Mordell-Weil Groups of Elliptic Curves

Caleb McWhorter
Syracuse University

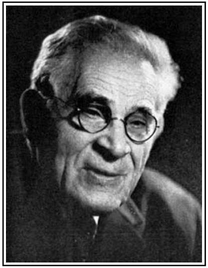
Binghamton University
Arithmetic Seminar
November 25, 2019

Theorem (Mordell, 1922)

Let $E/\mathbb{Q}$ be an elliptic curve. Then the group of $\mathbb{Q}$-rational points on E, denoted $E(\mathbb{Q})$, is a finitely generated abelian group. In particular,

$$E(\mathbb{Q}) \cong \mathbb{Z}^{r_{\mathbb{Q}}} \oplus E(\mathbb{Q})_{tors},$$

where $r_{\mathbb{Q}} \geq 0$ is the rank of E and $E(\mathbb{Q})_{tors}$ is the torsion subgroup.



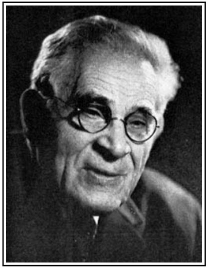
Louis J. Mordell

Theorem (Mordell-Weil, 1928)

Let K be a number field, and let A/K be an abelian variety. Then the group of K-rational points on A, denoted $A(K)$, is a finitely generated abelian group. In particular,

$$A(K) \cong \mathbb{Z}^{r_K} \oplus A(K)_{tors},$$

where $r_K \geq 0$ and $A(K)_{tors}$ is the torsion subgroup.



Louis J. Mordell

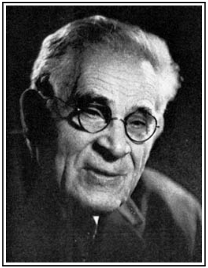
André Weil

Theorem (Mordell-Weil-Néron, 1952)

Let K be a field that is finitely generated over its prime field, and let A/K be an abelian variety. Then the group of K-rational points on A, denoted $A(K)$, is a finitely generated abelian group. In particular,

$$A(K) \cong \mathbb{Z}^{r_K} \oplus A(K)_{tors},$$

where $r_K \geq 0$ is the rank and $A(K)_{tors}$ is the torsion subgroup.



Louis J. Mordell

André Weil

André Néron

Question

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

This depends on what we vary.

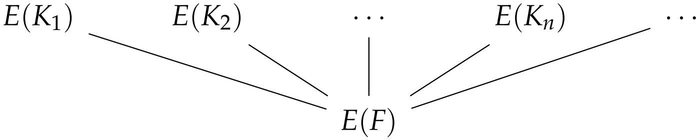
- Fix a global field K, and vary elliptic curves over K.

$$E_1(K), \quad E_2(K), \quad \dots \quad , \quad E_n(K), \quad \dots$$

- Fix a global field K, and vary elliptic curves over K.

$$E_1(K), \quad E_2(K), \quad \ldots \quad , \quad E_n(K), \quad \ldots$$

- Fix an elliptic curve defined over F, and vary over finite extensions K/F

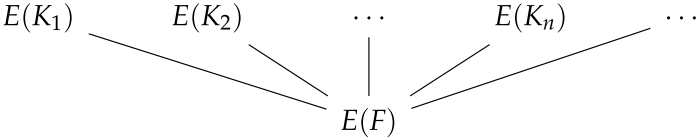


where $K_1, K_2, \ldots, K_n, \ldots$ are in some family of finite extensions of F, contained in some fixed algebraic closure $\overline{F}$. Or vary over all elliptic curves over all extensions $\{K_n\}$.

- Fix a global field K, and vary elliptic curves over K.

$$E_1(K), \quad E_2(K), \quad \ldots \quad , \quad E_n(K), \quad \ldots$$

- Fix an elliptic curve defined over F, and vary over finite extensions K/F

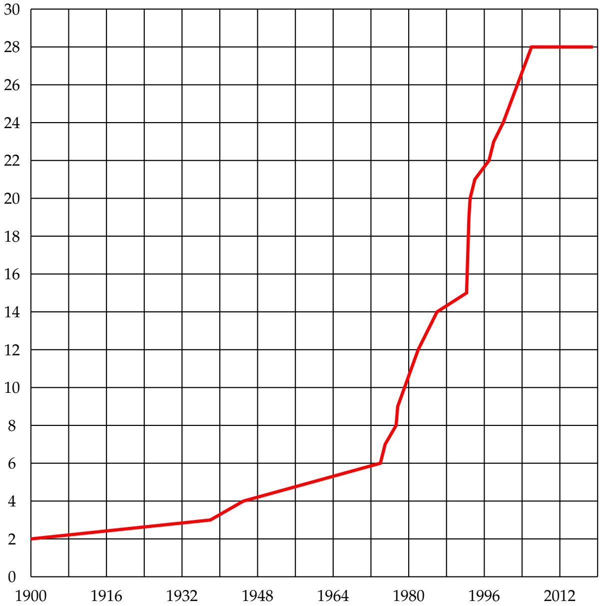


where $K_1, K_2, \ldots, K_n, \ldots$ are in some family of finite extensions of F, contained in some fixed algebraic closure $\overline{F}$. Or vary over all elliptic curves over all extensions $\{K_n\}$.

- Take the previous question and replace $\{E_n(K)\}$ with an object of interest, e.g. $r_K, E_n(K)_{\text{tors}}$, etc.

What are the possible ranks of elliptic curves $E/\mathbb{Q}$?

Rank	*Year*	*Due To*
3	1938	Billing
4	1945	Wiman
6	1974	Penney/Pomerance
7	1975	Penney/Pomerance
8	1977	Grunewald/Zimmert
9	1977	Brumer/Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao/Kouya
22	1997	Fermigier
23	1998	Martin/McMillen
24	2000	Martin/McMillen
28	2006	Elkies


30
28
26
24
22
20
18
16
14
12
10
8
6
4
2
0
1900
1916
1932
1948
1964
1980
1996
2012

Are the ranks of elliptic curves $E/\mathbb{Q}$ unbounded?

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of 'random' rational elliptic curves.

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of ‘random’ rational elliptic curves.

In particular, the p-adic Selmer group is modeled by the intersection between randomly chosen maximal isotropic subspaces in some large orthogonal spaces over $\mathbb{Z}_p$.

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of 'random' rational elliptic curves.

In particular, the p-adic Selmer group is modeled by the intersection between randomly chosen maximal isotropic subspaces in some large orthogonal spaces over $\mathbb{Z}_p$.

The model predicts…

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of 'random' rational elliptic curves.

In particular, the p-adic Selmer group is modeled by the intersection between randomly chosen maximal isotropic subspaces in some large orthogonal spaces over $\mathbb{Z}_p$.

The model predicts…

- rank $E(\mathbb{Q})$ is 0 or 1 each with density 50%.

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of 'random' rational elliptic curves.

In particular, the p-adic Selmer group is modeled by the intersection between randomly chosen maximal isotropic subspaces in some large orthogonal spaces over $\mathbb{Z}_p$.

The model predicts…

- rank $E(\mathbb{Q})$ is 0 or 1 each with density 50%.
- rank $E(\mathbb{Q}) \geq 2$ with density 0%.

Some Heuristics

New heuristics of Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood model the distribution of Selmer groups, Tate-Shafarevich groups, and Mordell-Weil groups of 'random' rational elliptic curves.

In particular, the p-adic Selmer group is modeled by the intersection between randomly chosen maximal isotropic subspaces in some large orthogonal spaces over $\mathbb{Z}_p$.

The model predicts…

- rank $E(\mathbb{Q})$ is 0 or 1 each with density 50%.
- rank $E(\mathbb{Q}) \geq 2$ with density 0%.
- Only finitely many elliptic curves over $\mathbb{Q}$ have rank ≥ 22.

What is the 'average' rank of elliptic curves $E/\mathbb{Q}$?

What does ‘average’ mean here?

$\mathcal{A}$:= Some property
S_n := set of objects up to size n.
A_n := set of objects in S with property $\mathcal{A}$ in S_n.

$$\mu(\mathcal{A}) = \lim_{n\to\infty} \frac{|A_n|}{|S_n|}$$

We need two things:

- A notion of 'size' for elliptic curves.
- A way of counting the number of elliptic curves up to a given 'size.'

Fact. Any elliptic curve $E/\mathbb{Q}$ is isomorphic to an elliptic curve of the form

$$E_{A,B} \colon y^2 = x^3 + Ax + B.$$

where $A, B \in \mathbb{Z}$.

Fact. Any elliptic curve $E/\mathbb{Q}$ is isomorphic to an elliptic curve of the form

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

where $A, B \in \mathbb{Z}$.

In fact, $E/\mathbb{Q}$ is isomorphic to a unique $E_{A,B}$ if we require that if $p^4 \mid A$ then $p^6 \nmid B$.

There are many notions of 'size' (a.k.a. complexity) of an elliptic curve $E_{A,B} := y^2 = x^3 + Ax + B$:

- Naïve Height: $H(E_{A,B}) := \max\{|A|^3, |B|^2\}$
- Falting's Height
- Discriminant, Δ_E: $\Delta(E_{A,B}) := -16(4A^3 + 27B^2)$
- Conductor, $N_E := \prod_{p \text{ prime}} p^{f_p(E)}$, where

$$f_p(E) = \begin{cases} 0, & E \text{ has good reduction at } p \\ 1, & E \text{ has multiplicative reduction at } p \\ 2, & E \text{ has additive reduction at } p \end{cases}$$

The naïve height can also be defined as $H(E_{A,B}) := \max\{4|A|^3, 27B^2\}$.

Advantage of Naïve Height

Let $\mathcal{E}_{H \leq X}$ denote the set of isomorphism classes of elliptic curves of (naïve) height at most X.

Advantage of Naïve Height

Let $\mathcal{E}_{H\leq X}$ denote the set of isomorphism classes of elliptic curves of (naïve) height at most X.

$$\#\mathcal{E}_{H\leq X} = 4\zeta(10)^{-1}X^{5/6} + O(X^{1/2})$$

Advantage of Naïve Height

Let $\mathcal{E}_{H\leq X}$ denote the set of isomorphism classes of elliptic curves of (naïve) height at most X.

$$\#\mathcal{E}_{H\leq X} = 4\zeta(10)^{-1}X^{5/6} + O(X^{1/2})$$

This essentially comes from the fact that there are $X^{1/3}$ choices for A and $X^{1/2}$ choices for B.

Advantage of Naïve Height

Let $\mathcal{E}_{H\leq X}$ denote the set of isomorphism classes of elliptic curves of (naïve) height at most X.

$$\#\mathcal{E}_{H\leq X} = 4\zeta(10)^{-1}X^{5/6} + O(X^{1/2})$$

This essentially comes from the fact that there are $X^{1/3}$ choices for A and $X^{1/2}$ choices for B.

It is conjectured that all the measures of heights give the same order of magnitude for all but a 'small' proportion of elliptic curves.

Conjecture (Goldfeld, Katz–Sarnak)

When ordered by height, the average rank of elliptic curves $E/\mathbb{Q}$ is $\frac{1}{2}$. More precisely, 50% of curves should have rank 0 and 50% of curves should have rank 1.

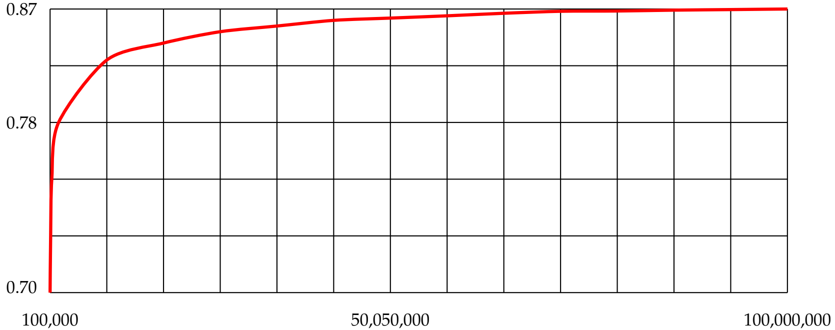
Dorian Goldfeld

Nick Katz

Peter Sarnak

Prior to the conjecture, the average rank was not even known to be finite!

COMPUTATIONS OF BRUMER, MCGUINNESS, BEKTEMIROV, STEIN, WATKINS



Average rank of elliptic curves of conductor $\leq 10^8$. The average turns out to be $0.8664\ldots$.

Previously Known Results

1992: Assuming BSD & GRH, Brumer showed the average rank is bounded (by 2.3).

Previously Known Results

1992: Assuming BSD & GRH, Brumer showed the average rank is bounded (by 2.3).

2004: Heath-Brown (assuming BSD, GRH) improved this average rank to ≤ 2.0

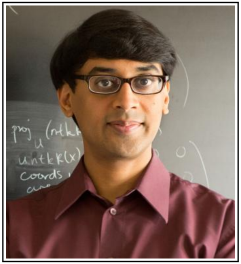
Previously Known Results

1992: Assuming BSD & GRH, Brumer showed the average rank is bounded (by 2.3).

2004: Heath-Brown (assuming BSD, GRH) improved this average rank to ≤ 2.0

2009: Young (assuming BSD, GRH) improved this to $\leq 25/14 \approx 1.786$.

Is there a proof of boundedness (with an estimate) without assuming BSD, GRH?



Manjul Bhargava

Arul Shankar

IDEA OF BHARGAVA-SHANKAR

We do not know how to compute $E(\mathbb{Q})$, so we study the 'simpler' group $E(\mathbb{Q})/nE(\mathbb{Q})$.

IDEA OF BHARGAVA-SHANKAR

We do not know how to compute $E(\mathbb{Q})$, so we study the 'simpler' group $E(\mathbb{Q})/nE(\mathbb{Q})$.

By the Mordell-Weil Theorem, we know that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

IDEA OF BHARGAVA-SHANKAR

We do not know how to compute $E(\mathbb{Q})$, so we study the 'simpler' group $E(\mathbb{Q})/nE(\mathbb{Q})$.

By the Mordell-Weil Theorem, we know that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

Then we must have

$$E(\mathbb{Q})/nE(\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^r \oplus E(\mathbb{Q})_{\text{tors}}/nE(\mathbb{Q})_{\text{tors}}$$

Idea of Bhargava-Shankar

If we knew $E(\mathbb{Q})/nE(\mathbb{Q})$ and $E(\mathbb{Q})_{\text{tors}}$, we could compute r.

Idea of Bhargava-Shankar

If we knew $E(\mathbb{Q})/nE(\mathbb{Q})$ and $E(\mathbb{Q})_{\text{tors}}$, we could compute r.

Example. If $n = p$, then

$$\dim_{\mathbb{F}_p} E(\mathbb{Q})/pE(\mathbb{Q}) = \dim_{\mathbb{F}_p} E(\mathbb{Q})[p] + \operatorname{rank} E(\mathbb{Q})$$

Define a computable group $S^n(E)$, called the Selmer group, containing $E(\mathbb{Q})/nE(\mathbb{Q})$.

Selmer & Shafarevich-Tate Groups

Define a computable group $S^n(E)$, called the Selmer group, containing $E(\mathbb{Q})/nE(\mathbb{Q})$.

Approximate $E(\mathbb{Q})/nE(\mathbb{Q})$ by $S^{(n)}(E)$. We define an 'error term' $Ш(E)$, called the Shafarevich-Tate group.

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow S^{(n)}(E) \longrightarrow Ш[n] \longrightarrow 0$$

Definition

Let $\varphi : E/K \to E'/K$ be an isogeny. The φ-Selmer group E/K is the subgroup of $H^1(G_{\overline{K}/K}, E[\varphi])$ defined by

$$S^{(\varphi)}(E/K) := \ker \left\{ H^1(G_{\overline{K}/K}, E[\varphi]) \longrightarrow \prod_{v \in M_K} \mathrm{WC}(E/K_v) \right\}$$

The Shafarevich-Tate group of E/K is the subgroup of $\mathrm{WC}(E/K)$ defined by

$$Ш(E/K) := \ker \left\{ \mathrm{WC}(E/K) \longrightarrow \prod_{v \in M_K} \mathrm{WC}(E/K_v) \right\}.$$

Idea of Bhargava-Shankar

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow S^{(n)}(E) \longrightarrow Ш[n] \longrightarrow 0$$

If $E(\mathbb{Q})[n] = \{\mathcal{O}\}$, then

$$n^{\operatorname{rank} E} \leq |S^{(n)}(E)|.$$

Idea of Bhargava-Shankar

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow S^{(n)}(E) \longrightarrow Ш[n] \longrightarrow 0$$

If $E(\mathbb{Q})[n] = \{\mathcal{O}\}$, then

$$n^{\operatorname{rank} E} \leq |S^{(n)}(E)|.$$

To prove boundedness of average rank, it is enough to show that the average size of $|S^{(n)}(E)|$ for any $n > 1$.

Outline of the Proof

1. For $n \leq 5$, construct a representation V of an algebraic group G defined over $\mathbb{Z}$ related to A, B.
2. Count the elements under the action of G on V with bounded A, B.
3. Sieve to count the elements of $S^{(n)}(E_{A,B})$ 'in' the representation.

Theorem (Bhargava–Shankar)

Let $n = 1, 2, 3, 4, 5$. When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average number of order n elements in the n-Selmer group is n.

Theorem (Bhargava–Shankar)

Let $n = 1, 2, 3, 4, 5$. When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average number of order n elements in the n-Selmer group is n.

Corollary

Let $n = 1, 2, 3, 4, 5$. When ordered by height, the average size of the n-Selmer group for elliptic curves $E/\mathbb{Q}$ is $\sigma(n)$.

Theorem (Bhargava–Shankar)

Let $n = 1, 2, 3, 4, 5$. When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average number of order n elements in the n-Selmer group is n.

Corollary

Let $n = 1, 2, 3, 4, 5$. When ordered by height, the average size of the n-Selmer group for elliptic curves $E/\mathbb{Q}$ is $\sigma(n)$.

Conjecture (Bhargava–Shankar)

Let $n \geq 1$. When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average size of the n-Selmer group is $\sigma(n)$.

Proposition (Bhargava–Shankar)

If the previous conjecture is true for all n, then when elliptic curves are ordered by height, a density of 100% of elliptic curves have rank 0 or 1.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is bounded (by $0.885 < 1$).

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbb{Q}$ are ordered by height, the average rank is bounded (by $0.885 < 1$).

Corollary

When elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion have rank 0.

Corollary

When elliptic curves $E/\mathbb{Q}$ are ordered by height, more than 80% have rank 0 or 1.

Theorem (Bhargava, Shankar, Skinner)

When elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion have rank 1.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion have analytic rank 0.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion have analytic rank 0.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion have analytic rank 1.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion have analytic rank 0.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion have analytic rank 1.

Corollary

A positive proportion of elliptic curves satisfy the BSD conjecture.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion have analytic rank 0.

Theorem (Bhargava–Shankar)

When elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion have analytic rank 1.

Corollary

A positive proportion of elliptic curves satisfy the BSD conjecture.

Theorem (Bhargava–Shankar–Zhang)

More than 66% of elliptic curves have analytic rank 0 or 1, and thus satisfy BSD.

What about Torsion?

Theorem (Levi-Ogg Conjecture; Mazur, 1977)

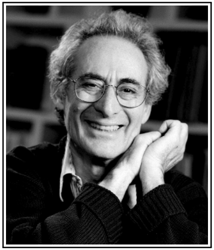
If $E/\mathbb{Q}$ is a rational elliptic curve, then the possible torsion subgroups $E(\mathbb{Q})_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 4 \end{cases}$$

Furthermore, each possibility occurs infinitely often.

Beppo Levi

Andrew Ogg



Barry Mazur

What about the groups $E(K)_{\textbf{tors}}$, where K is a number field of degree d?

With massive loss of generality, let $d = 2$

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

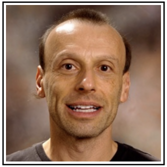
Let $K/\mathbb{Q}$ be a quadratic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 16, 18 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 6 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & n = 1, 2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \end{cases}$$

Moreover, each possibility occurs infinitely often.

Monsur Kenku

Fumiyuki Momose



Sheldon Kamienny

Theorem (Jeon,Kim,Schweizer, 2004; Etropolski-Morrow-Zureick Brown; Derickx, 2016)

Let $K/\mathbb{Q}$ be a cubic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 16, 18, 20, 21 \\ \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 7 \end{cases}$$

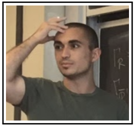
Each of these possibilities occurs infinitely many times except $\mathbb{Z}/21\mathbb{Z}$.

Jeon

Kim

Schweizer

Etropolski



Morrow

Z-B.

Derickx

Theorem (Jeon, Kim, Park, 2006)

Let $K/\mathbb{Q}$ be a quartic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 18, 20, 21, 22 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 9 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & n = 1, 2, 3 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & n = 1, 2 \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \end{cases}$$

Daeyeol Jeon

Chang Kim

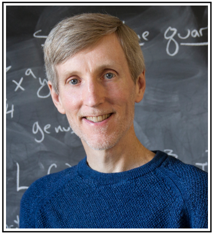
Eui-Sung Park

Theorem (Derickx, Sutherland, 2016)

Let $K/\mathbb{Q}$ be a quintic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, \ldots, 22, 24, 25 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 8 \end{cases}$$

Maarten Derickx



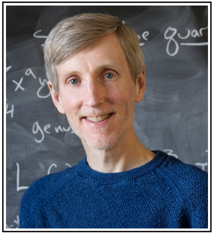
Drew Sutherland

Theorem (Derickx, Sutherland, 2016)

Let $K/\mathbb{Q}$ be a sextic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, \ldots, 30; n \neq 23, 25, 29 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 10 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & n = 1, \ldots, 4 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & n = 1, 2 \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \end{cases}$$

Maarten Derickx



Drew Sutherland

What about CM Elliptic Curves?

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

Let K be a number field of degree $d = 1, 2, \ldots, 13$ and E/K be an elliptic curve with CM. Then all possible torsion subgroups are given, and an algorithm to compute the list.

Pete Clark

Patrick Corn

Alex Rice

James Stankewicz

Theorem (Bourdon, Pollack; 2018)

Let K be an odd degree number field and E/K be an elliptic curve with CM. Then the torsion subgroups $E(K)_{tors}$ are computable.

Abbey Bourdon

Paul Pollack

What about Rational Elliptic Curves

Theorem (Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, Ogg, et al.)

If $E/\mathbb{Q}$ has an n-isogeny over $\mathbb{Q}$, then

$$n \in \{1, 2, \ldots, 19, 21, 25, 27, 37, 43, 67, 163\}.$$

If E does not have CM, then $n \leq 18$ or $n \in \{21, 25, 37\}$.

Theorem (Chou,Daniels,González-Jimenez,Lozano-Robledo,Najman,Tornero,et al.)

Let $\mathcal{C}_n$ denote the cyclic subgroup of order n. Then

$$\begin{aligned}
\Phi_{\mathbb{Q}}(2) &= \{\mathcal{C}_n : n = 1, 2, \ldots, 10, 12, 15, 16\} \\
&\qquad \cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} : 1, 2, \ldots, 6\} \cup \{\mathcal{C}_3 \oplus \mathcal{C}_3, \mathcal{C}_3 \oplus \mathcal{C}_6, \mathcal{C}_4 \oplus \mathcal{C}_4\} \\
\Phi_{\mathbb{Q}}(3) &= \{\mathcal{C}_n : n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21\} \\
&\qquad \cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} : n = 1, 2, 3, 4, 7\} \\
\Phi_{\mathbb{Q}}(4) &= \{\mathcal{C}_n : n = 12, \ldots, 10, 12, 13, 15, 16, 20, 24\} \\
&\qquad \cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} : n = 1, 2, \ldots, 6, 8\} \cup \{\mathcal{C}_3 \oplus \mathcal{C}_{3n} : n = 1, 2\} \\
&\qquad\quad \cup \{\mathcal{C}_4 \oplus \mathcal{C}_{4n} : n = 1, 2\} \cup \{\mathcal{C}_5 \oplus \mathcal{C}_5\} \cup \{\mathcal{C}_6 \oplus \mathcal{C}_6\} \\
\Phi_{\mathbb{Q}}(5) &= \{\mathcal{C}_n : n = 1, 2, \ldots, 12, 25\} \cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} : n = 1, 2, 3, 4\} \\
\Phi_{\mathbb{Q}}(6) &\supseteq \{\mathcal{C}_n : n = 1, 2, \ldots, 21, 30 : n \neq 11, 17, 19, 20\} \\
&\qquad \cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} : n = 1, 2, \ldots, 7, 9\} \\
&\qquad\quad \cup \{\mathcal{C}_3 \oplus \mathcal{C}_{3n} : n = 1, 2, 3, 4\} \cup \{\mathcal{C}_4 \oplus \mathcal{C}_4, \mathcal{C}_6 \oplus \mathcal{C}_6\}
\end{aligned}$$

$$\Phi_{\mathbb{Q}}(d^*) = \Phi_{\mathbb{Q}}(1)$$

Michael Chou

Harris Daniels

Enrique González-Jiménez

Álvaro Lozano-Robledo

Filip Najman

José Tornero

The Result for Nonic Galois Fields

Theorem (M.)

Let $K/\mathbb{Q}$ be a nonic Galois field, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 13, 14, 18, 19, 21, 27 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4, 7 \end{cases}$$

Theorem (M.)

Let $K/\mathbb{Q}$ *be a nonic Galois field with* $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$*, and let* $E/\mathbb{Q}$ *be a rational elliptic curve. Then the possible torsion subgroups* $E(K)_{tors}$ *are precisely:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4, 7 \end{cases}$$

Theorem (M.)

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ are:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 13^*, 18^*, 19, 21, 27 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4 \end{cases}$$

Outline of the Method

Step 1. Determine the Possible Prime Orders

Theorem (Lozano-Robledo)

Let $S_{\mathbb{Q}}(d)$ be the set of primes such that there exists an elliptic curve $E/\mathbb{Q}$ with a point of order p defined in an extension $K/\mathbb{Q}$ of degree at most d. Then $S_{\mathbb{Q}}(9) = \{2, 3, 5, 7, 11, 13, 17, 19\}$.

Álvaro Lozano-Robledo

Remark

Lozano-Robledo computes $S_{\mathbb{Q}}(d)$ for $1 \leq d \leq 21$, and gives a conjecturally formula valid for all $1 \leq d \leq 42$, following from a positive answer to Serre's uniformity question.

Proposition (González-Jiménez, Najman)

i $11 \in R_{\mathbb{Q}}(d)$ *if and only if* $5 \mid d$.

ii $13 \in R_{\mathbb{Q}}(d)$ *if and only if* $3 \mid d$ *or* $4 \mid d$.

iii $17 \in R_{\mathbb{Q}}(d)$ *if and only if* $8 \mid d$.

Enrique González-Jiménez

Filip Najman

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then if $P \in E(K)$ is a point of prime order p, then $p \in \{2, 3, 5, 7, 13, 19\}$.

Step 2. Bound the Size of the Sylow Subgroups

Lemma

Let $K/\mathbb{Q}$ be an odd degree number field, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain full p-torsion for all odd primes.

Lemma

Let $K/\mathbb{Q}$ be a Galois extension, and let $E/\mathbb{Q}$ be a rational elliptic curve. If $E(K)[n] \cong \mathbb{Z}/n\mathbb{Z}$, then E has a rational n-isogeny.

Theorem (Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, Ogg, et al.)

If $E/\mathbb{Q}$ has an n-isogeny over $\mathbb{Q}$, then

$$n \in \{1, 2, \ldots, 19, 21, 25, 27, 37, 43, 67, 163\}.$$

If E does not have CM, then $n \leq 18$ or $n \in \{21, 25, 37\}$.

Lemma

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then

$$E(K)[3^\infty] \subseteq \mathbb{Z}/27\mathbb{Z}$$
$$E(K)[5^\infty] \subseteq \mathbb{Z}/25\mathbb{Z}$$
$$E(K)[7^\infty] \subseteq \mathbb{Z}/7\mathbb{Z}$$
$$E(K)[13^\infty] \subseteq \mathbb{Z}/13\mathbb{Z}$$
$$E(K)[19^\infty] \subseteq \mathbb{Z}/19\mathbb{Z}$$

Theorem (Rouse,Zureick-Brown, 2015)

Let $E/\mathbb{Q}$ be a rational elliptic curve without CM. Then the index of $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ divides 64 or 96, and all such indices occur. Furthermore, the image of $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the inverse image in $\mathrm{GL}_2(\mathbb{Z}_2)$ of the image of $\rho_{E,32}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$.

Jeremy Rouse

David Zureick-Brown

Remark

They also enumerate all 1,208 possibilities and find their rational points.

Theorem (González-Jiménez, Lozano-Robledo)

Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $1 \leq s \leq N$ be fixed integers, and let $T \subseteq E[2^N]$ be a subgroup isomorphic to $\mathbb{Z}/2^s/Z \oplus \mathbb{Z}/2^N\mathbb{Z}$. Then $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by 2 if $s = N = 2$, and otherwise by $2^{2N+2s-8}$ if $N \geq 3$, unless $s \geq 4$ and $j(E)$ is one of the two values:

$$-\frac{3 \cdot 18249920^3}{17^{16}} \quad \text{or} \quad -\frac{7 \cdot 1723187806080^3}{79^{16}}$$

in which case $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $3 \cdot 2^{2N+2s-9}$. Moreover, this is best possible in that there are one-parameter families $E_{s,N}(t)$ of elliptic curves over $\mathbb{Q}$ such that for each $s, N \geq 0$ and each $t \in \mathbb{Q}$, and subgroups $T_{s,N} \in E_{s,N}(t)(\overline{\mathbb{Q}})$ isomorphic to $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$ such that $[\mathbb{Q}(T_{s,N}) : \mathbb{Q}]$ is equal to the bound given above.

Lemma

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then

$$E(K)_{tors} \subseteq (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}) \oplus \mathbb{Z}/27\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z} \oplus \mathbb{Z}/19\mathbb{Z}.$$

Step 3. Eliminate Possibilities

Lemma

Let $K/\mathbb{Q}$ be a nonic Galois field, and let $E/\mathbb{Q}$ be a rational elliptic curve. Let $P \in E(K)$ be a point of order p.

1. *If $p = 2, 3, 5$, then P is rational or defined over a cubic field.*
2. *If $p = 7, 13, 19$, then P is defined over a cubic field.*

Lemma (Najman)

Let p, q be distinct odd primes, F_2/F_1 a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$ and E/F_1 an elliptic curve with no p-torsion over F_1. Then if q does not divide $p-1$ and $\mathbb{Q}(\zeta_p) \not\subset F_2$, then $E(F_2)[p] = 0$.

Lemma (Najman)

Let p be an odd prime number, q a prime not dividing p, F_2/F_1 a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$, E/F_1 an elliptic curve, and suppose $E(F_1) \supset \mathbb{Z}/p\mathbb{Z}$, $E(F_1) \not\supset \mathbb{Z}/p^2\mathbb{Z}$, and $\zeta_p \notin F_2$. Then $E(F_2) \not\supset \mathbb{Z}/p^2\mathbb{Z}$.

Proposition (Najman)

Let K be a cubic field. Then the 5-Sylow groups of $E(\mathbb{Q})$ and $E(K)$ are equal.

Proposition (Najman)

Let K be a cubic field. Then the 5-Sylow groups of $E(\mathbb{Q})$ and $E(K)$ are equal.

Proposition (Najman)

If the torsion subgroup of an elliptic curve E over $\mathbb{Q}$ has a nontrivial 2-Sylow subgroup, then over any number field of odd degree the torsion of E will have the same 2-Sylow subgroup as over $\mathbb{Q}$.

Proposition (Najman)

Let K be a cubic field. Then the 5-Sylow groups of $E(\mathbb{Q})$ and $E(K)$ are equal.

Proposition (Najman)

If the torsion subgroup of an elliptic curve E over $\mathbb{Q}$ has a nontrivial 2-Sylow subgroup, then over any number field of odd degree the torsion of E will have the same 2-Sylow subgroup as over $\mathbb{Q}$.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Let F be cubic subfield of K. If the 2-Sylow subgroup of $E(F)_{tors}$ is nontrivial, then $E(K)[2^\infty] = E(F)[2^\infty]$.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/15\mathbb{Z}$.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/16\mathbb{Z}$.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/16\mathbb{Z}$.

Proof.

- We know $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ is not an option.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/16\mathbb{Z}$.

Proof.

- We know $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ is not an option.
- If $E(\mathbb{Q})[2^\infty] \neq \{\mathcal{O}\}$, then $E(\mathbb{Q})[2^\infty] \supseteq \mathbb{Z}/16\mathbb{Z}$.
- $E(K)[16] \cong \mathbb{Z}/16\mathbb{Z}$ so E has a 16-isogeny.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/16\mathbb{Z}$.

Proof.

- We know $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ is not an option.
- If $E(\mathbb{Q})[2^\infty] \neq \{\mathcal{O}\}$, then $E(\mathbb{Q})[2^\infty] \supseteq \mathbb{Z}/16\mathbb{Z}$.
- $E(K)[16] \cong \mathbb{Z}/16\mathbb{Z}$ so E has a 16-isogeny.
- Choose a model $E : y^2 = x^3 + Ax + B$.
- Then $\mathbb{Q}(x^3 + Ax + B) \subseteq K$ is a cubic field.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/16\mathbb{Z}$.

Proof.

- We know $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ is not an option.
- If $E(\mathbb{Q})[2^\infty] \neq \{\mathcal{O}\}$, then $E(\mathbb{Q})[2^\infty] \supseteq \mathbb{Z}/16\mathbb{Z}$.
- $E(K)[16] \cong \mathbb{Z}/16\mathbb{Z}$ so E has a 16-isogeny.
- Choose a model $E : y^2 = x^3 + Ax + B$.
- Then $\mathbb{Q}(x^3 + Ax + B) \subseteq K$ is a cubic field.
- We must have $\operatorname{disc} f(x) = \square$.

Proposition

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/16\mathbb{Z}$.

Proof.

- We know $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ is not an option.
- If $E(\mathbb{Q})[2^\infty] \neq \{\mathcal{O}\}$, then $E(\mathbb{Q})[2^\infty] \supseteq \mathbb{Z}/16\mathbb{Z}$.
- $E(K)[16] \cong \mathbb{Z}/16\mathbb{Z}$ so E has a 16-isogeny.
- Choose a model $E : y^2 = x^3 + Ax + B$.
- Then $\mathbb{Q}(x^3 + Ax + B) \subseteq K$ is a cubic field.
- We must have $\operatorname{disc} f(x) = \square$.
- $j = \dfrac{(h^8 - 16h^4 + 16)^3}{h^4(h^4 - 16)}$ for $h \in \mathbb{Q} \setminus \{0, \pm 2\}$.

For $h \in \mathbb{Q} \setminus \{0, \pm 2\}$, E must be

$$y^2 = x^3 - \frac{27(h^8 - 16h^4 + 16)^3}{(h^{12} - 24h^8 + 120h^4 + 64)^2} x + \frac{54(h^8 - 16h^4 + 16)^3}{(h^{12} - 24h^8 + 120h^4 + 64)^2}$$

For $h \in \mathbb{Q} \setminus \{0, \pm 2\}$, E must be

$$y^2 = x^3 - \frac{27(h^8 - 16h^4 + 16)^3}{(h^{12} - 24h^8 + 120h^4 + 64)^2}\, x + \frac{54(h^8 - 16h^4 + 16)^3}{(h^{12} - 24h^8 + 120h^4 + 64)^2}$$

Its discriminant must be a square, so

$$M^2 = \frac{136048896h^4(h^4 - 16)(h^8 - 16h^4 + 16)^6}{(h^{12} - 24h^8 + 120h^4 + 64)^6}$$

For $h \in \mathbb{Q} \setminus \{0, \pm 2\}$, E must be

$$y^2 = x^3 - \frac{27(h^8 - 16h^4 + 16)^3}{(h^{12} - 24h^8 + 120h^4 + 64)^2}\,x + \frac{54(h^8 - 16h^4 + 16)^3}{(h^{12} - 24h^8 + 120h^4 + 64)^2}$$

Its discriminant must be a square, so

$$M^2 = \frac{136048896h^4(h^4 - 16)(h^8 - 16h^4 + 16)^6}{(h^{12} - 24h^8 + 120h^4 + 64)^6}$$

Any solution is a subset of the rational points on the curve

$$X : y^2 = h^4 - 16$$

For $h \in \mathbb{Q} \setminus \{0, \pm 2\}$, E must be

$$y^2 = x^3 - \frac{27(h^8 - 16h^4 + 16)^3}{(h^{12} - 24h^8 + 120h^4 + 64)^2}\, x + \frac{54(h^8 - 16h^4 + 16)^3}{(h^{12} - 24h^8 + 120h^4 + 64)^2}$$

Its discriminant must be a square, so

$$M^2 = \frac{136048896h^4(h^4 - 16)(h^8 - 16h^4 + 16)^6}{(h^{12} - 24h^8 + 120h^4 + 64)^6}$$

Any solution is a subset of the rational points on the curve

$$X : y^2 = h^4 - 16$$

$X(\mathbb{Q}) = \{\mathcal{O}, (8, 24), (0, 8), (-4, 0), (0, -8), (8, -24)\}$, none of which are solutions.

Nonic Bicyclic Galois Fields

Theorem (Daniels, Lozano-Robledo, Najman, Sutherland, 2017)

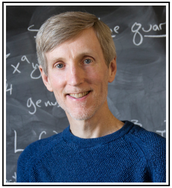
Let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(\mathbb{Q}(3^\infty))_{tors}$ is finite and is isomorphic to one of the following:

$$\begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1,2,4,5,7,8,13 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}4n\mathbb{Z}, & n = 1,2,4,7 \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6n\mathbb{Z}, & n = 1,2,3,5,7 \\ \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 4,6,7,9 \end{cases}$$


Harris Daniels


Álvaro Lozano-Robledo


Filip Najman


Drew Sutherland

Theorem (Najman)

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

$$E(F)_{tors} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, \ldots, 10, 12, 13, 14, 18, 21 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 4, 7 \end{cases}$$

Moreover, the elliptic curve 162B1 over $\mathbb{Q}(\zeta_9)^+$ is the unique rational elliptic curve over a cubic number field with torsion subgroup $\mathbb{Z}/21\mathbb{Z}$.

Filip Najman

Nonic Cyclic Galois Fields

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.
- Using division polynomials, it must be that $F = \mathbb{Q}(\zeta_7)^+$.

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.
- Using division polynomials, it must be that $F = \mathbb{Q}(\zeta_7)^+$.
- $F \subseteq K \subseteq \mathbb{Q}(\zeta_N)$ for some $N = 7^s m$.

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.
- Using division polynomials, it must be that $F = \mathbb{Q}(\zeta_7)^+$.
- $F \subseteq K \subseteq \mathbb{Q}(\zeta_N)$ for some $N = 7^s m$.
- $|(\mathbb{Z}/7^s\mathbb{Z})^\times| = 7^{s-1}(7-1) = 6 \cdot 7^{s-1} = 2 \cdot 3 \cdot 7^{s-1}$

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.
- Using division polynomials, it must be that $F = \mathbb{Q}(\zeta_7)^+$.
- $F \subseteq K \subseteq \mathbb{Q}(\zeta_N)$ for some $N = 7^s m$.
- $|(\mathbb{Z}/7^s\mathbb{Z})^\times| = 7^{s-1}(7-1) = 6 \cdot 7^{s-1} = 2 \cdot 3 \cdot 7^{s-1}$
- CRT produces $u \in \mathbb{N}$ with $\zeta_N \mapsto \zeta_N^u$ automorphism of K of order 3

Proposition

Let $K/\mathbb{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$, and let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$.

Proof (Sketch).

- Assume $K/F/\mathbb{Q}$ exists. Then $E(K)$ has a 14-isogeny.
- Then E has j-invariant $j = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$, so E must be the latter.
- Using division polynomials, it must be that $F = \mathbb{Q}(\zeta_7)^+$.
- $F \subseteq K \subseteq \mathbb{Q}(\zeta_N)$ for some $N = 7^s m$.
- $|(\mathbb{Z}/7^s\mathbb{Z})^\times| = 7^{s-1}(7-1) = 6 \cdot 7^{s-1} = 2 \cdot 3 \cdot 7^{s-1}$
- CRT produces $u \in \mathbb{N}$ with $\zeta_N \mapsto \zeta_N^u$ automorphism of K of order 3
- $\zeta_N \mapsto \zeta_N^u$ non-trivial in F, K, contradiction

□

Questions?