Torsion of Rational Elliptic Curves over Nonic Galois Fields

Syracuse University
43rd Annual New York State Regional Graduate Mathematics Conferece

Caleb McWhorter

March 24, 2018

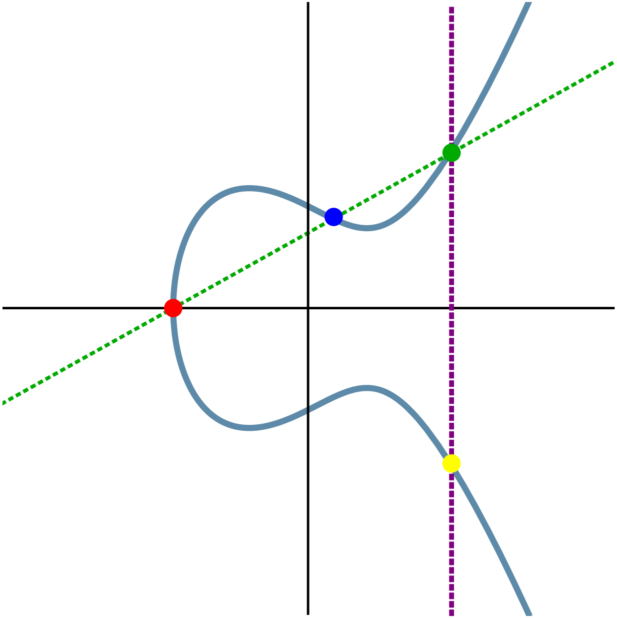
Definition (Elliptic Curve)

An elliptic curve is a nonsingular curve of genus one with a distinguished point, denoted $\mathcal{O}$.

Definition (Elliptic Curve)

An elliptic curve is a nonsingular curve of genus one with a distinguished point, denoted $\mathcal{O}$.

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



Theorem (Mordell-Weil)

For any abelian variety A over a number field K, $A(K)$ is a finitely generated abelian group, i.e.

$$A(K) \cong \mathbf{Z}^r \oplus \mathrm{Tor}(A(K))$$

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

$$E[m] \cong {}^{\mathbf{Z}}\!/_{m\mathbf{Z}} \oplus {}^{\mathbf{Z}}\!/_{m\mathbf{Z}}$$

Theorem (Merel, 1994)

For all $d \in \mathbf{Z}_+$*, there exists a constant* $B(d) \geq 0$ *such that for all elliptic curves* E *over a number field* K *with* $[K\colon \mathbf{Q}] = d$*, then*

$$|E(K)_{tors}| \leq B(d).$$

Theorem (Merel, 1994)

Let E/K be an elliptic curve with $[K\colon \mathbf{Q}] = d > 1$ and p be prime. If $E(K)$ has a p-torsion point, then $p < d^{3d^2}$.

Theorem (Merel, 1994)

Let E/K be an elliptic curve with $[K\colon \mathbf{Q}] = d > 1$ and p be prime. If $E(K)$ has a p-torsion point, then $p < d^{3d^2}$.

This was later improved by Oesterlé to $(3^{d/2} + 1)^2$. In the case over $\mathbf{Q}$, Lozano-Robledo improves this to $2d + 1$, $p \geq 11$ and $p \neq 13, 37$.

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

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

$$S_{\mathbf{Q}}(d) \subset S(d)$$

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

$$S_{\mathbf{Q}}(9) = \{2, 3, 5, 7, 11, 13, 17, 19\}$$
$$S_{\mathbf{Q}}(21) = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43\}$$

$$\Phi(d) := \{\text{Set of Isomorphism Classes of } E(K)_{\text{tors}} \colon [K \colon \mathbf{Q}] = d\}$$

$$\Phi(d) := \{\text{Set of Isomorphism Classes of } E(K)_{\text{tors}} \colon [K \colon \mathbf{Q}] = d\}$$

$$\Phi_{\mathbf{Q}}(d) \subseteq \Phi(d)$$

Theorem (Mazur)

$\Phi(1) = \{C_n : n = 1, \ldots, 10, 12\} \cup \{C_2 \times C_{2n} : n = 1, \ldots, 4\}$

Theorem (Najman, González-Jiménez, et al.)

$$\Phi_{\mathbf{Q}}(2) = \{C_n \colon n = 1, \ldots, 10, 12, 15, 16\} \cup \{C_2 \times C_{2n} \colon n = 1, \ldots, 6\}$$

$$\Phi_{\mathbf{Q}}(3) = \{C_n \colon 1, \ldots, 10, 12, 13, 14, 18, 21\} \cup \{C_2 \times C_{2n} \colon n, 1, 2, 3, 4, 7\}$$

$$\Phi_{\mathbf{Q}}(4) = \{C_n \colon n = 1, \ldots, 10, 12, 13, 15, 16, 20, 24\} \cup \{C_2 \times 2_{2n} \colon n = 1, \ldots, 6, 8\} \cup \{C_3 \times C_{3n} \colon n = 1, 2\} \cup \{C_4 \times C_{4n} \colon n = 1, 2\} \cup \{C_5 \times C_5\} \cup \{C_6 \times C_6\}$$

$$\Phi_{\mathbf{Q}}(5) = \{C_n \colon n = 1, \ldots, 12, 25\} \cup \{C_2 \times C_{2n} \colon n = 1, \ldots, 4\}$$

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 $\phi(\mathcal{O}) = \mathcal{O}$.

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* $n \in \{21, 25, 37\}$*.*

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

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

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

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

Definition (Weil Pairing)

If E/K be an elliptic curve and $m \geq 2$, then there exists a bilinear, nondegenerate, alternating, Galois invariant pairing on $E[m]$.

Idea

Bound the torsion subgroup (by some large sum of Sylow subgroups), then eliminate cases by isogeny, Galois representations, and the Weil pairing.

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. □

Now K cannot contain full 7-torsion so that $E(K)[7^\infty] = \mathbf{Z}\,/\,7^m\mathbf{Z}$. In particular, $E/\mathbf{Q}$ has a 7^k-isogeny. But $7^k \geq 49$ for $k > 1$, which is not a possible isogeny. Therefore,

$$E(K)[7^\infty] \subseteq {}^{\mathbf{Z}}\!/_{7\mathbf{Z}}$$

Theorem

If $K/\mathbf{Q}$ is a Galois extension of degree 9 and $E/\mathbf{Q}$ is an elliptic curve, then

$$E(K)_{tors} \subseteq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6983776800\mathbf{Z}$$

Furthermore, there are at most 34 possibilities for $E(K)_{tors}$.