Complex Multiplication

Yunhan (Alex) Sheng

yhsheng@uchicago.edu

UChicago REU, August 2022

Outline of the talk

1. Number-theoretic background
2. CM of elliptic curves
3. Generalization to abelian Varieties
4. Acknowledgements

Ramification

- Suppose that L/K is **abelian**, i.e., $\mathrm{Gal}(L/K)$ is an abelian group.

Ramification

- Suppose that L/K is **abelian**, i.e., $\mathrm{Gal}(L/K)$ is an abelian group.
- How does prime ideals $\mathfrak{p}$ in K split in L?

Ramification

- Suppose that L/K is **abelian**, i.e., $\mathrm{Gal}(L/K)$ is an abelian group.
- How does prime ideals $\mathfrak{p}$ in K split in L?
- Consider $L = \mathbb{Q}(i)/\mathbb{Q} = K$. Then

Ramification

- Suppose that L/K is **abelian**, i.e., $\mathrm{Gal}(L/K)$ is an abelian group.
- How does prime ideals $\mathfrak{p}$ in K split in L?
- Consider $L = \mathbb{Q}(i)/\mathbb{Q} = K$. Then
  1. $\mathfrak{p} = (2) = (1 - i)^2$, in which case $\mathfrak{p}$ is **ramified**;

Ramification

- Suppose that L/K is **abelian**, i.e., $\mathrm{Gal}(L/K)$ is an abelian group.
- How does prime ideals $\mathfrak{p}$ in K split in L?
- Consider $L = \mathbb{Q}(i)/\mathbb{Q} = K$. Then
  1. $\mathfrak{p} = (2) = (1-i)^2$, in which case $\mathfrak{p}$ is **ramified**;
  2. $\mathfrak{p} = (3)$ remains prime in $\mathbb{Q}(i)$, in which case $\mathfrak{p}$ is **inert**;

Ramification

- Suppose that L/K is **abelian**, i.e., $\mathrm{Gal}(L/K)$ is an abelian group.
- How does prime ideals $\mathfrak{p}$ in K split in L?
- Consider $L = \mathbb{Q}(i)/\mathbb{Q} = K$. Then
  1. $\mathfrak{p} = (2) = (1-i)^2$, in which case $\mathfrak{p}$ is **ramified**;
  2. $\mathfrak{p} = (3)$ remains prime in $\mathbb{Q}(i)$, in which case $\mathfrak{p}$ is **inert**;
  3. $\mathfrak{p} = (5) = (2+i)(2-i)$, in which case $\mathfrak{p}$ **splits completely**.

Ramification

- Suppose that L/K is **abelian**, i.e., $\mathrm{Gal}(L/K)$ is an abelian group.
- How does prime ideals $\mathfrak{p}$ in K split in L?
- Consider $L = \mathbb{Q}(i)/\mathbb{Q} = K$. Then
  1. $\mathfrak{p} = (2) = (1-i)^2$, in which case $\mathfrak{p}$ is **ramified**;
  2. $\mathfrak{p} = (3)$ remains prime in $\mathbb{Q}(i)$, in which case $\mathfrak{p}$ is **inert**;
  3. $\mathfrak{p} = (5) = (2+i)(2-i)$, in which case $\mathfrak{p}$ **splits completely**.
- If every prime in K is unramified in L, then L/K is unramified.

The case over $\mathbb{Q}$

- Can we explicitly describe the set of numbers that generates (unramified) abelian extensions of $\mathbb{Q}$?

Theorem 1 (Kronecker-Weber)

Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_N)$ for some $N > 0$.

Theorem 2 (Hermite-Minkowski)

There are no unramified extensions of $\mathbb{Q}$.

- What if we change the base field $K = \mathbb{Q}$ to an arbitrary number field (i.e. finite extensions of $\mathbb{Q}$)?

- What if we change the base field $K = \mathbb{Q}$ to an arbitrary number field (i.e. finite extensions of $\mathbb{Q}$)?
- Kronecker's Jugendtraum ("mein liebster Jugendtraum"), Hilbert's twelfth problem, explicit class field theory.

- What if we change the base field $K = \mathbb{Q}$ to an arbitrary number field (i.e. finite extensions of $\mathbb{Q}$)?
- Kronecker's Jugendtraum ("mein liebster Jugendtraum"), Hilbert's twelfth problem, explicit class field theory.
- Complex Multiplication solves the case $K = \mathbb{Q}(\sqrt{-D})$ an imaginary quadratic field (or more generally, when K is a imaginary quadratic extension of a totally real field).

- What if we change the base field $K = \mathbb{Q}$ to an arbitrary number field (i.e. finite extensions of $\mathbb{Q}$)?
- Kronecker's Jugendtraum ("mein liebster Jugendtraum"), Hilbert's twelfth problem, explicit class field theory.
- Complex Multiplication solves the case $K = \mathbb{Q}(\sqrt{-D})$ an imaginary quadratic field (or more generally, when K is a imaginary quadratic extension of a totally real field).
- This is the only known case besides $K = \mathbb{Q}$. The problem is far from being completely resolved.

- What if we change the base field $K = \mathbb{Q}$ to an arbitrary number field (i.e. finite extensions of $\mathbb{Q}$)?
- Kronecker's Jugendtraum ("mein liebster Jugendtraum"), Hilbert's twelfth problem, explicit class field theory.
- Complex Multiplication solves the case $K = \mathbb{Q}(\sqrt{-D})$ an imaginary quadratic field (or more generally, when K is a imaginary quadratic extension of a totally real field).
- This is the only known case besides $K = \mathbb{Q}$. The problem is far from being completely resolved.
- Complex Multiplication: this piece of **arithmetic** information will be extracted from studying **geometric** objects, namely, elliptic curves (or more generally, abelian varieties).

Outline of the talk

1. Number-theoretic background
2. CM of elliptic curves
3. Generalization to abelian Varieties
4. Acknowledgements

What is an elliptic curve?

By an **elliptic curve** E/K, we understand

- a one-dimensional nonsingular projective variety over K of genus one, together with a special point $O \in E$;
- or more naively, a curve given by so-called **Weierstrass equation**

$$y^2 = x^3 + Ax + B, \quad A, B \in K$$

(N.B. the equation takes this simplified form only if $\mathrm{char}(\overline{K}) \neq 2, 3$.)

Two elliptic curves are isomorphic iff they have the same j-**invariant**:

$$j(E) = \frac{1728(4A)^3}{-16(4A^3 + 27B^2)}.$$

Elliptic curves: basics

- An elliptic curve can be endowed with a group structure, which we now describe.

Elliptic curves: basics

- An elliptic curve can be endowed with a group structure, which we now describe.
- An **isogeny** between elliptic curves E_1 and E_2 is a morphism $\phi : E_1 \to E_2$ of varieties such that $\phi(O) = O$.

Elliptic curves: basics

- An elliptic curve can be endowed with a group structure, which we now describe.
- An **isogeny** between elliptic curves E_1 and E_2 is a morphism $\phi : E_1 \to E_2$ of varieties such that $\phi(O) = O$.
- For example, the multiplication-by-m map $[m] : E \to E$ by

$$P \mapsto mP = \underbrace{P + P + \ldots + P}_{m \text{ times}}$$

is an isogeny.

Elliptic curves: basics

- An elliptic curve can be endowed with a group structure, which we now describe.
- An **isogeny** between elliptic curves E_1 and E_2 is a morphism $\phi : E_1 \to E_2$ of varieties such that $\phi(O) = O$.
- For example, the multiplication-by-m map $[m] : E \to E$ by

$$P \mapsto mP = \underbrace{P + P + \ldots + P}_{m \text{ times}}$$

  is an isogeny.
- Let $\mathrm{End}(E)$ be the ring of isogenies from E to itself, is the map

$$[-] : \mathbb{Z} \to \mathrm{End}(E)$$

  is an isomorphism, or is $\mathrm{End}(E)$ strictly larger than $\mathbb{Z}$?

CM of elliptic curves

Theorem 3

Let $E/\mathbb{C}$ be an elliptic curve. Then either $\mathrm{End}(E) = \mathbb{Z}$ or $\mathrm{End}(E)$ is isomorphic to an order of $\mathbb{Q}(\sqrt{-D})$ for some $D > 0$.

N.B. Let K be a number field. An **order** R of a K is a subring of K that is finitely generated as $\mathbb{Z}$-module and spans K over $\mathbb{Q}$.

For example, $\mathbb{Z}[i]$ and $\{a + 2bi \mid a, b \in \mathbb{Z}\}$ are both orders of $\mathbb{Q}(i)$. The ring of integers is the largest order.

Definition 4

An elliptic curve $E/\mathbb{C}$ has **complex multiplication** (or CM for short) by R if $R = \mathrm{End}(E)$ is an order of an imaginary quadratic field.

Elliptic curves over $\mathbb{C}$

- Two lattice $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ are **homothetic** if $\Lambda_2 = \alpha\Lambda_1$ for some $\alpha \in \mathbb{C}$.

Elliptic curves over $\mathbb{C}$

- Two lattice $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ are **homothetic** if $\Lambda_2 = \alpha\Lambda_1$ for some $\alpha \in \mathbb{C}$.
- (Uniformization) For any $E/\mathbb{C}$, there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ as (complex) Lie groups.

Elliptic curves over $\mathbb{C}$

- Two lattice $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ are **homothetic** if $\Lambda_2 = \alpha\Lambda_1$ for some $\alpha \in \mathbb{C}$.
- (Uniformization) For any $E/\mathbb{C}$, there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ as (complex) Lie groups.
- Conversely, every complex torus arises as an elliptic curve.

Elliptic curves over $\mathbb{C}$

- Two lattice $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ are **homothetic** if $\Lambda_2 = \alpha\Lambda_1$ for some $\alpha \in \mathbb{C}$.
- (Uniformization) For any $E/\mathbb{C}$, there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ as (complex) Lie groups.
- Conversely, every complex torus arises as an elliptic curve.
- In fact, there is an equivalence of categories between:
  - elliptic curve E over $\mathbb{C}$ with isogenies, and
  - lattices $\Lambda \subset \mathbb{C}$ up to homothety, with

$$\mathrm{Hom}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subset \Lambda_2\}.$$

Proof of Theorem 3

Proof of Theorem 3.

Suppose $E/\mathbb{C} \cong \mathbb{C}/\Lambda$ as Lie groups. Up to homothety replace Λ by $\mathbb{Z} + \tau\mathbb{Z}$ for some $\tau \in \mathbb{C} \setminus \mathbb{R}$. For any $\alpha \in \mathrm{End}(E) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda = \Lambda\}$, there exists $m, n, p, q \in \mathbb{Z}$ such that $\alpha = m + n\tau$ and $\alpha\tau = p + q\tau$. Eliminate τ, we get

$$\alpha^2 - (m + q)\alpha + np = 0,$$

so that $\mathrm{End}(E)$ is an integral extension of $\mathbb{Z}$. If $\alpha \notin \mathbb{Z}$, then $n \neq 0$, so eliminating n we get an quadratic equation

$$n\tau^2 + (m - q)\tau - p = 0.$$

Since $\tau \notin \mathbb{R}$, $\mathbb{Q}(\tau)$ is an imaginary quadratic field. □

Construction of class fields

Theorem 5

Let R be an order of an imaginary quadratic field K. Let $E/\mathbb{C}$ be an elliptic curve with CM by R. Then

- *$K(j(E))$ is the maximal unramified extension of K*
- *$K(j(E), x(E_{tors}))$ is the maximal abelian extension of K, where E_{tors} are points of E of finite order, and $x(-)$ is the function taking x-coordinate.*

(N.B. the function $x(-)$ only works if $j(E) \neq 0, 1728$; otherwise we need something more subtle called Weber function.)

Construction of class fields

Theorem 5

Let R be an order of an imaginary quadratic field K. Let $E/\mathbb{C}$ be an elliptic curve with CM by R. Then

- $K(j(E))$ *is the maximal unramified extension of* K
- $K(j(E), x(E_{tors}))$ *is the maximal abelian extension of* K*, where* E_{tors} *are points of* E *of finite order, and* $x(-)$ *is the function taking* x*-coordinate.*

(N.B. the function $x(-)$ only works if $j(E) \neq 0, 1728$; otherwise we need something more subtle called Weber function.)

- Moral of the story: j-invariant and coordinate of torsion points generate abelian extensions of $\mathbb{Q}(\sqrt{-D})$ for some $D > 0$.

From numbe theory: idèles

- From number theory: let K be a global field (finite extensions of $\mathbb{Q}$). The completion of K_v at a place (given by an absolute value) v of K is a local field (think about $\mathbb{Q}_p$). Let $\mathcal{O}_v$ be the valuation subring (think about $\mathbb{Z}_p$), the **idèle group** is the topological group

$$\mathbf{A}_K^\times = \left\{ (a_v) \in \prod_v K_v^\times \mid a_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v \right\}.$$

From numbe theory: idèles

- From number theory: let K be a global field (finite extensions of $\mathbb{Q}$). The completion of K_v at a place (given by an absolute value) v of K is a local field (think about $\mathbb{Q}_p$). Let $\mathcal{O}_v$ be the valuation subring (think about $\mathbb{Z}_p$), the **idèle group** is the topological group

$$\mathbf{A}_K^\times = \left\{ (a_v) \in \prod_v K_v^\times \mid a_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v \right\}.$$

- Packing *local* information in the *global* setting.

From numbe theory: idèles

- From number theory: let K be a global field (finite extensions of $\mathbb{Q}$). The completion of K_v at a place (given by an absolute value) v of K is a local field (think about $\mathbb{Q}_p$). Let $\mathcal{O}_v$ be the valuation subring (think about $\mathbb{Z}_p$), the **idèle group** is the topological group

$$\mathbf{A}_K^\times = \left\{ (a_v) \in \prod_v K_v^\times \mid a_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v \right\}.$$

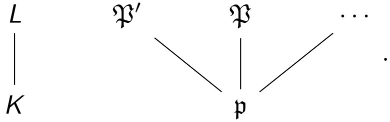
- Packing *local* information in the *global* setting.
- The fractional ideal (x) associated to an idèle $x \in \mathbf{A}_K^\times$ is

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x_{\mathfrak{p}})},$$

where $(x_{\mathfrak{p}}) = (x)\mathcal{O}_p$.

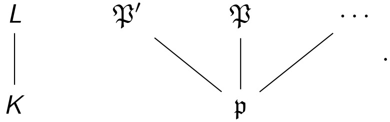
From number theory: Frobenius substitution

- Let L/K be a finite Galois extension of number fields and $\mathfrak{P}$ a prime lying over an unramified prime $\mathfrak{p}$:



From number theory: Frobenius substitution

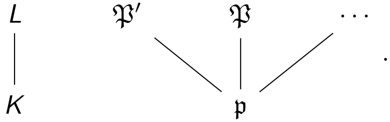
- Let L/K be a finite Galois extension of number fields and $\mathfrak{P}$ a prime lying over an unramified prime $\mathfrak{p}$:



- Let $\kappa_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$ and $\kappa_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ be the corresponding residue fields.

From number theory: Frobenius substitution

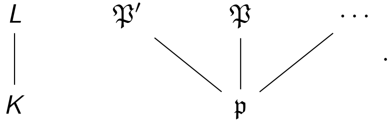
- Let L/K be a finite Galois extension of number fields and $\mathfrak{P}$ a prime lying over an unramified prime $\mathfrak{p}$:



- Let $\kappa_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$ and $\kappa_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ be the corresponding residue fields.
- The **Frobenius substitution** $\sigma_{\mathfrak{P}}$ is the generator of $\mathrm{Gal}(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}})$, which is cyclic since $\kappa_{\mathfrak{P}}$ and $\kappa_{\mathfrak{p}}$ are finite fields.

From number theory: Frobenius substitution

- Let L/K be a finite Galois extension of number fields and $\mathfrak{P}$ a prime lying over an unramified prime $\mathfrak{p}$:



- Let $\kappa_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$ and $\kappa_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ be the corresponding residue fields.
- The **Frobenius substitution** $\sigma_{\mathfrak{P}}$ is the generator of $\mathrm{Gal}(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}})$, which is cyclic since $\kappa_{\mathfrak{P}}$ and $\kappa_{\mathfrak{p}}$ are finite fields.
- If L/K is abelian, then $\sigma_{\mathfrak{P}} = \sigma_{\mathfrak{P}'}$, so we simply write $\sigma_{\mathfrak{p}}$.

From number theory: Artin reciprocity

- Let L/K be a finite abelian extension of number fields. Let K^{ab} be the maximal abelian extension of K.

From number theory: Artin reciprocity

- Let L/K be a finite abelian extension of number fields. Let K^{ab} be the maximal abelian extension of K.
- Class field theory tells us that there is a unique continuous map called the (global) **Artin map**

$$\mathbf{A}_K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

given by $s \mapsto [s, K]$, where if $(s) = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$ is not divisible by primes that ramify in L, then

$$[s, K]|_L = ((s), L/K) := \prod_{\mathfrak{p}} \sigma_\mathfrak{p}^{n_\mathfrak{p}}$$

From number theory: Artin reciprocity

- Let L/K be a finite abelian extension of number fields. Let K^{ab} be the maximal abelian extension of K.
- Class field theory tells us that there is a unique continuous map called the (global) **Artin map**

$$\mathbf{A}_K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

given by $s \mapsto [s, K]$, where if $(s) = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$ is not divisible by primes that ramify in L, then

$$[s, K]|_L = ((s), L/K) := \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{n_\mathfrak{p}}$$

- The Artin map is surjective with $K^\times$ contained in the kernel.

From arithmetic to algebra via analysis

- Let $K/\mathbb{Q}$ be an imaginary quadratic field.

From arithmetic to algebra via analysis

- Let $K/\mathbb{Q}$ be an imaginary quadratic field.
- Let $E/\mathbb{Q}$ be an elliptic curve with CM by the rings of integers $\mathcal{O}_K$.

From arithmetic to algebra via analysis

- Let $K/\mathbb{Q}$ be an imaginary quadratic field.
- Let $E/\mathbb{Q}$ be an elliptic curve with CM by the rings of integers $\mathcal{O}_K$.
- Let $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$.

From arithmetic to algebra via analysis

- Let $K/\mathbb{Q}$ be an imaginary quadratic field.
- Let $E/\mathbb{Q}$ be an elliptic curve with CM by the rings of integers $\mathcal{O}_K$.
- Let $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$.
- Let $s \in \mathbf{A}_K^\times$ be an idèle with $[s, K] = \sigma|_{K^{\mathrm{ab}}}$.

From arithmetic to algebra via analysis

- Let $K/\mathbb{Q}$ be an imaginary quadratic field.
- Let $E/\mathbb{Q}$ be an elliptic curve with CM by the rings of integers $\mathcal{O}_K$.
- Let $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$.
- Let $s \in \mathbf{A}_K^\times$ be an idèle with $[s, K] = \sigma|_{K^{\mathrm{ab}}}$.
- Let $f : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C})$ be a complex-analytic isomorphism.

Theorem 6 (The main theorem of CM of elliptic curves)

There exists a unique complex-analytic isomorphism $f' : \mathbb{C}/(s)^{-1}\mathfrak{a} \xrightarrow{\sim} E^\sigma(\mathbb{C})$ *such that the following diagram commutes:*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{(s)^{-1}} & K/(s)^{-1}\mathfrak{a} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ E(\mathbb{C}) & \xrightarrow{\sigma} & E^\sigma(\mathbb{C}) \end{array}$$

The associated Hecke character

- A **Hecke character** of a number field K is a continuous map

$$\psi : \mathbf{A}_K^\times \to \mathbb{C}^\times \quad \text{that satisfies } \chi(L^\times) = 1.$$

The associated Hecke character

- A **Hecke character** of a number field K is a continuous map

$$\psi : \mathbf{A}_K^\times \to \mathbb{C}^\times \quad \text{that satisfies } \chi(L^\times) = 1.$$

- Using the Main Theorem, we can define a Hecke character

$$\psi_{E/L}(s) = \alpha_{L/K}(s)\mathrm{Nm}_{L/K}(s^{-1})_\infty$$

of L/K, where E/L is an elliptic curve with CM by $\mathcal{O}_K$, and $\alpha_{L/K}$ is chosen to make following diagram commutes

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\alpha_{L/K}(s)/\mathrm{Nm}_{L/K}s} & K/\mathfrak{a} \\ \sim\downarrow & & \downarrow\sim \\ E^{\mathrm{ab}}(L) & \xrightarrow{[s,L]} & E^{\mathrm{ab}}(L) \end{array}.$$

The associated Hecke character

- A **Hecke character** of a number field K is a continuous map
$$\psi : \mathbf{A}_K^\times \to \mathbb{C}^\times \quad \text{that satisfies } \chi(L^\times) = 1.$$
- Using the Main Theorem, we can define a Hecke character
$$\psi_{E/L}(s) = \alpha_{L/K}(s)\mathrm{Nm}_{L/K}(s^{-1})_\infty$$
of L/K, where E/L is an elliptic curve with CM by $\mathcal{O}_K$, and $\alpha_{L/K}$ is chosen to make following diagram commutes
$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\alpha_{L/K}(s)/\mathrm{Nm}_{L/K}s} & K/\mathfrak{a} \\ \sim\downarrow & & \downarrow\sim \\ E^{\mathrm{ab}}(L) & \xrightarrow{[s,L]} & E^{\mathrm{ab}}(L) \end{array} .$$
- $\psi_{E/L}$ is unramified at $\mathfrak{P}$ of L iff E has good reduction at $\mathfrak{P}$.

L-series of an elliptic curve

The L-series of E/L encodes arithmetic information:

$$L(E/L, s) = \prod_{\mathfrak{P}} L_{\mathfrak{P}}(E/L, q_{\mathfrak{P}}^{-s})^{-1}$$

ranging over primes $\mathfrak{P}$ of L. Each local L-factor is given by

$$L_{\mathfrak{P}}(E/L, T) = 1 - a_{\mathfrak{P}} T + q_{\mathfrak{P}} T^2,$$

where $q_{\mathfrak{P}} = \mathrm{Nm}_{L/\mathbb{Q}} \mathfrak{P}$ and $a_{\mathfrak{P}} = q_{\mathfrak{P}} + 1 - \#\widetilde{E}(\kappa_{\mathfrak{P}})$, $\kappa_{\mathfrak{P}}$ is the residue field of L at $\mathfrak{P}$. In the case when E has bad reduction at $\mathfrak{P}$, we define

$$L_{\mathfrak{P}}(E/L, T) = \begin{cases} 1 - T, & \text{split multiplicative reduction} \\ 1 + T, & \text{non-split multiplicative reduction} \\ 1, & \text{additive reduction} \end{cases}.$$

Hecke L-series

- Let $\psi : \mathbf{A}_L^\times \to \mathbb{C}^\times$ be a Hecke character. Attach to it the L-series

$$L(s, \psi) = \prod_{\mathfrak{P}} (1 - \psi(\mathfrak{P}) q_{\mathfrak{P}}^{-s})^{-1},$$

where the product is taken over all primes $\mathfrak{P}$ of L.

Hecke L-series

- Let $\psi : \mathbf{A}_L^\times \to \mathbb{C}^\times$ be a Hecke character. Attach to it the L-series

$$L(s,\psi) = \prod_{\mathfrak{P}} (1 - \psi(\mathfrak{P}) q_{\mathfrak{P}}^{-s})^{-1},$$

where the product is taken over all primes $\mathfrak{P}$ of L.

- This is the generalization of the Dirichlet L-function

$$L(s,\chi) = \prod_{p} (1 - \chi(p) p^{-s})^{-1}$$

associated to a Dirichlet character χ.

Hecke L-series

- Let $\psi : \mathbf{A}_L^\times \to \mathbb{C}^\times$ be a Hecke character. Attach to it the L-series

$$L(s,\psi) = \prod_{\mathfrak{P}} (1 - \psi(\mathfrak{P}) q_{\mathfrak{P}}^{-s})^{-1},$$

  where the product is taken over all primes $\mathfrak{P}$ of L.
- This is the generalization of the Dirichlet L-function

$$L(s,\chi) = \prod_{p} (1 - \chi(p) p^{-s})^{-1}$$

  associated to a Dirichlet character χ.
- Hecke (and later Tate, in his thesis) proved that $L(s,\psi)$
  - has analytic continuation to the to the entire complex plane, and

Hecke L-series

- Let $\psi : \mathbf{A}_L^\times \to \mathbb{C}^\times$ be a Hecke character. Attach to it the L-series

$$L(s, \psi) = \prod_{\mathfrak{P}} (1 - \psi(\mathfrak{P}) q_{\mathfrak{P}}^{-s})^{-1},$$

  where the product is taken over all primes $\mathfrak{P}$ of L.

- This is the generalization of the Dirichlet L-function

$$L(s, \chi) = \prod_{p} (1 - \chi(p) p^{-s})^{-1}$$

  associated to a Dirichlet character χ.

- Hecke (and later Tate, in his thesis) proved that $L(s, \psi)$
  - has analytic continuation to the to the entire complex plane, and

Hecke L-series

- Let $\psi : \mathbf{A}_L^\times \to \mathbb{C}^\times$ be a Hecke character. Attach to it the L-series

$$L(s,\psi) = \prod_{\mathfrak{P}} (1 - \psi(\mathfrak{P}) q_{\mathfrak{P}}^{-s})^{-1},$$

  where the product is taken over all primes $\mathfrak{P}$ of L.
- This is the generalization of the Dirichlet L-function

$$L(s,\chi) = \prod_{p} (1 - \chi(p) p^{-s})^{-1}$$

  associated to a Dirichlet character χ.
- Hecke (and later Tate, in his thesis) proved that $L(s,\psi)$
  - has analytic continuation to the to the entire complex plane, and
  - satisfies a functional equation $L(s,\psi) = \epsilon L(N - s, \psi^\vee)$ for some ϵ, N depending on ψ.

A conjecture on the L-series

- The L-series $L(E/L, s)$ of an elliptic curve E/L converges for $\Re s > 3/2$.

Conjecture

The L-series $L(E/L, s)$ has an analytic continuation to the entire complex plane and satisfies a functional equation relating $L(E/L, 2)$ and $L(E/L, 2 - s)$.

A conjecture on the L-series

- The L-series $L(E/L, s)$ of an elliptic curve E/L converges for $\Re s > 3/2$.

Conjecture

The L-series $L(E/L, s)$ has an analytic continuation to the entire complex plane and satisfies a functional equation relating $L(E/L, 2)$ and $L(E/L, 2-s)$.

- For E having CM, Deuring and Weil proved that

$$L(E/L, s) = L(s, \psi_{E/L})L(s, \overline{\psi_{E/L}}),$$

so by Hecke's result the conjecture is resolved.

A conjecture on the L-series

- The L-series $L(E/L, s)$ of an elliptic curve E/L converges for $\Re s > 3/2$.

Conjecture

The L-series $L(E/L, s)$ has an analytic continuation to the entire complex plane and satisfies a functional equation relating $L(E/L, 2)$ and $L(E/L, 2 - s)$.

- For E having CM, Deuring and Weil proved that

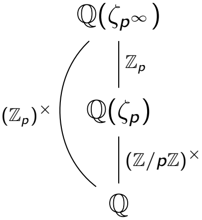
$$L(E/L, s) = L(s, \psi_{E/L})L(s, \overline{\psi_{E/L}}),$$

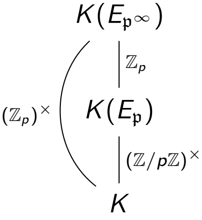
so by Hecke's result the conjecture is resolved.

- Works of Eichler, Shimura, and finally Wiles's modularity theorem resolves the case $E/\mathbb{Q}$.

Iwasawa theory of elliptic curves with CM

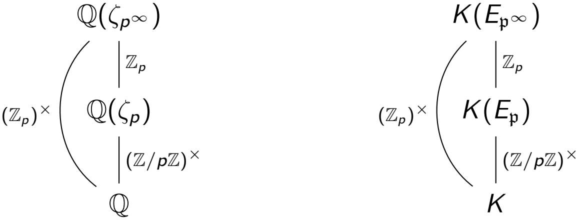
- In the classical Iwasawa theory we consider the infinite cyclotomic tower and study the p-adic analogue of Riemann zeta function.





Iwasawa theory of elliptic curves with CM

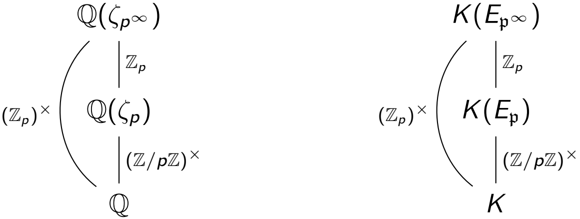
- In the classical Iwasawa theory we consider the infinite cyclotomic tower and study the p-adic analogue of Riemann zeta function.



- Substituting $\mathbb{Q}$ by K an imaginary quadratic field, the role of ζ_{p^n} is played by the $\mathfrak{p}^n$-torsion points on E.

Iwasawa theory of elliptic curves with CM

- In the classical Iwasawa theory we consider the infinite cyclotomic tower and study the p-adic analogue of Riemann zeta function.



- Substituting $\mathbb{Q}$ by K an imaginary quadratic field, the role of ζ_{p^n} is played by the $\mathfrak{p}^n$-torsion points on E.
- The p-adic $L(E,s)$ tells us the p-part of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$, which is helpful to understanding the BSD conjecture.

Outline of the talk

1. Number-theoretic background
2. CM of elliptic curves
3. Generalization to abelian Varieties
4. Acknowledgements

Facts about abelian varieties

- An **abelian variety** A/K is a connected projective group scheme over a field K (the $\overline{K}$-rational points $A(\overline{K})$ forms a group).

Facts about abelian varieties

- An **abelian variety** A/K is a connected projective group scheme over a field K (the $\overline{K}$-rational points $A(\overline{K})$ forms a group).
- Elliptic curves are one-dimensional abelian varieties.

Facts about abelian varieties

- An **abelian variety** A/K is a connected projective group scheme over a field K (the $\overline{K}$-rational points $A(\overline{K})$ forms a group).
- Elliptic curves are one-dimensional abelian varieties.
- Over $\mathbb{C}$, uniformization holds, but the converse does not! The obstruction is rectified by so-called **polarization**.

Facts about abelian varieties

- An **abelian variety** A/K is a connected projective group scheme over a field K (the $\overline{K}$-rational points $A(\overline{K})$ forms a group).
- Elliptic curves are one-dimensional abelian varieties.
- Over $\mathbb{C}$, uniformization holds, but the converse does not! The obstruction is rectified by so-called **polarization**.
- The category of abelian varieties with isogenies is semisimple, and $\mathrm{End}_{\mathbb{Q}}(A) := \mathrm{End}(A) \otimes \mathbb{Q}$ is a semisimple $\mathbb{Q}$-algebra.

Facts about abelian varieties

- An **abelian variety** A/K is a connected projective group scheme over a field K (the $\overline{K}$-rational points $A(\overline{K})$ forms a group).
- Elliptic curves are one-dimensional abelian varieties.
- Over $\mathbb{C}$, uniformization holds, but the converse does not! The obstruction is rectified by so-called **polarization**.
- The category of abelian varieties with isogenies is semisimple, and $\mathrm{End}_{\mathbb{Q}}(A) := \mathrm{End}(A) \otimes \mathbb{Q}$ is a semisimple $\mathbb{Q}$-algebra.
- Let B be a semisimple K-algebra. By Wedderburn-Artin theorem

$$B = \mathcal{M}_{n_i}(D_i).$$

Let K_i be the center of D_i, define the **reduced degree**

$$[B : K]_{\mathrm{red}} := [B_i : K_i]^{1/2}[K_i : K].$$

It is the degree of the maximal étale K-subalgebra of B.

Abelian variety with CM

Lemma 7

Notation as above, if M is a faithful B-module, then

$$\dim_K M \geq [B : K]_{\mathrm{red}},$$

with equality if and only if B_i are matrix algebras over K_i.

- Fix a uniformization $A \cong \mathbb{C}^g/\Lambda$. Interpret an analytic representation

$$\mathrm{End}_{\mathbb{Q}}(A) \cong \{M \in \mathcal{M}_g(\mathbb{C}) : M\mathbb{Q}\Lambda \subset \mathbb{Q}\Lambda\}.$$

Then $\mathbb{Q}\Lambda$ is a faithful $\mathrm{End}_{\mathbb{Q}}(A)$-module, so that

$$[\mathrm{End}_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}} \leq \dim_{\mathbb{Q}} \mathbb{Q}\Lambda = 2 \dim A.$$

Abelian variety with CM

Lemma 7

Notation as above, if M is a faithful B-module, then

$$\dim_K M \geq [B : K]_{\mathrm{red}},$$

with equality if and only if B_i are matrix algebras over K_i.

- Fix a uniformization $A \cong \mathbb{C}^g/\Lambda$. Interpret an analytic representation

$$\mathrm{End}_{\mathbb{Q}}(A) \cong \{M \in \mathcal{M}_g(\mathbb{C}) : M\mathbb{Q}\Lambda \subset \mathbb{Q}\Lambda\}.$$

  Then $\mathbb{Q}\Lambda$ is a faithful $\mathrm{End}_{\mathbb{Q}}(A)$-module, so that

$$[\mathrm{End}_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}} \leq \dim_{\mathbb{Q}} \mathbb{Q}\Lambda = 2 \dim A.$$

- We say that $A/\mathbb{C}$ has CM if equality holds.

CM-field

- A **CM-field** is an imaginary quadratic extension of a totally real field. Examples: $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$ and $\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_N + \overline{\zeta_N})$.

CM-field

- A **CM-field** is an imaginary quadratic extension of a totally real field. Examples: $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$ and $\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_N + \overline{\zeta_N})$.
- A **CM-algebra** is a finite product of CM-fields.

CM-field

- A **CM-field** is an imaginary quadratic extension of a totally real field. Examples: $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$ and $\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_N + \overline{\zeta_N})$.
- A **CM-algebra** is a finite product of CM-fields.
- By the lemma and the fact that A is semisimple, A has CM if and only if each of its simple factors has CM.

Theorem 8

An abelian variety $A/\mathbb{C}$ has CM if and only if

- *(if A is simple) $\mathrm{End}_{\mathbb{Q}}(A)$ is a CM-field of degree $2\dim A$ over $\mathbb{Q}$;*
- *(if A is isotypic) $\mathrm{End}_{\mathbb{Q}}(A)$ contains a field of degree $2\dim A$ over $\mathbb{Q}$;*
- *$\mathrm{End}_{\mathbb{Q}}(A)$ contains an étale $\mathbb{Q}$-subalgebra of dimension $2\dim A$.*

Moreover, the number field (resp. étale $\mathbb{Q}$-subalgebra) can be chosen to be a CM-field (resp. CM-algebra) invariant under the Rosati involution induced by a polarization of A.

Review: CM of elliptic curves

- Let us recall the main theorem of CM of elliptic curves.

Review: CM of elliptic curves

- Let us recall the main theorem of CM of elliptic curves.
- Let $K/\mathbb{Q}$ be an imaginary quadratic field.

Review: CM of elliptic curves

- Let us recall the main theorem of CM of elliptic curves.
- Let $K/\mathbb{Q}$ be an imaginary quadratic field.
- Let $E/\mathbb{Q}$ be an elliptic curve with CM by the rings of integers $\mathcal{O}_K$.

Review: CM of elliptic curves

- Let us recall the main theorem of CM of elliptic curves.
- Let $K/\mathbb{Q}$ be an imaginary quadratic field.
- Let $E/\mathbb{Q}$ be an elliptic curve with CM by the rings of integers $\mathcal{O}_K$.
- Let $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. Let $s \in \mathbf{A}_K^\times$ be an idèle with $[s, K] = \sigma|_{K^{\mathrm{ab}}}$.

Review: CM of elliptic curves

- Let us recall the main theorem of CM of elliptic curves.
- Let $K/\mathbb{Q}$ be an imaginary quadratic field.
- Let $E/\mathbb{Q}$ be an elliptic curve with CM by the rings of integers $\mathcal{O}_K$.
- Let $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. Let $s \in \mathbf{A}_K^\times$ be an idèle with $[s, K] = \sigma|_{K^{\mathrm{ab}}}$.
- Let $f : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C})$ be a complex-analytic isomorphism.

Theorem 9 (The main theorem of CM of elliptic curves)

There exists a unique complex-analytic isomorphism $f' : \mathbb{C}/(s)^{-1}\mathfrak{a} \xrightarrow{\sim} E^\sigma(\mathbb{C})$ *such that the following diagram commutes:*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{(s)^{-1}} & K/(s)^{-1}\mathfrak{a} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ E(\mathbb{C}) & \xrightarrow{\sigma} & E^\sigma(\mathbb{C}) \end{array}$$

The main theorem of CM of abelian varieties

- Let K be a CM-field of type (K, Φ).

The main theorem of CM of abelian varieties

- Let K be a CM-field of type (K, Φ).
- Let $(A, \iota, \mathcal{C})$ be a polarized CM abelian variety of type $(K, \Phi, \mathfrak{a}, \tau)$ with respect to an isomorphism $f : \mathbb{C}^g / u(\mathfrak{a}) \xrightarrow{\sim} A$.

The main theorem of CM of abelian varieties

- Let K be a CM-field of type (K, Φ).
- Let $(A, \iota, \mathcal{C})$ be a polarized CM abelian variety of type $(K, \Phi, \mathfrak{a}, \tau)$ with respect to an isomorphism $f : \mathbb{C}^g / u(\mathfrak{a}) \xrightarrow{\sim} A$.
- Let $\sigma \in \mathrm{Aut}(\mathbb{C}/K^*)$. Let $s \in \mathbf{A}_K^\times$ be an idèle with $[s, K^*] = \sigma|_{(K^*)^{\mathrm{ab}}}$.

Theorem 10 (The main theorem of CM of abelian varieties)

There is a unique isomorphism $\xi' : \mathbb{C}^g / u(\mathrm{Nm}_\Phi(s)^{-1}\mathfrak{a}) \xrightarrow{\sim} A^\sigma$ *such that* A^σ *is of type* $(K, \Phi, \mathrm{Nm}_\Phi(s)^{-1}\mathfrak{a}, \mathrm{Nm}_{K/\mathbb{Q}}((s))\tau)$ *with respect to* ξ'*, and the following diagram commutes:*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\mathrm{Nm}_\Phi(s)^{-1}} & K/\mathrm{Nm}_\Phi(s)^{-1}\mathfrak{a} \\ \downarrow{\scriptstyle \xi \circ u} & & \downarrow{\scriptstyle \xi' \circ u} \\ A & \xrightarrow{\sigma} & A^\sigma \end{array}$$

A little history

- The classical theory of CM was developed by Weber, Fueter, Hasse and Duering before 1950s.
- The main theorem we gave above was restricted over the reflex field K^*. It was due to Shimura, Taniyama, and Weil in the 1950s. It is sufficient for constructing class fields, though.
- The most general case over $\mathbb{Q}$ was proved by Langlands, Tate, and Deligne in the 1980s, also called motivic CM theory.

Outline of the talk

1. Number-theoretic background
2. CM of elliptic curves
3. Generalization to abelian Varieties
4. Acknowledgements

Acknowledgements

I'd like to thank my mentor Wei for introducing to me this fascinating topic to learn about. I thank both of my mentors, Wei and Pallav, for hostng weekly meetings with me and answering my endless questions. Finally, I thank Peter for giving me this opportunity.

Thanks for listening.

References I

[Mil20] J. S. Milne. *Complex Multiplication*. 2020.

[Shi71] Goro Shimura. *Introduction to Arithmetic Theory of Automorphic Functions.* Princeton University Press, 1971.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* GTM. Springer, 1994.