

618: Special Values

Nir Elber

Spring 2025

CONTENTS

How strange to actually have to see the path of your journey in order to make it.

—Neal Shusterman, [Shu16]

Contents	2
1 Explicit Class Field Theory	3
1.1 January 21	3
1.1.1 Overview	3
1.1.2 Complex Multiplication over \mathbb{C}	5
Bibliography	7
List of Definitions	8

THEME 1

EXPLICIT CLASS FIELD THEORY

*What we didn't do is make the construction at all usable in practice!
This time we will remedy this.*

—Kiran S. Kedlaya, [Ked21]

1.1 January 21

It is a surprise to everyone, but I made it on time. This course will have a mailing list because I cannot get access to canvas.

1.1.1 Overview

Let's begin with a rough overview of the course. Last semester, we defined the modular curve $Y(N)_{\mathbb{C}} = \Gamma(N) \backslash \mathcal{H}$ for $\Gamma(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ together with its compactification $X(N)_{\mathbb{C}}$. Note there are two actions.

- Rethinking this construction adelically makes it relatively straightforward to provide a Hecke action by the Hecke ring \mathbb{T} .
- Also, we learned that $Y(N)$ and $X(N)$ are defined over \mathbb{Q} , even though a priori we only defined their complex points as a Riemann surface; thus, there is a Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $X(N)$.

The importance of these two actions is that they are able to realize instances of the Langlands correspondence by comparing the two actions on $H_{\mathrm{et}}^{\bullet}(X(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_{\ell})$. This is a special case of a larger process involving Shimura varieties.

Let's explain where the Langlands correspondence is coming in. The point is that certain elliptic curves E can be realized as quotients of $X(N)$. Let f be a weight 2 eigenform for $\Gamma(N)$ defined over \mathbb{Q} . Then there is a one-dimensional quotient of $J(N) := \mathrm{Jac} X(N)$ onto some factor E_f , granting a composite

$$X(N) \rightarrow J(N) \rightarrow E_f.$$

Because both $X(N)$ and E_f are proper curves, and the map is non-constant, we conclude that this is a quotient. The moral of the story is that we are able to send an “automorphic” modular form to a “motivic” elliptic curve.

Remark 1.1 (Wiles–Taylor). It turns out that every elliptic curve is of the form E_f . However, this is a very hard theorem, and we won't need it for this class.

Remember that $Y(N)$ parameterizes elliptic curves; for example, this provides a good way to build the models over \mathbb{Q} . Explicitly, $Y(N)$ can be identified with the moduli space of elliptic curves E together with level- N structure, which amounts to a choice of isomorphism $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$. It should be considered rather coincidental that elliptic curves have appeared here twice. This vanishes in higher generality.

One benefit of having the moduli interpretation is that it tells us that some points of $X(N)$ are special. Namely, one may be interested in the CM elliptic curves in $Y(N) \subseteq X(N)$.

Definition 1.2 (complex multiplication). Fix an elliptic curve E . Then E is said to have *complex multiplication* if and only if $\text{End}(E)_{\mathbb{Q}}$ is larger than \mathbb{Q} . In this case, we may say that E admits complex multiplication by $K := \text{End}(E)_{\mathbb{Q}}$.

Remark 1.3. If an elliptic curve E has CM, then it turns out that $\text{End}(E)$ is an order of an imaginary quadratic number field. In short, this follows from a classification of the possible endomorphism algebras, which must be division algebras of bounded dimension equipped with a positive (Rosati) involution.

Remark 1.4. It turns out that the CM elliptic curves E in $X(1)$ with $\text{End}(E)_{\mathbb{Q}} = K$ for number field K has E defined over K^{ab} . We will prove this later.

Remark 1.5. If E has complex multiplication by K , then it turns out that the Galois representation lands in $T_K := \text{Res}_{K/\mathbb{Q}} \mathbb{G}_{m,K}$ embedded in $\text{GL}_{2,\mathbb{Q}}$. Roughly speaking, the CM points with complex multiplication by K are the image of the Shimura variety

$$\text{Sh}(T_K) \rightarrow \text{Sh}(\text{GL}_2).$$

The first topic in the class will focus on these CM points and the theory of complex multiplication of elliptic curves at large.

The last topic of the course combines the two (coincidental) appearances of elliptic curves. In particular, for a modular elliptic curve $X(N) \rightarrow E_f$, one can ask where the CM points of $X(N)$ go.

Definition 1.6 (Heegner point). Fix a modular elliptic curve $X(N) \rightarrow E_f$. Then a point on E_f is a *Heegner point* if and only if it is the image of a CM points from $X(N)$.

For example, one has the following roughly stated theorem.

Theorem 1.7 (Gross–Zagier). The Néron–Tate height pairing of two such Heegner points on E_f is non-vanishing if and only if the following hold.

- The sign $\varepsilon(f_K, 1)$ of the functional equation is -1 (so that $L(f_K, 1) = 0$).
- The derivative $L'(f_K, 1) \neq 0$.

Here, f_K denotes the base-change of f (defined over \mathbb{Q}) to K .

The moral of the story is that special values are related to Heegner points.

So far we have discussed the first and last topics of the course. Let's give some of our other topics. The first (and slightly shorter) half of the course will cover explicit class field theory.

- We will talk about explicit class field theory for imaginary quadratic fields K . Not only are CM points of $X(N)$ with CM by K defined over K^{ab} , it turns out that this CM theory can explicitly construct K^{ab} .

Namely, one finds that the j -invariant and torsion points together define K^{ab} . This is analogous to how the Kronecker–Weber theorem constructs \mathbb{Q}^{ab} by attaching the roots of unity, which are torsion points of $\mathbb{G}_{m, \mathbb{Q}}$.

- Locally, Lubin and Tate constructed the maximal abelian extension of a p -adic field K_v . This is inspired by the above CM theory, but it cannot be done globally over number fields. (Roughly speaking, one can localize the previous construction, but then if one wants to only recover the totally ramified part of K_v^{ab} , one is allowed to only talk about the formal group.) It turns out that one can also use this theory to talk a little about nonabelian extensions; we may or may not mention this.
- However, one can extend these notions to work globally over function fields. This gives rise to the story to geometric class field theory and the theory of shtukas. The goal here is to have some basic notions so that we can listen in during seminars.

The second (and slightly longer) half of the course will build towards the Gross–Zagier formula. We will talk about special values in the special case of a torus T embedding in GL_2 .

- The standard L -functions due to Hecke arise from the split maximal torus T inside GL_2 . One can also define the Rankin–Selberg L -function attached to modular forms.
- Waldspurger’s formula, which roughly speaking tells us that $L(f_K, 1)$ is nonzero if and only if the functional

$$f_0 \mapsto \int_{T(\mathbb{Q}) \backslash T(\mathbb{A}_{\mathbb{Q}})} f_0$$

is nonzero, where we are realizing our functional on the base-change of f . There are two proofs of this result: Waldspurger’s original proof by the theta correspondence, and Jacquet’s proof using the relative trace formula. We will try to talk about both of them.

- Lastly, we will return to arithmetic from automorphic considerations and discuss the Gross–Zagier formula. The original proof of Gross and Zagier (later generalized by Yuan, Zhang, and Zhang) is based on the theta correspondence. There is another proof due to (Wei) Zhang based on an arithmetic relative trace formula.

1.1.2 Complex Multiplication over \mathbb{C}

Fix an elliptic curve E defined over an algebraically closed field K . Then $\text{End}(E)_{\mathbb{Q}}$ can be \mathbb{Q} , an imaginary quadratic number field, or an order of a quaternion algebra. To see this, one needs to bound $\dim_{\mathbb{Q}} \text{End}(E)_{\mathbb{Q}}$, which is not totally trivial. This is due to Tate.

Theorem 1.8 (Tate). Fix an elliptic curve E defined over an algebraically closed field K , and choose a prime ℓ not dividing $\text{char } K$. Then $\text{End}(E)$ is a free \mathbb{Z} -module, and the Tate module construction provides an embedding

$$\text{End}(E) \hookrightarrow \text{End}(T_{\ell}E).$$

Remark 1.9. Because $T_{\ell}E \cong \mathbb{Z}_{\ell}^2$, this tells us that $\text{End}(E)$ needs to be split at ℓ . However, $\text{End}(E)$ itself must be non-split (namely, not $M_2(\mathbb{Q})$) because $\text{End}(E)_{\mathbb{Q}}$ is a division algebra.

Remark 1.10. In characteristic 0, one can realize E over \mathbb{C} as \mathbb{C}/Λ for some lattice Λ . Then one is able to explicitly compute $\text{End } E$, thereby ruling out the third possibility.

We now see that E having complex multiplication needs to be a free \mathbb{Z} -submodule of K , which is an order \mathcal{O} . It turns out that \mathcal{O} needs to be contained in \mathcal{O}_K : everything in \mathcal{O} satisfies a monic quadratic equation by taking the characteristic polynomial, so \mathcal{O} is integral over \mathbb{Z} .

Definition 1.11 (conductor). Fix an order \mathcal{O} inside \mathcal{O}_K for some imaginary quadratic field K . For dimension reasons, one can write $\mathcal{O} = \mathbb{Z} + f\mathbb{Z}$ for some $f \in \mathcal{O}$, which is called the *conductor*.

Remark 1.12. Over \mathbb{C} , one writes $E(\mathbb{C}) = \mathbb{C}/\Lambda$ for some lattice $\Lambda \subseteq \mathbb{C}$. Up to homothety, we may write $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ for some $\tau \in \mathcal{H}$, and then the automorphisms are the homotheties of Λ . Then one finds that E has complex multiplication by K if and only if $\tau \in K$ by computing the automorphism group of this lattice.

Here is one example.

Example 1.13. Take $\Lambda = \mathcal{O}$ for some order \mathcal{O} . Then \mathbb{C}/Λ has complex multiplication by \mathcal{O} by construction.

However, there may be other examples, even up to homothety, roughly speaking due to the failure of class number 1.

Definition 1.14 (proper). Fix an order \mathcal{O} of an imaginary quadratic field K . A *proper fractional ideal* I of \mathcal{O} is a sublattice $I \subseteq K$ which is stable under \mathcal{O} and such that $\text{End}(\mathbb{C}/I) = \mathcal{O}$.

This gives the following bijection.

Proposition 1.15. Fix an order \mathcal{O} of an imaginary quadratic field K . Isomorphism classes of elliptic curves E with complex multiplication by \mathcal{O} are in bijection with the set of proper fractional ideals $I \subseteq \mathcal{O}$ taken modulo the principal ideals (i.e., scaling by \mathcal{O}).

Proof. For the forward map, write E as \mathbb{C}/Λ , write Λ (up to scaling in \mathbb{C}) as $\mathbb{Z} + \tau\mathbb{Z} \subseteq K$, and then the order is $\mathbb{Z} + \tau\mathbb{Z}$. For the backward map, take E as \mathbb{C}/\mathcal{O} . ■

When $\mathcal{O} = \mathcal{O}_K$, we see that the second set is the class group of \mathcal{O}_K . This motivates the following definition.

Definition 1.16. Fix an order \mathcal{O} of an imaginary quadratic field K . We let $\text{Cl}(\mathcal{O})$ denote the set of proper fractional ideals $I \subseteq \mathcal{O}$ taken modulo the principal ideals.

Later in the course, we will see that all these elliptic curves are defined over K^{ab} ; for example, when $\mathcal{O} = \mathcal{O}_K$, we find that \mathbb{C}/\mathcal{O} is defined over the Hilbert class field of K . More precisely, we will have a main theorem of complex multiplication.

Theorem 1.17. Fix an imaginary quadratic field K , and let H denote the Hilbert class field. Then $\sigma \in \text{Gal}(H/K)$ corresponds to some ideal class $\mathfrak{a} \subseteq \mathcal{O}_K$. Then E given by \mathcal{O}_K twisted by $\sigma^{\pm 1}$ is isomorphic to E given by \mathfrak{a} .

Notably, we need to pay attention to the Galois structure here, so we cannot over \mathbb{C} the entire time. Thus, we need to retell our story of complex multiplication beginning with a more abstract theory from algebraic geometry.

BIBLIOGRAPHY

- [Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.
- [Ked21] Kiran S. Kedlaya. *Notes on Class Field Theory*. 2021. URL: <https://kskedlaya.org/papers/cft-ptx.pdf>.

LIST OF DEFINITIONS

complex multiplication, [4](#)

conductor, [6](#)

Heegner point, [4](#)

proper, [6](#)