Complex Multiplication

Yunhan (Alex) Sheng

yhsheng@uchicago.edu

UChicago REU, August 2022

Outline of the talk

Number-theoretic background

- L/K is **abelian** if $\mathrm{Gal}(L/K)$ is an abelian group.

Number-theoretic background

- L/K is **abelian** if $\mathrm{Gal}(L/K)$ is an abelian group.
- Prime ideals $\mathfrak{p}$ in K split in L. For example, in $\mathbb{Q}(i)/\mathbb{Q}$,

$$(2) = (1-i)^2, \quad (3) = (3), \quad (5) = (2+i)(2-i).$$

We say that (2) is **ramified**, while (3) and (5) are **unramified**.

Number-theoretic background

- L/K is **abelian** if $\mathrm{Gal}(L/K)$ is an abelian group.
- Prime ideals $\mathfrak{p}$ in K split in L. For example, in $\mathbb{Q}(i)/\mathbb{Q}$,

$$(2) = (1-i)^2, \quad (3) = (3), \quad (5) = (2+i)(2-i).$$

  We say that (2) is **ramified**, while (3) and (5) are **unramified**.
- L/K is unramified if every prime in K is unramified in L

The case over $\mathbb{Q}$

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

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 $N > 0$.

- The maximal abelian extension of $\mathbb{Q}$ is generated by roots of unities.

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 $N > 0$.

- The maximal abelian extension of $\mathbb{Q}$ is generated by roots of unities.

Theorem 2 (Hermite-Minkowski)

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

- That is, the maximal unramified extension of $\mathbb{Q}$ is $\mathbb{Q}$.

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 $N > 0$.

- The maximal abelian extension of $\mathbb{Q}$ is generated by roots of unities.

Theorem 2 (Hermite-Minkowski)

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

- That is, the maximal unramified extension of $\mathbb{Q}$ is $\mathbb{Q}$.
- What if we change the base field to a finite extension of $\mathbb{Q}$ instead?

- This is known as the Hilbert's twelfth problem, or explicit CFT.

- This is known as the Hilbert's twelfth problem, or explicit CFT.
- **Complex Multiplication** resolves the case when the base field is an imaginary quadratic field, i.e., $\mathbb{Q}(\sqrt{-D})$ for some $D > 0$.

- This is known as the Hilbert's twelfth problem, or explicit CFT.
- **Complex Multiplication** resolves the case when the base field is an imaginary quadratic field, i.e., $\mathbb{Q}(\sqrt{-D})$ for some $D > 0$.
- These two are essentially the only known cases. The problem is wide open.

- This is known as the Hilbert's twelfth problem, or explicit CFT.
- **Complex Multiplication** resolves the case when the base field is an imaginary quadratic field, i.e., $\mathbb{Q}(\sqrt{-D})$ for some $D > 0$.
- These two are essentially the only known cases. The problem is wide open.
- Slogan: this piece of **arithmetic** information will be extracted from studying **geometric** objects, namely, elliptic curves.

Outline of the talk

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 $O \in E$;
  - naïvely, it is a smooth curve given by a cubic equation

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

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 $O \in E$;
  - naïvely, it is a smooth curve given by a cubic equation

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

- Elliptic curves are classified up to isomorphism by an numerical invariant called the j-**invariant**, denoted by $j(E)$.

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 $O \in E$;
  - naïvely, it is a smooth curve given by a cubic equation

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

- Elliptic curves are classified up to isomorphism by an numerical invariant called the j-**invariant**, denoted by $j(E)$.
- An elliptic curve can be endowed with a group structure.

Endomorphism of elliptic curves

- An endomorphism of an elliptic curve E is a morphism of varieties

$$\phi : E \to E \quad \text{such that} \quad \phi(O) = O.$$

Endomorphism of elliptic curves

- An endomorphism of an elliptic curve E is a morphism of varieties

$$\phi : E \to E \quad \text{such that} \quad \phi(O) = O.$$

- Example: the multiplication-by-m map $[m] : E \to E$ defined by

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

Endomorphism of elliptic curves

- An endomorphism of an elliptic curve E is a morphism of varieties

$$\phi : E \to E \quad \text{such that} \quad \phi(O) = O.$$

- Example: the multiplication-by-m map $[m] : E \to E$ defined by

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

- Question: are there endomorphisms other than maps of form $[m]$?

CM of elliptic curves

- Write $\mathrm{End}(E)$ for the endomorphism ring of E.

Theorem 3

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

CM of elliptic curves

- Write $\mathrm{End}(E)$ for the endomorphism ring of E.

Theorem 3

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

- An elliptic curve $E/\mathbb{C}$ has **complex multiplication by** R if $R = \mathrm{End}(E)$ is the subring of an imaginary quadratic field.

Construction of class fields

- Now we state the main result of CM of elliptic curves.

Theorem 4

Let K be an imaginary quadratic field. Let $E/\mathbb{C}$ be an elliptic curve with CM by ring of integers $\mathcal{O}_K$. Then

- $K(j(E))$ *is the maximal unramified extension of* K
- $K(j(E), x(E_{tors}))$ *is the maximal abelian extension of* K.

Construction of class fields

- Now we state the main result of CM of elliptic curves.

Theorem 4

Let K be an imaginary quadratic field. Let $E/\mathbb{C}$ be an elliptic curve with CM by ring of integers $\mathcal{O}_K$. Then

- $K(j(E))$ *is the maximal unramified extension of* K
- $K(j(E), x(E_{tors}))$ *is the maximal abelian extension of* K.

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

Prospect: Iwasawa theory of elliptic curves

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

$$\begin{tikzcd}
\mathbb{Q}(\zeta_{p^\infty}) \arrow[d, dash, "\mathbb{Z}_p"] \arrow[dd, dash, bend right=60, "(\mathbb{Z}_p)^\times"'] \\
\mathbb{Q}(\zeta_p) \arrow[d, dash, "(\mathbb{Z}/p\mathbb{Z})^\times"] \\
\mathbb{Q}
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
K(E_{\mathfrak{p}^\infty}) \arrow[d, dash, "\mathbb{Z}_p"] \arrow[dd, dash, bend right=60, "(\mathbb{Z}_p)^\times"'] \\
K(E_{\mathfrak{p}}) \arrow[d, dash, "(\mathbb{Z}/p\mathbb{Z})^\times"] \\
K
\end{tikzcd}$$

Prospect: Iwasawa theory of elliptic curves

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

$$\begin{tikzcd}
\mathbb{Q}(\zeta_{p^\infty}) \arrow[d, dash, "\mathbb{Z}_p"] \arrow[dd, dash, bend right=60, "(\mathbb{Z}_p)^\times"'] \\
\mathbb{Q}(\zeta_p) \arrow[d, dash, "(\mathbb{Z}/p\mathbb{Z})^\times"] \\
\mathbb{Q}
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
K(E_{\mathfrak{p}^\infty}) \arrow[d, dash, "\mathbb{Z}_p"] \arrow[dd, dash, bend right=60, "(\mathbb{Z}_p)^\times"'] \\
K(E_{\mathfrak{p}}) \arrow[d, dash, "(\mathbb{Z}/p\mathbb{Z})^\times"] \\
K
\end{tikzcd}$$

- 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.

Prospect: Iwasawa theory of elliptic curves

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

$$
\begin{tikzcd}
\mathbb{Q}(\zeta_{p^\infty}) \arrow[d, dash, "\mathbb{Z}_p"] \\
\mathbb{Q}(\zeta_p) \arrow[d, dash, "(\mathbb{Z}/p\mathbb{Z})^\times"] \\
\mathbb{Q} \arrow[uu, dash, bend left=60, "(\mathbb{Z}_p)^\times"]
\end{tikzcd}
\qquad
\begin{tikzcd}
K(E_{\mathfrak{p}^\infty}) \arrow[d, dash, "\mathbb{Z}_p"] \\
K(E_{\mathfrak{p}}) \arrow[d, dash, "(\mathbb{Z}/p\mathbb{Z})^\times"] \\
K \arrow[uu, dash, bend left=60, "(\mathbb{Z}_p)^\times"]
\end{tikzcd}
$$

- 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.
- We then study the p-adic L-series attached to an elliptic curve, which helps us understand the BSD conjecture.

Outline of the talk

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.
- Hence abelian varieties are higher-dimensional analogues of elliptic curves. They have a structure of an abelian group.

CM of abelian varieties

- In the case of abelian varieties, even defining complex multiplication requires quite some work.

CM of abelian varieties

- In the case of abelian varieties, even defining complex multiplication requires quite some work.
- A **CM-field** is an imaginary quadratic extension of a totally real field.

CM of abelian varieties

- In the case of abelian varieties, even defining complex multiplication requires quite some work.
- A **CM-field** is an imaginary quadratic extension of a totally real field.
- Examples: $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$ and $\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_N + \overline{\zeta_N})$ for $N > 2$.

CM of abelian varieties

- In the case of abelian varieties, even defining complex multiplication requires quite some work.
- A **CM-field** is an imaginary quadratic extension of a totally real field.
- Examples: $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$ and $\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_N + \overline{\zeta_N})$ for $N > 2$.
- A **CM-algebra** is a finite product of CM-fields.

CM of abelian varieties

- In the case of abelian varieties, even defining complex multiplication requires quite some work.
- A **CM-field** is an imaginary quadratic extension of a totally real field.
- Examples: $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$ and $\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_N + \overline{\zeta_N})$ for $N > 2$.
- A **CM-algebra** is a finite product of CM-fields.
- Roughly speaking, an abelian variety $A/\mathbb{C}$ has CM iff $\mathrm{End}(A) \otimes \mathbb{Q}$ contains a CM-algebra of dimension $2 \dim A$.

CM of abelian varieties

- In the case of abelian varieties, even defining complex multiplication requires quite some work.
- A **CM-field** is an imaginary quadratic extension of a totally real field.
- Examples: $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$ and $\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_N + \overline{\zeta_N})$ for $N > 2$.
- A **CM-algebra** is a finite product of CM-fields.
- Roughly speaking, an abelian variety $A/\mathbb{C}$ has CM iff $\mathrm{End}(A) \otimes \mathbb{Q}$ contains a CM-algebra of dimension $2 \dim A$.
- Sadly, we obtain some (not all!) finite abelian extensions of a CM-field.

A little history

- The classical theory of CM was developed by Weber, Fueter, Hasse and Duering before 1950s.

A little history

- The classical theory of CM was developed by Weber, Fueter, Hasse and Duering before 1950s.
- The main theorem of CM of abelian varieties over a reflex field was due to Shimura, Taniyama, and Weil in the 1950s. It is sufficient for constructing the class fields.

A little history

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

A little history

- The classical theory of CM was developed by Weber, Fueter, Hasse and Duering before 1950s.
- The main theorem of CM of abelian varieties over a reflex field was due to Shimura, Taniyama, and Weil in the 1950s. It is sufficient for constructing the class fields.
- The most general case, the main theorem over $\mathbb{Q}$, was proved by Langlands, Tate, and Deligne in the 1980s, called motivic CM theory.
- CM has deep relations with the BSD conjecture and other arithmetic theories.

A little history

- The classical theory of CM was developed by Weber, Fueter, Hasse and Duering before 1950s.
- The main theorem of CM of abelian varieties over a reflex field was due to Shimura, Taniyama, and Weil in the 1950s. It is sufficient for constructing the class fields.
- The most general case, the main theorem over $\mathbb{Q}$, was proved by Langlands, Tate, and Deligne in the 1980s, called motivic CM theory.
- CM has deep relations with the BSD conjecture and other arithmetic theories.
- It also has fruitful applications to cryptography.

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 hosting 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.