Torsion for CM Elliptic Curves Defined over Number Fields of Degree $2p$

Holly Paige Chaos (Wake Forest University)

June 13, 2020

Introduction

Classical Question: Given a polynomial equation, what are the rational solutions?

Introduction

Classical Question: Given a polynomial equation, what are the rational solutions?

$$y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Q}$$

Introduction

Classical Question: Given a polynomial equation, what are the rational solutions?

$$y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Q}$$

$E =$ elliptic curve / $\mathbb{Q}$

Introduction

Classical Question: Given a polynomial equation, what are the rational solutions?

$$y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Q}$$

$E =$ elliptic curve / $\mathbb{Q}$

Theorem (Mordell)

$E(\mathbb{Q})$ is a finitely generated abelian group.

$$E(\mathbb{Q}) \cong E(\mathbb{Q})[\text{tors}] \times \mathbb{Z}^r$$

Question: Which finite groups arise?

Question: Which finite groups arise?

Theorem (Mazur, 1977)

For $E/\mathbb{Q}$*,* $E(\mathbb{Q})[\text{tors}]$ *is isomorphic to*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 10 \text{ or } m = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 4 \end{array}$$

Question: Which finite groups arise?

Theorem (Mazur, 1977)

For $E/\mathbb{Q}$, $E(\mathbb{Q})[\text{tors}]$ *is isomorphic to*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 10 \text{ or } m = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 4 \end{array}$$

Theorem (Kamienny-Kenku-Momose)

Let F *be a quadratic field. For* E/F *the group* $E(F)[\text{tors}]$ *is isomorphic to*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 18,\ m \neq 17 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 6 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} & 1 \leq m \leq 2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \end{array}$$

Question

Consider all number fields F of degree d and all E/F. What $E(F)[\text{tors}]$ arise?

Question

Consider all number fields F of degree d and all E/F. What $E(F)[\text{tors}]$ arise?

Theorem (Merel, 1996)

If E is an elliptic curve defined over a number field F of degree d,

$$\#E(F)[\text{tors}] \leq C(d).$$

Question

Consider all number fields F of degree d and all E/F. What $E(F)[\text{tors}]$ arise?

Theorem (Merel, 1996)

If E is an elliptic curve defined over a number field F of degree d,

$$\#E(F)[\text{tors}] \leq C(d).$$

$[F : \mathbb{Q}] = d$: Only finitely many groups arise.

CM Elliptic Curves

For most elliptic curves, $\mathrm{End}_{\bar{F}}(E) \cong \mathbb{Z}$.

- Usual endomorphisms: $P \mapsto [n]P$, $n \in \mathbb{Z}$.

CM Elliptic Curves

For most elliptic curves, $\mathrm{End}_{\bar{F}}(E) \cong \mathbb{Z}$.

- Usual endomorphisms: $P \mapsto [n]P$, $n \in \mathbb{Z}$.

For elliptic curves with complex multiplication (CM), $\mathrm{End}_{\bar{F}}(E) \cong \mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$.

CM Elliptic Curves

For most elliptic curves, $\text{End}_{\bar{F}}(E) \cong \mathbb{Z}$.

- Usual endomorphisms: $P \mapsto [n]P$, $n \in \mathbb{Z}$.

For elliptic curves with complex multiplication (CM), $\text{End}_{\bar{F}}(E) \cong \mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$.

- The elliptic curve $y^2 = x^3 + 1$ has CM by the maximal order in $\mathbb{Q}(\sqrt{-3})$.
- Extra endomorphism:

$$(x, y) \mapsto \left(\frac{-1 + \sqrt{-3}}{2} x, y \right)$$

Torsion on CM Elliptic Curves

Theorem (Olson, 1974)

Let $E/\mathbb{Q}$ be a CM elliptic curve. Then $E(\mathbb{Q})[\text{tors}]$ is isomorphic to one of the following 6 groups:

$$\{\cdot\}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Torsion on CM Elliptic Curves

Theorem (Olson, 1974)

Let $E/\mathbb{Q}$ be a CM elliptic curve. Then $E(\mathbb{Q})[\mathrm{tors}]$ is isomorphic to one of the following 6 groups:

$$\{\cdot\}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

- $[F : \mathbb{Q}] \leq 13$: Clark, Corn, Rice, Stankewicz, 2014.

Torsion on CM Elliptic Curves

Theorem (Olson, 1974)

Let $E/\mathbb{Q}$ be a CM elliptic curve. Then $E(\mathbb{Q})[\text{tors}]$ is isomorphic to one of the following 6 groups:

$$\{\cdot\}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

- $[F : \mathbb{Q}] \leq 13$: Clark, Corn, Rice, Stankewicz, 2014.
- $[F : \mathbb{Q}] = p$ or p^2: Bourdon, Clark, Stankewicz, 2015.

Torsion on CM Elliptic Curves

Theorem (Olson, 1974)

Let $E/\mathbb{Q}$ be a CM elliptic curve. Then $E(\mathbb{Q})[\text{tors}]$ is isomorphic to one of the following 6 groups:

$$\{\cdot\}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

- $[F : \mathbb{Q}] \leq 13$: Clark, Corn, Rice, Stankewicz, 2014.
- $[F : \mathbb{Q}] = p$ or p^2: Bourdon, Clark, Stankewicz, 2015.
- $[F : \mathbb{Q}]$ odd : Bourdon, Pollack, 2017.

What happens when E is defined over a number field of degree 14?

What happens when E is defined over a number field of degree 14?

Theorem (C., 2019)

Let F be a number field of degree 14. Let E/F be a CM elliptic curve. For E/F the group $E(F)[\text{tors}]$ is isomorphic to one of the following:

$\mathbb{Z}/m\mathbb{Z}$	$1 \leq m \leq 4$ *or* $m = 6, 7, 10, 29, 43, 49, 53$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$	$1 \leq m \leq 3$
$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$	

What happens when E is defined over a number field of degree 14?

Theorem (C., 2019)

Let F be a number field of degree 14. Let E/F be a CM elliptic curve. For E/F the group $E(F)[\text{tors}]$ is isomorphic to one of the following:

$\mathbb{Z}/m\mathbb{Z}$	$1 \leq m \leq 4$ *or* $m = 6, 7, 10, 29, 43, 49, 53$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$	$1 \leq m \leq 3$
$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$	

The groups that did not arise in degree 2 are

$$\mathbb{Z}/29\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/49\mathbb{Z}, \mathbb{Z}/58\mathbb{Z}, .$$

Proof-ish

Theorem (Bourdon, Clark, 2018)

If a CM elliptic curve E defined over a number field F of degree 14 has a point of order N, then

$$\frac{\varphi(N)}{\#\mathcal{O}^\times} \mid 14.$$

Proof-ish Part 2

Lemma (C., 2019)

Let $\mathcal{O}$ be the order of discriminant Δ and let $\ell_1^{a_1} \cdots \ell_n^{a_n}$ denote the prime power decomposition of $N \geq 4$. If $\frac{\varphi(N)}{\omega} = d$, then, in order to have a point of order N occur in degree d, we must have $\left(\frac{\Delta}{\ell}\right) = 0$ for every odd prime $\ell \mid N$. Furthermore, if the largest power of two dividing N is 2, then two may be split but otherwise 2 must also be ramified.

Proof-ish Part 2

Lemma (C., 2019)

Let $\mathcal{O}$ be the order of discriminant Δ and let $\ell_1^{a_1} \cdots \ell_n^{a_n}$ denote the prime power decomposition of $N \geq 4$. If $\frac{\varphi(N)}{\omega} = d$, then, in order to have a point of order N occur in degree d, we must have $\left(\frac{\Delta}{\ell}\right) = 0$ for every odd prime $\ell \mid N$. Furthermore, if the largest power of two dividing N is 2, then two may be split but otherwise 2 must also be ramified.

- Bourdon, Clark, 2019.

But wait! There's more!

Theorem (C., 2019)

Let F be a number field of degree $2p$. Let E/F be a CM elliptic curve. Then $E(F)[\text{tors}]$ is isomorphic to one of the groups arising over quadratic fields or to one of the following groups:

degree	*group*
22	

But wait! There's more!

Theorem (C., 2019)

Let F be a number field of degree $2p$. Let E/F be a CM elliptic curve. Then $E(F)[\text{tors}]$ is isomorphic to one of the groups arising over quadratic fields or to one of the following groups:

degree	*group*
22	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/46\mathbb{Z}$
26	$\mathbb{Z}/m\mathbb{Z}$ $m = 21, 53, 79, 106$

But wait! There's more!

Theorem (C., 2019)

Let F be a number field of degree $2p$. Let E/F be a CM elliptic curve. Then $E(F)[\text{tors}]$ is isomorphic to one of the groups arising over quadratic fields or to one of the following groups:

degree	*group*
22	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/46\mathbb{Z}$
26	$\mathbb{Z}/m\mathbb{Z}$ $m = 21, 53, 79, 106$
34	$\mathbb{Z}/103\mathbb{Z}$

But wait! There's more!

Theorem (C., 2019)

Let F be a number field of degree $2p$. Let E/F be a CM elliptic curve. Then $E(F)[\text{tors}]$ is isomorphic to one of the groups arising over quadratic fields or to one of the following groups:

degree	*group*
22	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/46\mathbb{Z}$
26	$\mathbb{Z}/m\mathbb{Z}$ $m = 21, 53, 79, 106$
34	$\mathbb{Z}/103\mathbb{Z}$
38	*NONE!*

Connection to Sophie Germain primes

Theorem (C.,2019)

Let F be a number field of degree $2p$ for $p > 3$ prime and E/F be a CM elliptic curve. If $E(F)[\text{tors}]$ is new and $j(E) \neq 0$ or 1728, then

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 5, 8, 12, \text{ or } 2p+1, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & m = 2p+1, \end{cases}$$

where $2p + 1$ is a prime greater than 3.

Theorem (C.,2019)

Let F be a number field of degree $2p$ for $p > 3$ prime and E/F be a CM elliptic curve. If $E(F)[\text{tors}]$ is new and $j(E) = 1728$, then

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 4p+1, \\ \mathbb{Z}/2m\mathbb{Z} & m = 4p+1, \end{cases}$$

where $4p+1$ is a prime greater than 3.

Theorem (C.,2019)

Let F be a number field of degree $2p$ for $p > 3$ prime and E/F be a CM elliptic curve. If $E(F)[\text{tors}]$ is new, $j(E) = 0$, and

- $p \neq 7$, *then*

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 6p+1, \end{cases}$$

- $p = 7$, *then*

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 6p+1, \\ \mathbb{Z}/m^2\mathbb{Z} & m = 7, \end{cases}$$

where $6p+1$ is a prime greater than 3.

Thanks for listening!