

$$\begin{array}{cl} \mathbb{Z}/N\mathbb{Z} & \textit{with } N = 1, \ldots, 12, 14, 15, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{with } N = 1, \ldots, 6, \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \textit{with } N = 1, 2, 3, \\ \mathbb{Z}/4N\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \textit{with } N = 1, 2, \\ (\mathbb{Z}/N\mathbb{Z})^2 & \textit{with } N = 5, 6. \end{array}$$

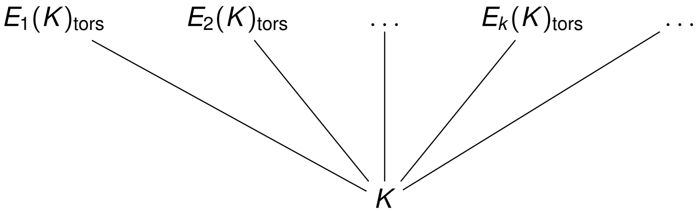
If $p \mid \#E(K)_{\mathrm{tors}}$, then $p \leq 13$, and $E(K)_{\mathrm{tors}}$ is one of

$$\begin{array}{cl} \mathbb{Z}/p\mathbb{Z} & \textit{if } p = 2, 3, 5, 7, 11, 13, \\ \mathbb{Z}/2p\mathbb{Z}, \mathbb{Z}/2p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{if } p = 3, 5, 7, \\ \mathbb{Z}/3p\mathbb{Z}, \mathbb{Z}/4p\mathbb{Z} & \textit{if } p = 2, 3, 5 \\ \mathbb{Z}/5p\mathbb{Z}, \mathbb{Z}/6p\mathbb{Z}, \mathbb{Z}/7p\mathbb{Z}, \mathbb{Z}/8p\mathbb{Z} & \textit{if } p = 2, 3, \\ \mathbb{Z}/2N\mathbb{Z} & \textit{for } N = 9, 10, 11, 15, \ \textit{if } p = 2, \\ \mathbb{Z}/6N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \textit{for } N = 1, 2, 3, \ \textit{if } p = 2, \\ \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} & \textit{if } p = 2, \\ \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \textit{if } p = 3, \\ (\textit{and possibly } \mathbb{Z}/143\mathbb{Z}, & \textit{for } p = 13). \end{array}$$

Torsion subgroups of elliptic curves over quad. field K

$$
\begin{tikzcd}
E_1(K)_{\text{tors}} \arrow[drr, dash] & E_2(K)_{\text{tors}} \arrow[dr, dash] & \cdots \arrow[d, dash] & E_k(K)_{\text{tors}} \arrow[dl, dash] & \cdots \arrow[dll, dash] \\
 & & K & &
\end{tikzcd}
$$

Torsion subgroups of elliptic curves over quad. field K



Filip Najman

Theorem (Najman, 2011)

Let $E/\mathbb{Q}(i)$ be an elliptic curve. Then

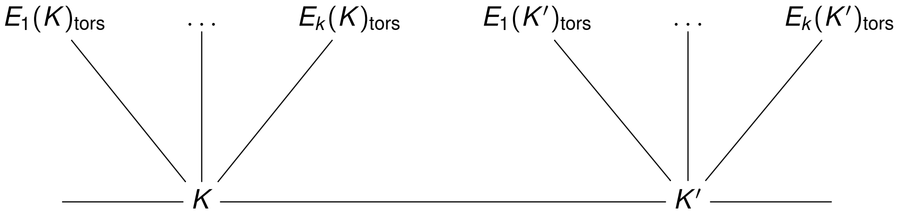
$$E(\mathbb{Q}(i))_{tors} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \text{ or } M = 12, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 4, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

Moreover, each torsion subgroup occurs infinitely many times.

Torsion subgroups of elliptic curves over quad. fields K

$$
\begin{tikzcd}
E_1(K)_{\text{tors}} \arrow[dr, dash] & \ldots \arrow[d, dash] & E_k(K)_{\text{tors}} \arrow[dl, dash] & E_1(K')_{\text{tors}} \arrow[dr, dash] & \ldots \arrow[d, dash] & E_k(K')_{\text{tors}} \arrow[dl, dash] \\
{} \arrow[r, dash] & K \arrow[rrr, dash] & & & K' \arrow[r, dash] & {}
\end{tikzcd}
$$

Torsion subgroups of elliptic curves over quad. fields K



Theorem (Kenku and Momose, 1988; Kamienny, 1992)

Let $K/\mathbb{Q}$ be a quadratic field and let E/K be an elliptic curve. Then

$$E(K)_{tors} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 16 \text{ or } M = 18, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 6, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \text{with } M = 1 \text{ or } 2, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. & \end{cases}$$

Moreover, each torsion subgroup occurs infinitely many times.

Torsion subgroups of elliptic curves over quad. fields K

Monsur Kenku

Fumiyuki Momose

Sheldon Kamienny

Theorem (Kenku and Momose, 1988; Kamienny, 1992)

Let $K/\mathbb{Q}$ be a quadratic field and let E/K be an elliptic curve. Then

$$E(K)_{tors} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 16 \text{ or } M = 18, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 6, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \text{with } M = 1 \text{ or } 2, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

Moreover, each torsion subgroup occurs infinitely many times.

Example: a point of order 13 (due to Markus Reichert)

Example

Let $K = \mathbb{Q}(\sqrt{17})$. The elliptic curve E/K defined by

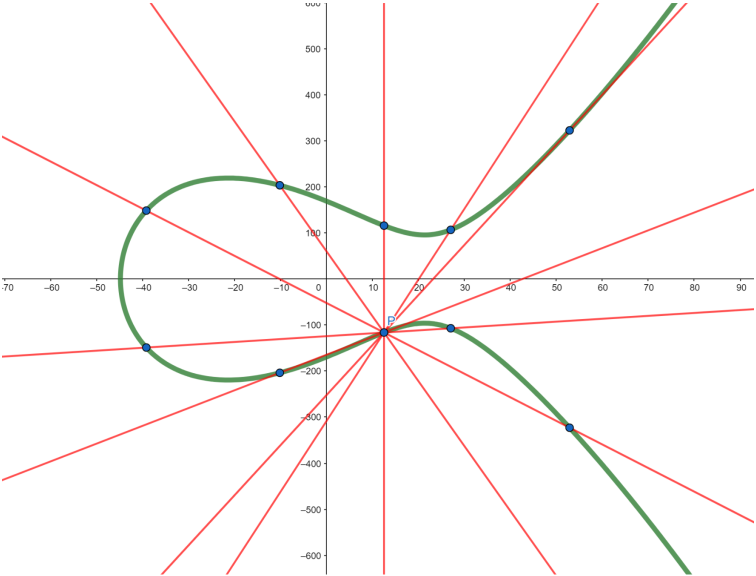
$$y^2 = x^3 + (-411864 + 99560\sqrt{17})x + (211240640 - 51226432\sqrt{17})$$

has a point

$$P = (-474 + 118\sqrt{17}, -9088 + 2176\sqrt{17})$$

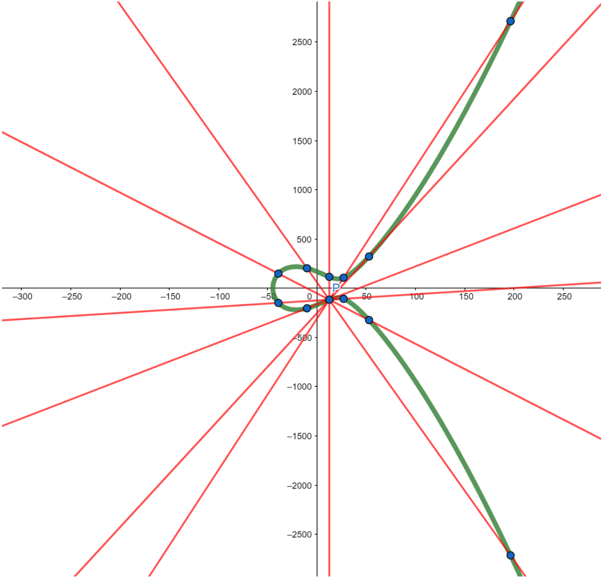
of exact order 13.

Example: a point of order 13 (due to Markus Reichert)



$$y^2 = x^3 + (-411864 + 99560\sqrt{17})x + (211240640 - 51226432\sqrt{17})$$

Example: a point of order 13 (due to Markus Reichert)



$$y^2 = x^3 + (-411864 + 99560\sqrt{17})x + (211240640 - 51226432\sqrt{17})$$

Example: Another point of order 13

Example

Let E be the elliptic curve defined by

$$y^2 + y = x^3 + x^2 - 114x + 473.$$

Then, E has a torsion point of order 13 defined over $K/\mathbb{Q}$, a cubic Galois extension, where $K = \mathbb{Q}(\alpha)$ and

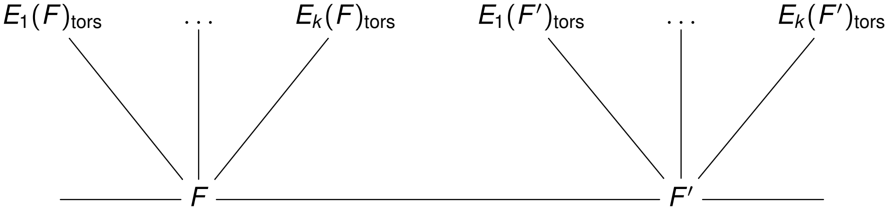
$$\alpha^3 - 48\alpha^2 + 425\alpha - 1009 = 0.$$

The point P of order 13 is $(\alpha, 7\alpha - 39)$.

Torsion subgroups of elliptic curves over cubic fields

$$\begin{tikzcd}[arrows=dash]
E_1(F)_{\text{tors}} \arrow[dr] & \cdots \arrow[d] & E_k(F)_{\text{tors}} \arrow[dl] & E_1(F')_{\text{tors}} \arrow[dr] & \cdots \arrow[d] & E_k(F')_{\text{tors}} \arrow[dl] \\
{} \arrow[r] & F \arrow[rrr] & & & F' \arrow[r] & {}
\end{tikzcd}$$

Torsion subgroups of elliptic curves over cubic fields



Theorem (Jeon, Kim, Schweizer, 2004)

Let F be a **cubic** *number field, and let E be an elliptic curve defined over F. The groups that appear as torsion subgroups for* **infinitely many** *non-isomorphic elliptic curves E/F are precisely:*

$$\begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{with } 1 \leq m \leq 20, m \neq 17, 19, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \text{with } 1 \leq m \leq 7. \end{cases}$$

Daeyeol Jeon

Chang Heon Kim

Andreas Schweizer

Theorem (Jeon, Kim, Schweizer, 2004)

Let F be a **cubic** *number field, and let E be an elliptic curve defined over F. The groups that appear as torsion subgroups for* **infinitely many** *non-isomorphic elliptic curves E/F are precisely:*

$$\begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{with } 1 \leq m \leq 20, m \neq 17, 19, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \text{with } 1 \leq m \leq 7. \end{cases}$$

Warning! These are not all the possible groups!

Daeyeol Jeon

Chang Heon Kim

Andreas Schweizer

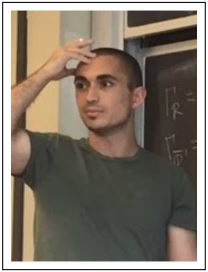
Theorem (Jeon, Kim, Schweizer, 2004)

Let F be a **cubic** *number field, and let E be an elliptic curve defined over F. The groups that appear as torsion subgroups for* **infinitely many** *non-isomorphic elliptic curves E/F are precisely:*

$$\begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{with } 1 \le m \le 20, m \ne 17, 19, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \text{with } 1 \le m \le 7. \end{cases}$$

Warning! These are not all the possible groups! Najman has shown that for $E : 162B1/\mathbb{Q}$ and $F = \mathbb{Q}(\zeta_9)^+$ we have $E(F)_{\text{tors}} \cong \mathbb{Z}/21\mathbb{Z}$.

Anastasia
Etropolski



Jackson
Morrow

David
Zureick-Brown

Marteen
Derickx

Theorem (Etropolski–Morrow–Z-B., and Derickx, 2016)

Let F be a cubic number field, and let E be an elliptic curve defined over F. The groups that appear as torsion subgroups of $E(F)$ are precisely:

$$\begin{cases} \mathbb{Z}/m\mathbb{Z} & \textit{with } 1 \leq m \leq 21, m \neq 17, 19, \textit{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \textit{with } 1 \leq m \leq 7. \end{cases}$$

Quartic, Quintic, Sextic, and beyond

Daeyeol Jeon

Chang Heon Kim

Euisung Park

Theorem (Jeon, Kim, Park, 2006)

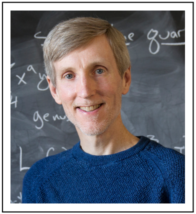
Let F be a **quartic** *number field, and let E be an elliptic curve defined over F. The groups that appear as torsion subgroups for* **infinitely many** *non-isomorphic elliptic curves E/F are precisely:*

$$\begin{cases} \mathbb{Z}/m\mathbb{Z} & \textit{with } 1 \leq m \leq 24, m \neq 19, 23, \textit{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \textit{with } 1 \leq m \leq 9, \textit{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} & \textit{with } 1 \leq m \leq 3, \textit{ or} \end{cases}$$

$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, *or* $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Quartic, Quintic, Sextic, and beyond

Marteen Derickx



Drew Sutherland

Theorem (Derickx, Sutherland, 2016)

Let F be a **quintic** *number field, and let E be an elliptic curve defined over F. The groups that appear as torsion subgroups for* **infinitely many** *non-isomorphic elliptic curves E/F are precisely:*

$$\begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{with } 1 \leq m \leq 25, m \neq 23, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \text{with } 1 \leq m \leq 8. \end{cases}$$

Maarten Derickx (and L-R.)

Theorem (Derickx, Sutherland, 2016)

Let F be a **sextic** *number field, and let E be an elliptic curve defined over F. The groups that appear as torsion subgroups for* **infinitely many** *non-isomorphic elliptic curves E/F are precisely:*

$$\begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{with } 1 \leq m \leq 30,\, m \neq 23, 25, 29 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \text{with } 1 \leq m \leq 10, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} & \text{with } 1 \leq m \leq 4, \text{ or} \end{cases}$$

$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, *or* $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

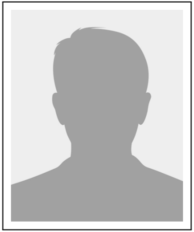
A special case: elliptic curves with CM

Let F be a number field, and let E/F be an elliptic curve with CM.

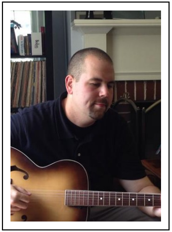
A special case: elliptic curves with CM

Let F be a number field, and let E/F be an elliptic curve with CM.

Pete
Clark



Patrick
Corn



Alex
Rice

James
Stankewicz

Theorem (Clark, Corn, Rice, Stankewicz, 2013)

Let F be a number field of degree $1 \leq d \leq 13$, and let E/F be an elliptic curve with CM. Then, the complete list of possible torsion subgroups $E(F)_{tors}$ is given, and an algorithm to compute the list for $d \geq 1$.

A special case: elliptic curves with CM

Let F be a number field, and let E/F be an elliptic curve with CM.

Theorem (Clark, Corn, Rice, Stankewicz, 2013)

Let F be a number field of degree $1 \leq d \leq 13$, and let E/F be an elliptic curve with CM. Then, the complete list of possible torsion subgroups $E(F)_{tors}$ is given.

For example, over $\mathbb{Q}$: $\{\mathcal{O}\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Over quadratics, not over $\mathbb{Q}$:
$\mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Over quartics, besides quadratics and $\mathbb{Q}$:
$\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/13\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$,
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

A special case: elliptic curves with CM

Abbey Bourdon

Pete Clark

Theorem (Bourdon, Clark, 2017)

Let K be quad. imaginary, let $K \subseteq F$ be a number field, let E/F be an elliptic curve with CM by an order $\mathcal{O} \subseteq K$, and let $N \geq 2$. There is an explicit constant $T(\mathcal{O}, N)$ such that if there is a point of order N in $E(F)_{tors}$, then $T(\mathcal{O}, N)$ divides $[F : K(j(E))]$. Moreover, this bound is best possible.

See also **Davide Lombardo**'s work on torsion bounds for abelian varieties with CM.

A simpler case: base extension of $E/\mathbb{Q}$

Let $E/\mathbb{Q}$ be an elliptic curve, and let $F/\mathbb{Q}$ be a finite extension. Then, $E(\mathbb{Q})_{\text{tors}} \subseteq E(F)_{\text{tors}}$.

Variations: **torsion for a fixed curve $E/\mathbb{Q}$ over extensions $F/\mathbb{Q}$**

$$
\begin{tikzcd}
E(F_1)_{\text{tors}} & E(F_2)_{\text{tors}} & \dots & E(F_k)_{\text{tors}} & \dots \\
 & & E/\mathbb{Q} \arrow[ull, dash] \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] \arrow[urr, dash] & &
\end{tikzcd}
$$

where $F_1, F_2, \dots, F_k, \dots$ is some family of (perhaps all) finite extensions of $\mathbb{Q}$, contained in some fixed algebraic closure $\overline{\mathbb{Q}}$.

A simpler case: base extension of $E/\mathbb{Q}$

Theorem (L-R., 2011)

Let $S^1_{\mathbb{Q}}(d)$ be the set of primes such that there is an elliptic curve $E/\mathbb{Q}$ with a point of order p defined in an extension $F/\mathbb{Q}$ of degree $\leq d$. Then:

- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7\}$ *for* $d = 1$ *and* 2;
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 13\}$ *for* $d = 3$ *and* 4;
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13\}$ *for* $d = 5$, 6, *and* 7;
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17\}$ *for* $d = 8$;
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17, 19\}$ *for* $d = 9$, 10, *and* 11;
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17, 19, 37\}$ *for* $12 \leq d \leq 20$.
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43\}$ *for* $d = 21$.

A simpler case: base extension of $E/\mathbb{Q}$

Theorem (L-R., 2011)

Let $S^1_{\mathbb{Q}}(d)$ be the set of primes such that there is an elliptic curve $E/\mathbb{Q}$ with a point of order p defined in an extension $F/\mathbb{Q}$ of degree $\leq d$. Then:

- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7\}$ *for* $d = 1$ *and* 2*;*
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 13\}$ *for* $d = 3$ *and* 4*;*
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13\}$ *for* $d = 5$*,* 6*, and* 7*;*
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17\}$ *for* $d = 8$*;*
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17, 19\}$ *for* $d = 9$*,* 10*, and* 11*;*
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17, 19, 37\}$ *for* $12 \leq d \leq 20$*.*
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43\}$ *for* $d = 21$*.*

Moreover, there is a conjectural formula for $S^1_{\mathbb{Q}}(d)$ for all $d \geq 1$, which is valid for all $1 \leq d \leq 42$, and would follow from a positive answer to Serre's uniformity question.

A simpler case: base extension of $E/\mathbb{Q}$

Let $E/\mathbb{Q}$ be an elliptic curve, let p be a prime, and let $T \subseteq E[p^n]$ be a subgroup with $T \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z}$. We studied the minimal degree $[\mathbb{Q}(T) : \mathbb{Q}]$ of definition of T.

Enrique González-Jiménez (and L-R.)

For example:

Theorem (González-Jiménez, L-R., 2017)

Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ without CM, and let $P \in E[2^N]$ be a point of exact order 2^N, with $N \geq 4$. Then, the degree $[\mathbb{Q}(P) : \mathbb{Q}]$ is divisible by 2^{2N-7}. Moreover, this bound is best possible.

Base extension of $E/\mathbb{Q}$ to a quadratic field

Filip Najman

Theorem (Najman, 2015)

Let $E/\mathbb{Q}$ be an elliptic curve and let F be a quadratic number field. Then

$$E(F)_{\mathrm{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \text{ or } M = 12, 15, 16, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 6, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \text{with } 1 \leq M \leq 2 \text{ and } F = \mathbb{Q}(\sqrt{-3}), \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \text{with } F = \mathbb{Q}(\sqrt{-1}). \end{cases}$$

Base extension of $E/\mathbb{Q}$ to a cubic field

Let $E/\mathbb{Q}$ be an elliptic curve, and let $K/\mathbb{Q}$ be a finite extension. Then, $E(\mathbb{Q})_{\text{tors}} \subseteq E(K)_{\text{tors}}$.

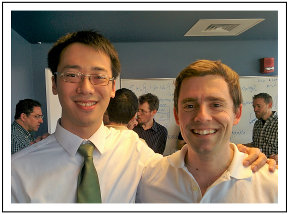
Theorem (Najman, 2015)

Let $E/\mathbb{Q}$ be an elliptic curve and let F be a cubic number field. Then

$$E(F)_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \text{ or } 12, 13, 14, 18, 21, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 4 \text{ or } M = 7. \end{cases}$$

Moreover, the elliptic curve 162B1 over $\mathbb{Q}(\zeta_9)^+$ is the unique rational elliptic curve over a cubic field with torsion subgroup isomorphic to $\mathbb{Z}/21\mathbb{Z}$. For all other groups T listed above there are infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$ for which $E(F) \simeq T$ for some cubic field F.

Base extension of $E/\mathbb{Q}$ to a quartic field



Michael Chou (and L-R.)

Theorem (Chou, 2015)

Let $E/\mathbb{Q}$ be an elliptic curve and let F be a Galois quartic field F with $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ *or* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$*. Then*

$$E(F)_{\mathrm{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \le M \le 16 \text{ but } M \ne 11, 14 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \le M \le 6, \text{ or } M = 8, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \text{with } 1 \le M \le 2 \text{ or} \end{cases}$$

$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, *or* $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Base extension of $E/\mathbb{Q}$ to a quartic field

Enrique González-Jiménez

Theorem (González-Jiménez, L-R., 2016)

We give a complete classification of torsion subgroups that appear **infinitely often** *for elliptic curves over $\mathbb{Q}$ base-extended to a quartic number field.*

Warning! The torsion group $\mathbb{Z}/15\mathbb{Z}$ appears infinitely often for curves *defined* over quartic fields F, but if $E/\mathbb{Q}$ and $E(F)_{\text{tors}} \cong \mathbb{Z}/15\mathbb{Z}$, then $j(E) \in \{-5^2/2, -5^2 \cdot 241^3/2^3, -5 \cdot 29^3/2^5, 5 \cdot 211^3/2^{15}\}$.

Base extension of $E/\mathbb{Q}$ to a quartic field

Enrique González-Jiménez

Filip Najman

Theorem (González-Jiménez, Najman, 2016)

Let $E/\mathbb{Q}$ be an elliptic curve and let F be a quartic field. Then

$$E(F)_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \textit{with } 1 \leq M \leq 10 \textit{ or } 12, 13, 15, 16, 20, 24 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \textit{with } 1 \leq M \leq 6, \textit{ or } 8, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \textit{with } 1 \leq M \leq 2 \textit{ or} \end{cases}$$

$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, *or* $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Base extension of $E/\mathbb{Q}$ to a quartic field

Enrique González-Jiménez

Filip Najman

Further, they determine all the possible prime orders of a point $P \in E(F)_{\text{tors}}$, where $[F : \mathbb{Q}] = d$ for all $d \leq 3342296$.

Base extension of $E/\mathbb{Q}$ to an infinite extension

Let $E/\mathbb{Q}$ be an elliptic curve, and let $F/\mathbb{Q}$ be an **infinite algebraic extension.** Then, $E(\mathbb{Q})_{\text{tors}} \subseteq E(F)_{\text{tors}}$. But, $E(F)_{\text{tors}}$ may no longer be finite!

Base extension of $E/\mathbb{Q}$ to an infinite extension

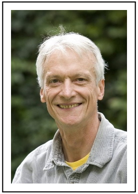
Let $E/\mathbb{Q}$ be an elliptic curve, and let $F/\mathbb{Q}$ be an **infinite algebraic extension.** Then, $E(\mathbb{Q})_{\text{tors}} \subseteq E(F)_{\text{tors}}$. But, $E(F)_{\text{tors}}$ may no longer be finite! Let $F_1 \subseteq F_2 \subseteq \ldots \subseteq F_k \subseteq \ldots$ be a **tower** of finite extensions of $\mathbb{Q}$.

Variations: **torsion for a fixed curve $E/\mathbb{Q}$ over extensions $F_k/\mathbb{Q}$**

$$
\begin{tikzcd}
 & & & E(F_k)_{\text{tors}} \arrow[ddddl, no head] & \ldots \arrow[ddddll, no head] \\
 & & \ldots \arrow[ur, hook] \arrow[dddd, no head] & & \\
 & E(F_2)_{\text{tors}} \arrow[ur, hook] \arrow[ddr, no head] & & & \\
E(F_1)_{\text{tors}} \arrow[ur, hook] \arrow[drr, no head] & & & & \\
 & & E/\mathbb{Q} & &
\end{tikzcd}
$$

Base extension of $E/\mathbb{Q}$ to an infinite extension

Michael Laska



Martin Lorenz

Yasutsugu Fujita

Theorem (Laska, Lorenz, 1985; Fujita, 2005)

Let $E/\mathbb{Q}$ be an elliptic curve and let $\mathbb{Q}(2^\infty) := \mathbb{Q}(\{\sqrt{m} : m \in \mathbb{Z}\})$. The torsion subgroup $E(\mathbb{Q}(2^\infty))_{\mathrm{tors}}$ is finite, and

$$E(\mathbb{Q}(2^\infty))_{\mathrm{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } M \in 1,3,5,7,9,15, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 6 \text{ or } M = 8, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \text{or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4M\mathbb{Z} & \text{with } 1 \leq M \leq 4, \text{ or} \\ \mathbb{Z}/2M\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 3 \leq M \leq 4. \end{cases}$$

Özlem Ejder

Theorem (Ejder, 2017)

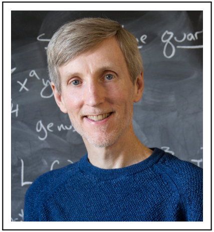
Let $K = \mathbb{Q}(i)$, or $\mathbb{Q}(\sqrt{-3})$, let E/K be an elliptic curve and let F be the maximal elementary 2-abelian extension of K. Then,

$$E(F)_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 2 \leq M \leq 6 \text{ or } M = 8, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4M\mathbb{Z} & \text{with } 2 \leq M \leq 4, \text{ or} \\ \mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/M\mathbb{Z} & \text{with } M = 2, 3, 4, 6, \text{ or } 8, \end{cases}$$

if $K = \mathbb{Q}(i)$, and if $K = \mathbb{Q}(\sqrt{-3})$, then $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$ is also possible.

Harris Daniels (and L-R.)

(L-R. and) Filip Najman



Drew Sutherland

Theorem (Daniels, L-R., Najman, Sutherland, 2017)

Let $E/\mathbb{Q}$ be an elliptic curve, and let $\mathbb{Q}(3^\infty)$ be the compositum of all cubic fields. The torsion subgroup $E(\mathbb{Q}(3^\infty))_{\mathrm{tors}}$ is finite, and

$$E(\mathbb{Q}(3^\infty))_{\mathrm{tors}} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \textit{with } M = 1,2,4,5,7,8,13, \textit{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4M\mathbb{Z} & \textit{with } M = 1,2,4,7, \textit{ or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6M\mathbb{Z} & \textit{with } M = 1,2,3,5,7, \textit{ or} \\ \mathbb{Z}/2M\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \textit{with } M = 4,6,7,9. \end{cases}$$

All but 4 of the torsion subgroups occur infinitely often.

Base extension of $E/\mathbb{Q}$ to an infinite extension

New results of classification of torsion subgroups of $E/\mathbb{Q}$ after base-extension to infinite extensions:

- **Daniels**: classification of torsion over $\mathbb{Q}(D_4^\infty)$.
- **Daniels, Derickx, Hatley**: classification of torsion over $\mathbb{Q}(A_4^\infty)$.

Harris Daniels

Marteen Derickx

Jeffrey Hatley

Base extension of $E/\mathbb{Q}$ to an infinite abelian extension

Ken Ribet, (L-R.) and Michael Chou

Theorem (Ribet, 1981)

Let $A/\mathbb{Q}$ be an abelian variety and let $\mathbb{Q}^{ab}$ be the maximal abelian extension of $\mathbb{Q}$. Then, $A(\mathbb{Q}^{ab})_{tors}$ is finite.

Base extension of $E/\mathbb{Q}$ to an infinite abelian extension

Yurii Zarhin

Theorem (Zarhin, 1983)

Let K be a number field, let A/K be an abelian variety, and let K^{ab} be the maximal abelian extension of K. Then, $A(K^{ab})_{tors}$ is finite if and only if A has no abelian subvariety with CM over K.

Base extension of $E/\mathbb{Q}$ to an infinite abelian extension

Theorem (González-Jiménez, L-R., 2015)

Let $E/\mathbb{Q}$ be an elliptic curve. If there is an integer $n \geq 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4$, or 5.

Base extension of $E/\mathbb{Q}$ to an infinite abelian extension

Theorem (González-Jiménez, L-R., 2015)

Let $E/\mathbb{Q}$ be an elliptic curve. If there is an integer $n \geq 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4$, or 5. More generally, if $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian, then $n = 2, 3, 4, 5, 6$, or 8.

Base extension of $E/\mathbb{Q}$ to an infinite abelian extension

Theorem (González-Jiménez, L-R., 2015)

Let $E/\mathbb{Q}$ be an elliptic curve. If there is an integer $n \geq 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4,$ or 5. More generally, if $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian, then $n = 2, 3, 4, 5, 6,$ or 8. Moreover, $G_n = \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is isomorphic to one of the following groups:

n	2	3	4	5	6	8
G_n	$\{0\}$ $\mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$ $(\mathbb{Z}/2\mathbb{Z})^4$	$\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/4\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$	$(\mathbb{Z}/2\mathbb{Z})^4$ $(\mathbb{Z}/2\mathbb{Z})^5$ $(\mathbb{Z}/2\mathbb{Z})^6$

Furthermore, each possible Galois group occurs for infinitely many distinct j-invariants.

Base extension of $E/\mathbb{Q}$ to an infinite abelian extension

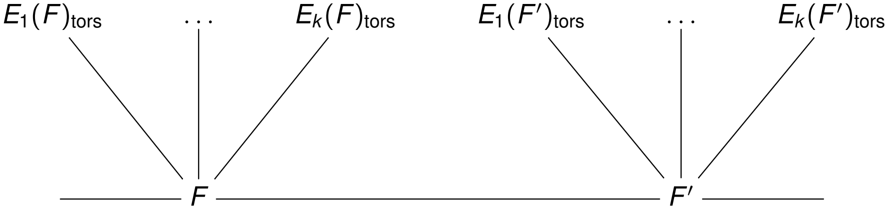
Ken Ribet, (L-R.) and Michael Chou

Theorem (Chou, 2018)

Let $E/\mathbb{Q}$ be an elliptic curve and let $\mathbb{Q}^{ab}$ be the maximal abelian extension of $\mathbb{Q}$. Then, $\#E(\mathbb{Q}^{ab})_{tors} \leq 163$. This bound is sharp, as the curve `26569a1` has a point of order 163 over $\mathbb{Q}^{ab}$. Moreover, a full classification of the possible torsion subgroups is given.

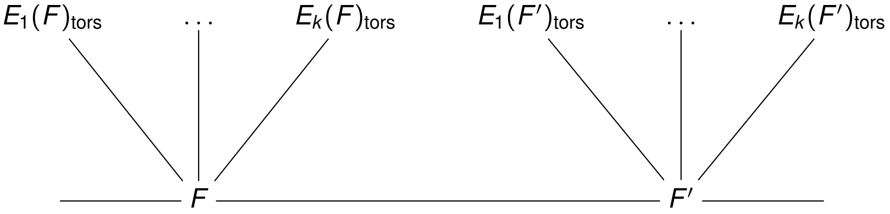
The Uniform Boundedness Conjecture

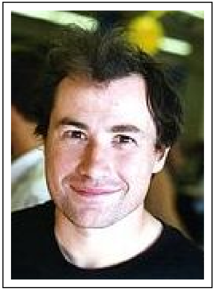
Variations: fix a **degree** d, and vary elliptic curves E over F of deg. d.



The Uniform Boundedness Conjecture

Variations: fix a **degree** d, and vary elliptic curves E over F of deg. d.





Loïc Merel

Theorem (Merel, 1996)

Let F be a number field of degree $[F:\mathbb{Q}] = d > 1$. Then, there is a number $B(d) > 0$ such that $|E(F)_{tors}| \leq B(d)$ **for all** *elliptic curves E/F.*

The Uniform Boundedness ~~Conjecture~~ Theorem

Theorem (Merel, 1996)

Let F be a number field of degree $[F:\mathbb{Q}] = d > 1$. There is a number $B(d) > 0$ such that $|E(F)_{tors}| \leq B(d)$ **for all** *elliptic curves E/F.*

The Uniform Boundedness ~~Conjecture~~ Theorem

Theorem (Merel, 1996)

Let F be a number field of degree $[F:\mathbb{Q}] = d > 1$. There is a number $B(d) > 0$ such that $|E(F)_{tors}| \leq B(d)$ **for all** *elliptic curves E/F.*

For instance, $B(1) = 16$, and $B(2) = 24$.

The Uniform Boundedness ~~Conjecture~~ Theorem

Theorem (Merel, 1996)

Let F be a number field of degree $[F:\mathbb{Q}] = d > 1$. There is a number $B(d) > 0$ such that $|E(F)_{tors}| \leq B(d)$ **for all** *elliptic curves E/F.*

For instance, $B(1) = 16$, and $B(2) = 24$.

Folklore Conjecture (As seen in Clark, Cook, Stankewicz)

There is a constant $C > 0$ such that

$$B(d) \leq C \cdot d \cdot \log \log d \quad \text{for all} \quad d \geq 3.$$

Folklore Conjecture

There is a constant $C > 0$ such that

$$B(d) \leq C \cdot d \cdot \log\log d \;\text{ for all }\; d \geq 3.$$

Folklore Conjecture

There is a constant $C > 0$ such that

$$B(d) \leq C \cdot d \cdot \log\log d \quad \text{for all} \quad d \geq 3.$$

Theorem (Hindry, Silverman, 1999)

Let F be a field of degree $d \geq 2$, and let E/F be an elliptic curve such that $j(E)$ is an algebraic integer. Then, we have

$$|E(F)_{tors}| \leq 1977408 \cdot d \cdot \log d.$$

Folklore Conjecture

There is a constant $C > 0$ such that

$$B(d) \leq C \cdot d \cdot \log\log d \quad \text{for all} \quad d \geq 3.$$

Theorem (Clark, Pollack, 2015)

There is an absolute, effective constant C such that for all number fields F of degree $d \geq 3$ and all elliptic curves E/F with CM, we have

$$|E(F)_{tors}| \leq C \cdot d \cdot \log\log d.$$

Folklore Conjecture

There is a constant $C > 0$ such that

$$B(d) \leq C \cdot d \cdot \log\log d \ \text{ for all } \ d \geq 3.$$

Folklore Conjecture

There is a constant $C > 0$ such that

$$B(d) \leq C \cdot d \cdot \log\log d \ \text{ for all } \ d \geq 3.$$

Assuming the conjecture, if $F/\mathbb{Q}$ is of degree $d \geq 3$, and $E(F)_{\text{tors}}$ contains a point of order p^n, for some prime p, and $n \geq 1$, then

$$p^n \leq |E(F)_{\text{tors}}| \leq B(d) \leq C \cdot d \log\log d.$$

Folklore Conjecture

There is a constant $C > 0$ such that

$$B(d) \leq C \cdot d \cdot \log\log d \quad \text{for all} \quad d \geq 3.$$

Assuming the conjecture, if $F/\mathbb{Q}$ is of degree $d \geq 3$, and $E(F)_{\text{tors}}$ contains a point of order p^n, for some prime p, and $n \geq 1$, then

$$p^n \leq |E(F)_{\text{tors}}| \leq B(d) \leq C \cdot d \log\log d.$$

Theorem

Let F be a number field of degree $[F : \mathbb{Q}] = d > 1$. If $P \in E(F)$ is a point of exact prime power order p^n, then

1. *(Merel,1996) $p \leq d^{3d^2}$.*

Folklore Conjecture

There is a constant $C > 0$ such that

$$B(d) \leq C \cdot d \cdot \log\log d \quad \text{for all} \quad d \geq 3.$$

Assuming the conjecture, if $F/\mathbb{Q}$ is of degree $d \geq 3$, and $E(F)_{\text{tors}}$ contains a point of order p^n, for some prime p, and $n \geq 1$, then

$$p^n \leq |E(F)_{\text{tors}}| \leq B(d) \leq C \cdot d \log\log d.$$

Theorem

Let F be a number field of degree $[F : \mathbb{Q}] = d > 1$. If $P \in E(F)$ is a point of exact prime power order p^n, then

1. *(Merel, 1996)* $p \leq d^{3d^2}$.
2. *(Parent, 1999)* $p^n \leq 129(5^d - 1)(3d)^6$.

Definition

Let p be a prime, and let F/L be an extension of number fields. We define $e_{\text{max}}(p, F/L)$ as the largest ramification index $e(\mathfrak{P}|\wp)$ for a prime $\mathfrak{P}$ of $\mathcal{O}_F$ over a prime $\wp$ of $\mathcal{O}_L$ lying above the rational prime p.

Definition

Let p be a prime, and let F/L be an extension of number fields. We define $e_{\max}(p, F/L)$ as the largest ramification index $e(\mathfrak{P}|\wp)$ for a prime $\mathfrak{P}$ of $\mathcal{O}_F$ over a prime $\wp$ of $\mathcal{O}_L$ lying above the rational prime p.

Theorem (L-R., 2013)

Let F be a number field with degree $[F : \mathbb{Q}] = d \geq 1$, and suppose there is an elliptic curve E/F with CM by a full order, with a point of order p^n. Then,

$$\varphi(p^n) \leq 24 \cdot e_{max}(p, F/\mathbb{Q}) \leq 24d.$$

Definition

Let p be a prime, and let F/L be an extension of number fields. We define $e_{\max}(p, F/L)$ as the largest ramification index $e(\mathfrak{P}|\wp)$ for a prime $\mathfrak{P}$ of $\mathcal{O}_F$ over a prime $\wp$ of $\mathcal{O}_L$ lying above the rational prime p.

Theorem (L-R., 2013)

Let F be a number field with degree $[F : \mathbb{Q}] = d \geq 1$, and suppose there is an elliptic curve E/F with CM by a full order, with a point of order p^n. Then,

$$\varphi(p^n) \leq 24 \cdot e_{max}(p, F/\mathbb{Q}) \leq 24d.$$

Note! The ramification index $e_{\max}(p, F/\mathbb{Q}) = 1$ for all but finitely many primes p, for a fixed field F.

Definition

We define $e_{\max}(p, F/L)$ as the largest ramification index $e(\mathfrak{P}|\wp)$ for a prime $\mathfrak{P}$ of $\mathcal{O}_F$ over a prime $\wp$ of $\mathcal{O}_L$ lying above the rational prime p.

Theorem (L-R., 2013)

Let F be a number field with degree $[F:\mathbb{Q}] = d \geq 1$, and suppose there is an elliptic curve E/F with CM by a full order, with a point of order p^n. Then,

$$\varphi(p^n) \leq 24 \cdot e_{max}(p, F/\mathbb{Q}) \leq 24d.$$

Definition

We define $e_{\max}(p, F/L)$ as the largest ramification index $e(\mathfrak{P}|\wp)$ for a prime $\mathfrak{P}$ of $\mathcal{O}_F$ over a prime $\wp$ of $\mathcal{O}_L$ lying above the rational prime p.

Theorem (L-R., 2013)

Let F be a number field with degree $[F:\mathbb{Q}] = d \geq 1$, and suppose there is an elliptic curve E/F with CM by a full order, with a point of order p^n. Then,

$$\varphi(p^n) \leq 24 \cdot e_{max}(p, F/\mathbb{Q}) \leq 24d.$$

Theorem (L-R., 2014)

Let F be a number field with degree $[F:\mathbb{Q}] = d \geq 1$, and let p be a prime such that there is an elliptic curve E/F with a point of order p^n. Suppose that F has a prime $\mathfrak{P}$ over p such that E/F has potential good supersingular reduction at $\mathfrak{P}$. Then,

$$\varphi(p^n) \leq 24e(\mathfrak{P}|p) \leq 24e_{max}(p, F/\mathbb{Q}) \leq 24d.$$

Theorem (L-R., 2014)

Let F be a number field with degree $[F:\mathbb{Q}] = d \geq 1$, and let p be a prime such that there is an elliptic curve E/F with a point of order p^n. Suppose that F has a prime $\mathfrak{P}$ over p such that E/F has potential good supersingular reduction at $\mathfrak{P}$. Then,

$$\varphi(p^n) \leq 24e(\mathfrak{P}|p) \leq 24e_{max}(p, F/\mathbb{Q}) \leq 24d.$$

Note: Hanson Smith has shown an improved version of this theorem in the case of **good** supersingular reduction, showing that $\varphi(p^n) \leq d$.

Hanson Smith

Conjecture

There is $C > 0$ s.t. if there is a point of order p^n in $E(F)$ for some E/F with $[F : \mathbb{Q}] \leq d$, then

$$\varphi(p^n) \leq C \cdot e_{\max}(p, F/\mathbb{Q}) \leq C \cdot d.$$

Variations: **torsion subgroups under field extensions**

$$\begin{tikzcd}
E(L_1)_{\mathrm{tors}} & E(L_2)_{\mathrm{tors}} & \cdots & E(L_k)_{\mathrm{tors}} & \cdots \\
 & & E/F \arrow[ull, dash] \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] \arrow[urr, dash] & &
\end{tikzcd}$$

where $L_1, L_2, \ldots, L_k, \ldots$ is some family of (perhaps all) finite extensions of a fixed field F.

Theorem (L-R., 2013)

If $p > 2$ and there is an elliptic curve $E/\mathbb{Q}$ with a point of order p^n defined in an extension $L/\mathbb{Q}$ of degree $d \geq 2$, then

$$\varphi(p^n) \leq 222 \cdot e_{max}(p, L/\mathbb{Q}) \leq 222 \cdot d.$$

Theorem (L-R., 2013)

If $p > 2$ and there is an elliptic curve $E/\mathbb{Q}$ with a point of order p^n defined in an extension $L/\mathbb{Q}$ of degree $d \geq 2$, then

$$\varphi(p^n) \leq 222 \cdot e_{max}(p, L/\mathbb{Q}) \leq 222 \cdot d.$$

Theorem (L-R., 2013)

Let F be a number field, and let $p > 2$ be a prime such that there is an elliptic curve E/F with a point of order p^n defined in an extension L of F, with $[L : \mathbb{Q}] = d \geq 2$. Then, there is a constant C_F such that

$$\varphi(p^n) \leq C_F \cdot e_{max}(p, L/\mathbb{Q}) \leq C_F \cdot d.$$

Theorem (L-R., 2013)

If $p > 2$ and there is an elliptic curve $E/\mathbb{Q}$ with a point of order p^n defined in an extension $L/\mathbb{Q}$ of degree $d \geq 2$, then

$$\varphi(p^n) \leq 222 \cdot e_{max}(p, L/\mathbb{Q}) \leq 222 \cdot d.$$

Theorem (L-R., 2013)

Let F be a number field, and let $p > 2$ be a prime such that there is an elliptic curve E/F with a point of order p^n defined in an extension L of F, with $[L : \mathbb{Q}] = d \geq 2$. Then, there is a constant C_F such that

$$\varphi(p^n) \leq C_F \cdot e_{max}(p, L/\mathbb{Q}) \leq C_F \cdot d.$$

Moreover, there is a computable finite set Σ_F such that if p^n is as above and $j(E) \notin \Sigma_F$, then

$$\varphi(p^n) \leq 588 \cdot e_{max}(p, L/\mathbb{Q}) \leq 588 \cdot d.$$

THANK YOU

alvaro.lozano-robledo@uconn.edu

"*If by chance I have omitted anything*
more or less proper or necessary,
I beg forgiveness,
since there is no one who is without fault
and circumspect in all matters."

Leonardo Pisano (Fibonacci), *Liber Abaci*.

David Zywina

Theorem (Hindry–Ratazzi conjecture; Zywina, 2017)

Let A be a nonzero abelian variety over a number field F for which the Mumford-Tate conjecture holds. Let $A/\mathbb{C} \sim \prod_{i=1}^{n} A_i^{m_i}$ such that each A_i is simple and pairwise non-isogenous, and define $A_I = \prod_{i \in I} A_i^{m_i}$ for any subset $I \subseteq \{1, \dots, n\}$. Let G_{A_I} be the Mumford-Tate group of A_I. Define $\gamma_A = \max_{I \subseteq \{1,\dots,n\}} 2\dim A_I / dim G_{A_I}$. Then, γ_A is the smallest real value such that for any finite extension L/K and real number $\varepsilon > 0$, we have

$$\#A(L)_{tors} \leq C \cdot [L:K]^{\gamma_A + \varepsilon},$$

where C is a constant that depends only on A and ε.