Torsion Subgroups of Elliptic Curves over (Nonic Galois) Number Fields

9th Annual Upstate Number Theory Conference

Caleb McWhorter
Syracuse University

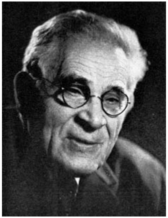
April 27, 2019

Theorem (Mordell, 1922)

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

$$E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus E(\mathbf{Q})_{tors},$$

where $r \geq 0$ is the rank and $E(\mathbf{Q})_{tors}$ is the set of points with finite order.

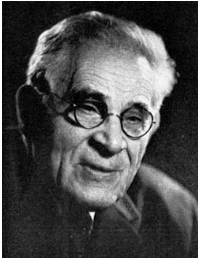


Louis J. Mordell
1888 – 1972

Theorem (Mordell-Weil-Néron, 1952)

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

$$A(F) \cong \mathbf{Z}^{r_{A/F}} \oplus A(F)_{tors}$$



Louis J. Mordell
1888 – 1972

André Weil
1906 – 1998

André Néron
1922 – 1985

Structure of the Torsion Subgroup

$$E(K)_{\text{tors}} \cong \mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/mn\mathbf{Z}$$

$$E[n] \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$$

Theorem (Levi-Ogg Conjecture; Mazur, 1977)

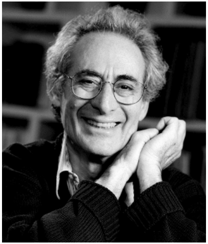
If $E/\mathbf{Q}$ is a rational elliptic curve, then $E(Q)_{tors}$ is isomorphic to one of the following:

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

Moreover, each possibility occurs infinitely often.

Beppo Levi
1875 – 1961

Andrew Ogg



Barry Mazur

Question

What torsion subgroups arise for elliptic curves E/K, where K is a number field of degree d?

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

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

Let $K/\mathbf{Q}$ be a quadratic number field and E/K be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to one of the following:

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

Moreover, each possibility occurs infinitely often.

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

Let $K/\mathbf{Q}$ be a cubic number field and E/K be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to one of the following:

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

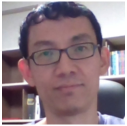
Each of these possibilities occurs infinitely many times except $\mathbf{Z}/21\mathbf{Z}$.

Theorem (Jeon, Kim, Park, 2006)

Let $K/\mathbf{Q}$ be a quartic number field and E/F an elliptic curve. If $E(K)_{tors}$ appears infinitely often, then $E(K)_{tors}$ is isomorphic to one of the following

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

Daeyeol Jeon



Chang Kim

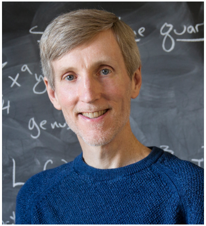
Eui-Sung Park

Theorem (Derickx, Sutherland, 2016)

Let $K/\mathbf{Q}$ be a quintic number field and E/K an elliptic curve. Then if $E(K)_{tors}$ appears infinitely often it must be isomorphic to one of the following:

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

Maarten Derickx

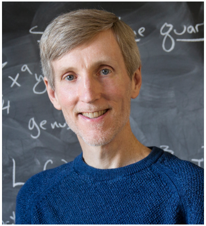


Drew Sutherland

Theorem (Derickx, Sutherland, 2016)

Let $K/\mathbf{Q}$ be a sextic number field and E/K an elliptic curve. If $E(K)_{tors}$ occurs infinitely often, then it must be isomorphic to one of the following:

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



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

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

What about you restrict to rational elliptic curves?

Definition (Isogeny)

Let E_1, E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism $\phi : E_1 \to E_2$ with $\phi(\mathcal{O}) = \mathcal{O}$. If $|\ker \phi| = n$, we say ϕ is an n-isogeny.

Definition (Isogeny)

Let E_1, E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism $\phi : E_1 \to E_2$ with $\phi(\mathcal{O}) = \mathcal{O}$. If $|\ker \phi| = n$, we say ϕ is an n-isogeny.

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

If $E/\mathbf{Q}$ has an n-isogeny over $\mathbf{Q}$, 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 $n \in \{21, 25, 37\}$.

In 2015, Jeremy Rouse and David-Zureick-Brown classified all possible 2-adic images of Galois representations attached to elliptic curves $E/\mathbf{Q}$. In particular, the index of $\rho_{E,2^\infty}(G_{\mathbf{Q}})$ divides 64 or 96. They also enumerate all 1,208 possibilities and find their rational points.

A bit of notation

$$\Phi_{\mathbf{Q}}(d) := \{\text{Set of Iso. Classes of } E(K)_{\text{tors}} \colon E_{\mathbf{Q}}(K), [K \colon \mathbf{Q}] = d\}$$

$$\Phi_{\mathbf{Q}}(d) := \{\text{Set of Iso. Classes of } E(K)_{\text{tors}} \colon E_{\mathbf{Q}}(K), [K \colon \mathbf{Q}] = d\}$$

$$S_{\mathbf{Q}}(d) := \{p \text{ prime} \colon \exists\, E_{\mathbf{Q}}(K), p \text{ divides } |E_{\mathbf{Q}}(K)|_{\text{tors}}, [K \colon \mathbf{Q}] \leq d\}$$

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

$$\Phi_{\mathbf{Q}}(2) = \begin{cases} \mathbf{Z}/n\mathbf{Z}, & n = 1, \ldots, 10, 12, 15, 16 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2n\mathbf{Z}, & n = 1, \ldots, 6 \end{cases}$$

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

$$\Phi_{\mathbf{Q}}(4) = \begin{cases} \mathbf{Z}/n\mathbf{Z}, & n = 1, \ldots, 10, 12, 13, 15, 16, 20, 24 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2n\mathbf{Z}, & n = 1, \ldots, 6, 8 \\ \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3n\mathbf{Z}, & n = 1, 2 \\ \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4n\mathbf{Z}, & n = 1, 2 \\ \mathbf{Z}/5\mathbf{Z} \oplus \mathbf{Z}/5\mathbf{Z}, \mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z} & \end{cases}$$

$$\Phi_{\mathbf{Q}}(5) = \begin{cases} \mathbf{Z}/n\mathbf{Z}, & n = 1, \ldots, 12, 25 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2n\mathbf{Z}, & n = 1, \ldots, 4 \end{cases}$$

Theorem (Najman)

Let $E/\mathbf{Q}$ be an elliptic curve and $K/\mathbf{Q}$ a cubic number field. Then

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

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

Filip Najman

Theorem (Mazur, Parent, Derickx, Kammienny, Stein, Stoll, Lozano-Robledo, et al.)

$$\begin{aligned} S_{\mathbf{Q}}(\{1,2\}) &= \{2,3,5,7\} \\ S_{\mathbf{Q}}(\{3,4\}) &= \{2,3,5,7,13\} \\ S_{\mathbf{Q}}(\{5,6,7\}) &= \{2,3,5,7,11,13\} \\ S_{\mathbf{Q}}(8) &= \{2,3,5,7,11,13,17\} \\ S_{\mathbf{Q}}(\{9,10,11\}) &= \{2,3,5,7,11,13,17,19\} \\ S_{\mathbf{Q}}(\{12,\ldots,20\}) &= \{2,3,5,7,11,13,17,19,37\} \\ S_{\mathbf{Q}}(21) &= \{2,3,5,7,11,13,17,19,37,43\} \end{aligned}$$

There is a conjectural formula for $S_{\mathbf{Q}}(d)$ for all $d \geq 1$ which is valid for all $1 \leq d \leq 42$, and follows from a positive answer to Serre's uniformity conjecture.

What about other cases?

(Nonic) Galois Case

Theorem

Let $K/\mathbf{Q}$ be a nonic Galois field and $E/\mathbf{Q}$ be an elliptic curve. Then $E_{\mathbf{Q}}(K)_{tors}$ is isomorphic to one of the following groups:

$$\begin{cases} \mathbf{Z}/n\mathbf{Z} & n = 1, 2, \ldots, 10, 12, 13, 14, \ldots, 18^*, 19, \underline{21}, 27 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2n\mathbf{Z} & n = 1, 2, 3, 4, 7, 9^* \end{cases}$$

Theorem

Let $K/\mathbf{Q}$ be a nonic Galois field with $\mathrm{Gal}(K/Q) \cong \mathbf{Z}/9\mathbf{Z}$ *and* $E/\mathbf{Q}$ *be an elliptic curve. Then* $E_{\mathbf{Q}}(K)_{tors}$ *is isomorphic to one of the following groups:*

$$\begin{cases} \mathbf{Z}/n\mathbf{Z} & n = 1, 2, \ldots, 10, 12, 13^*, 14^*, 18^*, 19, 21, 27 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2n\mathbf{Z} & n = 1, 2, 3, 4, 7^*, 9^* \end{cases}$$

Theorem

Let $K/\mathbf{Q}$ *be a nonic Galois field with* $\mathrm{Gal}(K/Q) \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ *and* $E/\mathbf{Q}$ *be an elliptic curve. Then* $E_{\mathbf{Q}}(K)_{tors}$ *is isomorphic to one of the following groups:*

$$\begin{cases} \mathbf{Z}/n\mathbf{Z} & n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2n\mathbf{Z} & n = 1, 2, 3, 4, 7, 9^* \end{cases}$$

$E(K)_{\mathrm{tors}}$	$[a_1, a_2, a_3, a_4, a_6]$	K
$\mathbf{Z}/19\mathbf{Z}$	$[0, 0, 1, -38, 90]$	$\mathbf{Q}(\zeta_{19})^+$
$\mathbf{Z}/27\mathbf{Z}$	$[0, 0, 1, -30, 63]$	$\mathbf{Q}(\zeta_{27})^+$

Proposition (Lozano-Robledo)

Let $K/\mathbf{Q}$ *be a nonic field and* $E/\mathbf{Q}$ *an elliptic curve. Then the only possible prime order points are* $2, 3, 5, 7, 11, 13, 17, 19$.

Proposition (González-Jiménez, Najman)

Let $K/\mathbf{Q}$ be a number field of degree d and $E/\mathbf{Q}$ be an elliptic curve. Then $E(K)$ contains a point of order 11 if and only if $5 \mid d$ and contains a point of order 17 if and only if $8 \mid d$.

Lemma

Let $K/\mathbf{Q}$ be an odd degree number field and $E/\mathbf{Q}$ an elliptic curve. Then $E(K)[n] \cong \mathbf{Z}/n\mathbf{Z}$ for $n > 2$.

Proof. If $E(K)[n] \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$, then the Weil pairing forces $\mathbf{Q}(\zeta_n) \subseteq K$. But then

$$[K\colon \mathbf{Q}] = [K\colon \mathbf{Q}(\zeta_n)]\,[\mathbf{Q}(\zeta_n)\colon \mathbf{Q}] = \phi(n)\,[K\colon \mathbf{Q}(\zeta_n)].$$

But $\phi(n)$ is even for $n > 2$. □

Lemma

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

Proof. Choose a $\mathbf{Z}/n\mathbf{Z}$ basis for $E[n]$, say $\{P, Q\}$. Without loss of generality, assume $P \in E(K)$ and $Q \notin E(K)$. If $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/Q)$, then $P^\sigma \in \langle P \rangle$. But then $\langle P \rangle$ is Galois-stable so that E has an n-isogeny over $\mathbf{Q}$. $\square$

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

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

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

Lemma

If $K/\mathbf{Q}$ is an odd degree number field and $E/\mathbf{Q}$ an elliptic curve. If $E(\mathbf{Q})$ contains a point of order 2, then the 2-Sylow subgroups of $E(K)$ and $E(\mathbf{Q})$ are equal.

Proof. The field K cannot contain any points of order 2 which are not defined over $\mathbf{Q}$ because any such points are contained in a quadratic field and K has odd degree. If the Sylow 2-subgroups of $E(K)$ and $E(\mathbf{Q})$ were not equal, there would be a K-rational point, say P, which was not $\mathbf{Q}$-rational but $2P = Q$, where Q is a $\mathbf{Q}$-rational point with order a power of 2. The equation $2P = Q$ has 4 solutions. However, the orbit from the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ must have length 2 or 4. But as $K/\mathbf{Q}$ has odd degree, this is impossible. $\square$

Lemma

Let $K/\mathbf{Q}$ be a nonic field and $E/\mathbf{Q}$ be an elliptic curve. If P is a point of order 3, 7, or 13, then $P \in E(\mathbf{Q})$ or $P \in E(K)$, where K is a cubic field. Furthermore, if P has order 5, then $P \in E(\mathbf{Q})$. In particular, the Sylow 5-subgroups of $E(K)_{tors}$ and $E(\mathbf{Q})_{tors}$ are equal.

Questions?