Torsion of Elliptic Curves over Number Fields of Small Degree

BUGCAT 2018

Caleb McWhorter
Syracuse University

October 14, 2018

Definition (Elliptic Curve)

An elliptic curve is a nonsingular projective curve of genus one.

Definition (Elliptic Curve)

An elliptic curve is an abelian variety of dimension one.

Definition (Elliptic Curve)

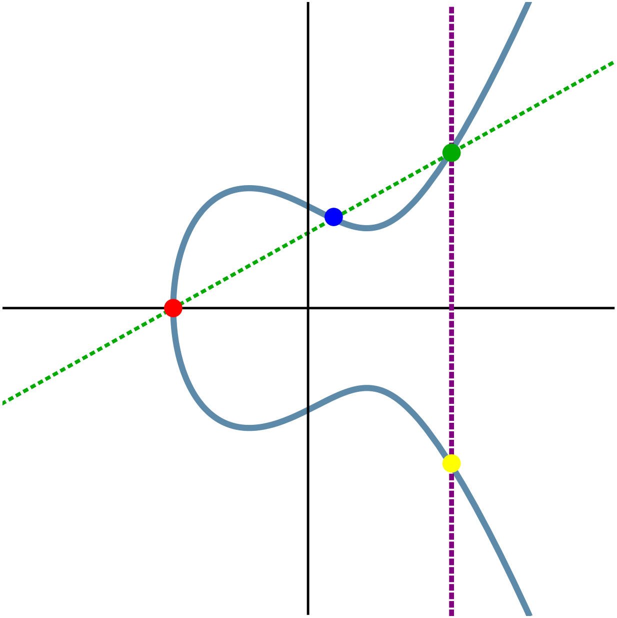
An elliptic curve is a nonempty smooth variety $V(F)$, where $\deg F = 3$.

Definition (Elliptic Curve)

An elliptic curve is a compact Riemann surface of genus 1.

Definition (Elliptic Curve)

An elliptic curve is the set of points
$\{(x, y) \colon y^2 = x^3 + Ax + B, -(4A^3 + 27B^2) \neq 0\}$.



Theorem (Mordell-Weil-Néron; 1922, 1928,1954)

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

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

Question

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

Let L/K be an extension of fields.

$$E_K(L) := \{y^2 = x^3 + Ax + B \colon x, y \in L, A, B \in K, -(4A^3 + 27B^2) \neq 0\}$$

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

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

Theorem (Levi-Ogg Conjecture; Mazur, 1977)

Let $E/\mathbf{Q}$ be an elliptic curve. Then $E(\mathbf{Q})_{tors}$ is one of the following:

$$\begin{cases} \mathbf{Z}/n\mathbf{Z}, & n = 1, 2, \ldots, 10, 12 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2n\mathbf{Z}, & n = 1, 2, 3, 4 \end{cases}$$

Moreover, possibility occurs infinitely many times.

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

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

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

Moreover, each possibility occurs infinitely many times.

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

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

$$\begin{cases} \mathbf{Z}/n\mathbf{Z}, & n = 1, 2, \ldots, 20, n \neq 17, 19 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2n\mathbf{Z}, & n = 1, 2, \ldots, 7 \end{cases}$$

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

If $K/\mathbf{Q}$ is a number field of degree d, the torsion subgroups $E(K)_{\mathrm{tors}}$ which occur infinitely often are known when…

- $d = 4$, 2006: Jeon, Kim, Park

If $K/\mathbf{Q}$ is a number field of degree d, the torsion subgroups $E(K)_{\mathrm{tors}}$ which occur infinitely often are known when…

- $d = 4$, 2006: Jeon, Kim, Park
- $d = 5$, 2016: Derickx, Sutherland

If $K/\mathbf{Q}$ is a number field of degree d, the torsion subgroups $E(K)_{\text{tors}}$ which occur infinitely often are known when…

- $d = 4$, 2006: Jeon, Kim, Park
- $d = 5$, 2016: Derickx, Sutherland
- $d = 6$, 2016: Derickx, Sutherland

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 $d \geq 1$.

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 $d \geq 1$.

Theorem (Bourdon, Clark; 2017)

Give a best possible constant T such that if $E(L)_{tors}$ has a point of order $N \geq 2$, then $T \mid [L : K(j(E))]$, where K is a quadratic imaginary field, L/K, and E/L has CM by an order $\mathcal{O} \subseteq K$.

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

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

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

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

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

Theorem (C.M.)

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

$$\begin{cases} \mathbf{Z}/n\mathbf{Z}, & n = 1, 2, \ldots, 21, 25, 27 \\ \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/2n\mathbf{Z}, & n = 1, 2, \ldots, 9 \end{cases}$$

Idea of the Proof

- Find the possible prime power orders,

Idea of the Proof

- Find the possible prime power orders, i.e. bound the Sylow subgroups.

Idea of the Proof

- Find the possible prime power orders, i.e. bound the Sylow subgroups.
- Eliminate cases by use of Weil pairing, isogenies, and Galois representations.

Galois Representations

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

Galois Representations

- $E[m] \cong \mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}$
- If $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then

$$[m](P^\sigma) = ([m]P)^\sigma = \mathcal{O}^\sigma = \mathcal{O}$$

Galois Representations

- $E[m] \cong \mathbf{Z}\,/\,m\mathbf{Z} \oplus \mathbf{Z}\,/\,m\mathbf{Z}$

- If $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then

$$[m](P^\sigma) = ([m]P)^\sigma = \mathcal{O}^\sigma = \mathcal{O}$$

- $\overline{\rho}_{E,n} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(E[n])$

Galois Representations

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

- If $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then

$$[m](P^\sigma) = ([m]P)^\sigma = \mathcal{O}^\sigma = \mathcal{O}$$

- $\overline{\rho}_{E,n} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2\,(\mathbf{Z} / n\mathbf{Z})$

Galois Representations

- $E[m] \cong \mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}$
- If $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then

$$[m](P^\sigma) = ([m]P)^\sigma = \mathcal{O}^\sigma = \mathcal{O}$$

- $\overline{\rho}_{E,n} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$

Possible images and indices of Galois representations are limited by the work of Zureick-Brown, Zywina, Clark, Rouse, Corn, Rice, Stankewicz, et al.

Proposition

$$E_{\mathbf{Q}}(K)[7^{\infty}] \subseteq \mathbf{Z}/7\mathbf{Z}$$

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 $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$. If E does not have CM, then $n \leq 18$ or $n \in \{21, 25, 37\}$.

Lemma

Let $K/\mathbf{Q}$ be a number field of odd degree. Then $E(K)_{tors}$ cannot contain full n-torsion for $n > 2$.

Lemma

Let $K/\mathbf{Q}$ be a number field of odd degree. Then $E(K)_{tors}$ cannot contain full n-torsion for $n > 2$.

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

Lemma

Let $K/\mathbf{Q}$ be a number field of odd degree. Then $E(K)_{tors}$ cannot contain full n-torsion for $n > 2$.

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

$$\begin{aligned}[K\colon \mathbf{Q}(\zeta_n)]\,[\mathbf{Q}(\zeta_n)\colon \mathbf{Q}] &= [K\colon \mathbf{Q}] \\ [K\colon \mathbf{Q}(\zeta_n)]\phi(n) &= [K\colon \mathbf{Q}]\end{aligned}$$

Lemma

Let $K/\mathbf{Q}$ be a number field of odd degree. Then $E(K)_{tors}$ cannot contain full n-torsion for $n > 2$.

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

$$\begin{aligned}[K\colon \mathbf{Q}(\zeta_n)]\,[\mathbf{Q}(\zeta_n)\colon \mathbf{Q}] &= [K\colon \mathbf{Q}] \\ [K\colon \mathbf{Q}(\zeta_n)]\phi(n) &= [K\colon \mathbf{Q}]\end{aligned}$$

but $\phi(n)$ is even for $n > 2$, a contradiction. □

Proposition

$$E_{\mathbf{Q}}(K)[7^\infty] \subseteq \mathbf{Z}/7\mathbf{Z}$$

Proof.

Proposition

$$E_{\mathbf{Q}}(K)[7^\infty] \subseteq \mathbf{Z}/7\mathbf{Z}$$

Proof.

- By the Lemma, $E_{\mathbf{Q}}(K)$ cannot contain full 7-torsion. Therefore, $\mathrm{Syl}_7(E_{\mathbf{Q}}(K)) \subseteq \mathbf{Z}/7^k\mathbf{Z}$ for some k.

Proposition

$$E_{\mathbf{Q}}(K)[7^{\infty}] \subseteq \mathbf{Z}/7\mathbf{Z}$$

Proof.

- By the Lemma, $E_{\mathbf{Q}}(K)$ cannot contain full 7-torsion. Therefore, $\mathrm{Syl}_7(E_{\mathbf{Q}}(K)) \subseteq \mathbf{Z}/7^k\mathbf{Z}$ for some k.
- If $k > 1$, then $E_{\mathbf{Q}}(K)$ contains a rational 7^k-isogeny, which is not possible for $k > 1$. Therefore, $k = 1$.

$\square$

Questions?