Elliptic curves and root numbers

Myungjun Yu

Korea Institute for Advanced Study

(joint work with Wan Lee)

November 26, 2019

Contents

1. Elliptic curves and the root numbers
2. Elliptic curves with complex multiplication
3. Lawful (CM) elliptic curves with $K \not\subset F$

Elliptic curves

Let F be a number field. Let E/F be an elliptic curve over F.

$$y^2 = x^3 + ax + b$$

where $a, b \in F$, and

$$\Delta := -16(4a^3 + 27b^2) \neq 0.$$

Elliptic curves

Let F be a number field. Let E/F be an elliptic curve over F.

$$y^2 = x^3 + ax + b$$

where $a, b \in F$, and

$$\Delta := -16(4a^3 + 27b^2) \neq 0.$$

Question

If E is an elliptic curve $y^2 = x^3 + ax + b$, find all points of E over F.

$$E(F) := \{(x, y) \in F \times F : y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

Elliptic curves

Theorem (Mordell, 1922)

The group $E(F)$ is a finitely generated abelian group.

Elliptic curves

Theorem (Mordell, 1922)

The group $E(F)$ is a finitely generated abelian group.

By the structure theorem of finitely generated abelian group, we have

$$E(F) \cong \mathbb{Z}^{\mathrm{rk}(E(F))} \oplus \text{torsion}$$

where

Theorem (Mordell, 1922)

The group $E(F)$ is a finitely generated abelian group.

By the structure theorem of finitely generated abelian group, we have

$$E(F) \cong \mathbb{Z}^{\mathrm{rk}(E(F))} \oplus \mathrm{torsion}$$

where

- $\mathrm{rk}(E(F))$ is a non-negative integer called the *Mordell-Weil rank*,

Elliptic curves

Theorem (Mordell, 1922)

The group $E(F)$ is a finitely generated abelian group.

By the structure theorem of finitely generated abelian group, we have

$$E(F) \cong \mathbb{Z}^{\mathrm{rk}(E(F))} \oplus \mathrm{torsion}$$

where

- $\mathrm{rk}(E(F))$ is a non-negative integer called the *Mordell-Weil rank*,
- There is no known general algorithm to find $\mathrm{rk}(E(F))$.

L-functions and the functional equation

Let $L(E/F, s)$ be the Hasse-Weil L-function for E/F. Put

$$\Lambda(E/F, s) := N(E/F)^{\frac{s}{2}}((2\pi)^{-s}\Gamma(s))^{[F:\mathbb{Q}]}L(E/F, s).$$

L-functions and the functional equation

Let $L(E/F, s)$ be the Hasse-Weil L-function for E/F. Put

$$\Lambda(E/F, s) := N(E/F)^{\frac{s}{2}}((2\pi)^{-s}\Gamma(s))^{[F:\mathbb{Q}]}L(E/F, s).$$

The Hasse-Weil conjecture asserts that $L(E/F, s)$ has an analytic continuation to the complex plane and satisfies a functional equation

$$\Lambda(E/F, 2-s) = W(E/F)\Lambda(E/F, s).$$

L-functions and the functional equation

Let $L(E/F,s)$ be the Hasse-Weil L-function for E/F. Put

$$\Lambda(E/F,s) := N(E/F)^{\frac{s}{2}}((2\pi)^{-s}\Gamma(s))^{[F:\mathbb{Q}]}L(E/F,s).$$

The Hasse-Weil conjecture asserts that $L(E/F,s)$ has an analytic continuation to the complex plane and satisfies a functional equation

$$\Lambda(E/F,2-s) = W(E/F)\Lambda(E/F,s).$$

The constant $W(E/F) = \pm 1$ is called the (global) *root number* of E/F.

L-functions and the functional equation

Let $L(E/F, s)$ be the Hasse-Weil L-function for E/F. Put

$$\Lambda(E/F, s) := N(E/F)^{\frac{s}{2}}((2\pi)^{-s}\Gamma(s))^{[F:\mathbb{Q}]}L(E/F, s).$$

The Hasse-Weil conjecture asserts that $L(E/F, s)$ has an analytic continuation to the complex plane and satisfies a functional equation

$$\Lambda(E/F, 2-s) = W(E/F)\Lambda(E/F, s).$$

The constant $W(E/F) = \pm 1$ is called the (global) *root number* of E/F.

Remark

1. The root number determines the parity of the vanishing order $\mathrm{ord}_{s=1}(L(E/F, s))$.

L-functions and the functional equation

Let $L(E/F, s)$ be the Hasse-Weil L-function for E/F. Put

$$\Lambda(E/F, s) := N(E/F)^{\frac{s}{2}}((2\pi)^{-s}\Gamma(s))^{[F:\mathbb{Q}]}L(E/F, s).$$

The Hasse-Weil conjecture asserts that $L(E/F, s)$ has an analytic continuation to the complex plane and satisfies a functional equation

$$\Lambda(E/F, 2-s) = W(E/F)\Lambda(E/F, s).$$

The constant $W(E/F) = \pm 1$ is called the (global) *root number* of E/F.

Remark

1. The root number determines the parity of the vanishing order $\mathrm{ord}_{s=1}(L(E/F, s))$.
2. Assuming BSD conjecture : $\mathrm{rk}(E(F)) = \mathrm{ord}_{s=1}(L(E/F, s))$,

L-functions and the functional equation

Let $L(E/F, s)$ be the Hasse-Weil L-function for E/F. Put

$$\Lambda(E/F, s) := N(E/F)^{\frac{s}{2}}((2\pi)^{-s}\Gamma(s))^{[F:\mathbb{Q}]}L(E/F, s).$$

The Hasse-Weil conjecture asserts that $L(E/F, s)$ has an analytic continuation to the complex plane and satisfies a functional equation

$$\Lambda(E/F, 2-s) = W(E/F)\Lambda(E/F, s).$$

The constant $W(E/F) = \pm 1$ is called the (global) *root number* of E/F.

Remark

1. The root number determines the parity of the vanishing order $\mathrm{ord}_{s=1}(L(E/F, s))$.
2. Assuming BSD conjecture : $\mathrm{rk}(E(F)) = \mathrm{ord}_{s=1}(L(E/F, s))$, the root number determines the parity of the rank.

Work of Langlands and Deligne

Work of Langlands and Deligne

Work of Langlands and Deligne

Work of Langlands and Deligne

1. We can define the local root number $W(E/F_v)$ for all places v of F.

Work of Langlands and Deligne

1. We can define the local root number $W(E/F_v)$ for all places v of F.
2. If there exist an analytic continuation of $L(E/F, s)$, then

$$W(E/F) = \prod_v W(E/F_v).$$

A list of formulas for the local root number

Lemma (local root number formula)

$$W(E/F_v) = \begin{cases} +1, & \text{if } E/F_v \text{ has good reduction.} \\ -1, & \text{if } E/F_v \text{ has split multiplicative reduction.} \\ +1, & \text{if } E/F_v \text{ has non-split multiplicative reduction.} \\ -1, & \text{if } v \text{ is an Archimedean place.} \end{cases}$$

Lawful elliptic curves

Definition

Let N be a number field or a (p-adic) local field. We say E/N is *lawful* if $W(E/M) = 1$ for all quadratic extensions M/N.

Lawful elliptic curves

Definition

Let N be a number field or a (p-adic) local field. We say E/N is *lawful* if $W(E/M) = 1$ for all quadratic extensions M/N.

Remark

1. It was first defined and studied by Dokchitser-Dokchitser (2009).

Lawful elliptic curves

Definition

Let N be a number field or a (p-adic) local field. We say E/N is *lawful* if $W(E/M) = 1$ for all quadratic extensions M/N.

Remark

1. It was first defined and studied by Dokchitser-Dokchitser (2009).
2. If N is a number field, then $W(E/N)W(E^M/N) = W(E/M)$.

Lawful elliptic curves

Definition

Let N be a number field or a (p-adic) local field. We say E/N is *lawful* if $W(E/M) = 1$ for all quadratic extensions M/N.

Remark

1. It was first defined and studied by Dokchitser-Dokchitser (2009).
2. If N is a number field, then $W(E/N)W(E^M/N) = W(E/M)$.
3. Therefore if N is a number field, then E/N is lawful if and only if $W(E^M/N)$ is a constant for all quadratic extensions M/N.

Local-Global principle for lawfulness

Lemma

Suppose E is defined over a number field F. Then the following conditions are equivalent.

1. E/F is lawful.
2. E/F_v is lawful for all places v of F.

Local-Global principle for lawfulness

Lemma

Suppose E is defined over a number field F. Then the following conditions are equivalent.

1. E/F is lawful.
2. E/F_v is lawful for all places v of F.

Let $\mathcal{C}(F)$ denote the set of quadratic characters of F and define $\mathcal{C}(F_v)$ similarly. Let S be a finite set of places of F containing all primes of bad reduction and infinite places. The restriction map

$$\mathcal{C}(F) \to \prod_{v \in S} \mathcal{C}(F_v)$$

is surjective.

Contents

1. Elliptic curves and the root numbers
2. Elliptic curves with complex multiplication
3. Lawful (CM) elliptic curves with $K \not\subset F$

CM elliptic curves

E/F elliptic curve over a number field F.

CM elliptic curves

E/F elliptic curve over a number field F.

The endomorphism ring $\mathrm{End}(E)$ can be one of the following.

CM elliptic curves

E/F elliptic curve over a number field F.

The endomorphism ring $\mathrm{End}(E)$ can be one of the following.

1. $\mathbb{Z}$
2. an order of an imaginary quadratic field K, i.e., $\mathrm{End}(E) \otimes \mathbb{Q} = K$.

CM elliptic curves

E/F elliptic curve over a number field F.

The endomorphism ring $\mathrm{End}(E)$ can be one of the following.

1. $\mathbb{Z}$
2. an order of an imaginary quadratic field K, i.e., $\mathrm{End}(E) \otimes \mathbb{Q} = K$.

If it is the second case, we say E/F has CM over K.

CM elliptic curves

E/F elliptic curve over a number field F.

The endomorphism ring $\mathrm{End}(E)$ can be one of the following.

1. $\mathbb{Z}$
2. an order of an imaginary quadratic field K, i.e., $\mathrm{End}(E) \otimes \mathbb{Q} = K$.

If it is the second case, we say E/F has CM over K.

If $K \subset F$, then the rank of $E(F)$ should be even because $E(F) \otimes \mathbb{Q}$ is a K-vector space and $[K : \mathbb{Q}] = 2$.

CM elliptic curves

E/F elliptic curve over a number field F.

The endomorphism ring $\mathrm{End}(E)$ can be one of the following.

1. $\mathbb{Z}$
2. an order of an imaginary quadratic field K, i.e., $\mathrm{End}(E) \otimes \mathbb{Q} = K$.

If it is the second case, we say E/F has CM over K.

If $K \subset F$, then the rank of $E(F)$ should be even because $E(F) \otimes \mathbb{Q}$ is a K-vector space and $[K : \mathbb{Q}] = 2$. Then according to BSD conjecture, $W(E/F)$ should be 1,

CM elliptic curves

E/F elliptic curve over a number field F.

The endomorphism ring $\mathrm{End}(E)$ can be one of the following.

1. $\mathbb{Z}$
2. an order of an imaginary quadratic field K, i.e., $\mathrm{End}(E) \otimes \mathbb{Q} = K$.

If it is the second case, we say E/F has CM over K.

If $K \subset F$, then the rank of $E(F)$ should be even because $E(F) \otimes \mathbb{Q}$ is a K-vector space and $[K:\mathbb{Q}] = 2$. Then according to BSD conjecture, $W(E/F)$ should be 1, which is indeed the case

A Hecke character associated to a CM elliptic curve

Theorem

Suppose E/F has CM over K and $K \subseteq F$. Then there exists a Hecke character

$$\psi : \mathbb{A}_F^\times / F^\times \to \mathbb{C}^\times$$

satisfying the following properties.

1. *If v is a finite prime of F, then $\psi(\mathcal{O}_v^\times) = 1$ if and only if E has good reduction at v.*
2. *If $x \in \mathbb{A}_F^\times$ is a finite idele (i.e., $x_\infty = 1$ for all infinite places ∞) and $\mathfrak{p}$ is a prime of K, then $\psi(x) \in K = \mathrm{End}(E) \otimes \mathbb{Q}$, $\psi(x)(\mathbf{N}_K^F x)_\mathfrak{p}^{-1} \in \mathcal{O}_\mathfrak{p}^\times$ and for every $P \in E[\mathfrak{p}^\infty]$, we have*

$$[x, F^{\mathrm{ab}}/F]P = \psi(x)(\mathbf{N}_K^F x)_\mathfrak{p}^{-1} P,$$

where $[\cdot, F^{\mathrm{ab}}/F]$ denotes the Artin map.

The root number of CM elliptic curve

Theorem

Suppose E/F has CM over K and $K \subseteq F$. Then $W(E/F) = 1$.

The root number of CM elliptic curve

Theorem

Suppose E/F has CM over K and $K \subseteq F$. Then $W(E/F) = 1$.

Proof.

In the CM elliptic curve case, the *Weil-Deligne* representation for F_v given by the action on the *Tate module* is decomposed into the direct sum $\psi_v \oplus \overline{\psi_v}$. Then the ϵ*-factor* computation is done by considering the 1-dimensional case, which is established by Tate in his thesis. What one can show is in fact:

$$W(E/F_v) = \psi_v(-1).$$

Then the result follows from the fact that ψ is a Hecke character on the idele class group. □

Lawfulness of CM elliptic curves

Corollary

If E/F has CM over K and $K \subset F$, then E/F is lawful.

Contents

1. Elliptic curves and the root numbers
2. Elliptic curves with complex multiplication
3. Lawful (CM) elliptic curves with $K \not\subset F$

Lawful elliptic curves E/L with $W(E/L) = 1$

Assumptions

1. E/F has CM over K.

Lawful elliptic curves E/L with $W(E/L) = 1$

Assumptions

1. E/F has CM over K.
2. $K \not\subset F$.

Lawful elliptic curves E/L with $W(E/L) = 1$

Assumptions

1. E/F has CM over K.
2. $K \not\subset F$.

Theorem (Lee-Y)

There exist infinitely many quadratic extensions L/F such that E/L is lawful with $W(E/L) = 1$.

Lawful elliptic curves E/L with $W(E/L) = 1$

Assumptions

1. E/F has CM over K.
2. $K \not\subset F$.

Theorem (Lee-Y)

There exist infinitely many quadratic extensions L/F such that E/L is lawful with $W(E/L) = 1$.

More interesting lawful elliptic curves

Lawful elliptic curves with $W(E/L) = -1$ are arithmetically more interesting.

Lawful elliptic curves E/L with $W(E/L) = -1$

Theorem (Lee-Y)

Suppose that there exists a rational prime p such that the following conditions are satisfied.

1. $p \equiv 3 \pmod 4$.
2. *p is ramified at $K/\mathbb{Q}$.*
3. *There exists a prime v of F such that $e(v|p)$ and $f(v|p)$ are both odd, where $e(v|p)$ and $f(v|p)$ denote the ramification index and the inertia degree of v above p, respectively.*

Then there exist infinitely many quadratic extensions L/F such that E/L is lawful with $W(E/L) = -1$.

Proof of the theorem

1. Let w be the unique prime of KF above v.

Proof of the theorem

1. Let w be the unique prime of KF above v.
2. Condition 2 shows that E/FK has bad reduction at w.

Proof of the theorem

1. Let w be the unique prime of KF above v.
2. Condition 2 shows that E/FK has bad reduction at w.
3. Condition 1 together with condition 3 show that $W(E/(FK)_w) = -1$.

Proof of the theorem

1. Let w be the unique prime of KF above v.
2. Condition 2 shows that E/FK has bad reduction at w.
3. Condition 1 together with condition 3 show that $W(E/(FK)_w) = -1$.
4. Recall the restriction map

$$\mathcal{C}(F) \to \prod_{v \in S} \mathcal{C}(F_v)$$

is surjective.

Proof of the theorem

1. Let w be the unique prime of KF above v.
2. Condition 2 shows that E/FK has bad reduction at w.
3. Condition 1 together with condition 3 show that $W(E/(FK)_w) = -1$.
4. Recall the restriction map
$$\mathcal{C}(F) \to \prod_{v \in S} \mathcal{C}(F_v)$$
is surjective.
5. Choose L so that the image of L and KF are the same except at v, and so that the image of L at v is the unramified quadratic extension.

Proof of the theorem

1. Let w be the unique prime of KF above v.
2. Condition 2 shows that E/FK has bad reduction at w.
3. Condition 1 together with condition 3 show that $W(E/(FK)_w) = -1$.
4. Recall the restriction map

$$\mathcal{C}(F) \to \prod_{v \in S} \mathcal{C}(F_v)$$

   is surjective.
5. Choose L so that the image of L and KF are the same except at v, and so that the image of L at v is the unramified quadratic extension.
6. Letting w' be the prime of L above v, we can prove $W(E/L_{w'}) = 1$.

Examples

Corollary

Suppose that $K \neq \mathbb{Q}(\sqrt{-d})$ for $d = 1, 2$ or 3. If $[F : \mathbb{Q}]$ is odd, then there exist infinitely many quadratic extensions L/F such that E/L is lawful with $W(E/L) = -1$.

Examples

Corollary

Suppose that $K \neq \mathbb{Q}(\sqrt{-d})$ for $d = 1, 2$ or 3. If $[F : \mathbb{Q}]$ is odd, then there exist infinitely many quadratic extensions L/F such that E/L is lawful with $W(E/L) = -1$.

Examples

Let $L = \mathbb{Q}(\sqrt{-m})$ for $m > 0$.

1. $y^2 + xy = x^3 - x^2 - 2x - 1$ with $\left(\frac{m}{7}\right) = 1$.
2. $y^2 + y = x^3 - x^2 - 7x + 10$ with $\left(\frac{m}{11}\right) = 1$.
3. $y^2 + y = x^3 - 38x + 90$ with $\left(\frac{m}{19}\right) = 1$.
4. $y^2 + y = x^3 - 860x + 9707$ with $\left(\frac{m}{43}\right) = 1$.

Thank you very much for your attention!