MTH697-MTH698

Elliptic Curves with Complex Multiplication and Heegner Points

Professor: Somnath Jha
Notes By: Ajay Prajapati

Autumn 2021

This report is expository in nature and no new result is being claimed.

ABSTRACT

This report is part of a year-long reading project on the topic "Heegner Points" under the guidance of Dr. Somnath Jha, IIT Kanpur. The Birch and Swinnerton-Dyer(BSD) conjecture is one of the central problems in the Theory of Elliptic Curves. This was formulated in 1960's based on the numerical evidence found by Bryan Birch and Peter Swinnerton Dyer. Although many were skeptical of it at the time, a major breakthrough came in 1970's when John Coates and Andrew Wiles proved it in a certain special case. This generated a lot of interest and soon, another major breakthrough came through the works of Gross-Zagier and Kolyvagin. In this report, we will cover the prerequisites required to understand this work.

Contents

1 Introduction **1**

2 Arithmetic Invariants of an Elliptic Curve **3**
2.1 The Regulator 3
2.2 The Conductor 3
2.3 The Weil-Châtelet Group 4
2.4 The Tate-Shafarevich Group 5

3 Class Field Theory **7**
3.1 Main theorems of CFT 7
3.2 The Idelic Approach to CFT 9

4 Complex Multiplication **10**
4.1 Properties of CM Elliptic Curves 10
4.2 The Main Theorem of Complex Multiplication 13
4.3 The Associated Grössencharacter 14
4.4 The L-Series Attached to a CM Elliptic Curve 17

5 Future Work **21**
5.1 Modular Curves 21
5.2 Weil Curves and the Modularity Theorem 22
5.3 The Congruent Number & The Class Number 1 Problems 22
5.4 Heegner Points 23
5.5 The Theorems of Gross-Zagier and Kolyvagin 25

§1. Introduction

Let L be an number field and E/L be an elliptic curve (EC) and $E(L) \subset E(\bar{L})$ is the group of L-rational points. A fundamental result in the study of ECs is the Mordell-Weil theorem.

Theorem 1.1. (Mordell-Weil theorem) The group $E(L)$ is finitely generated abelian group.

By the structure theorem of finitely generated abelian groups, we have the decomposition

$$E(L) \cong \mathbb{Z}^r \oplus E(L)_{tors}$$

Here r is called the (algebraic) *rank* of $E(L)$ and $E(L)_{tors}$ is the *torsion subgroup* of $E(L)$. The $E(L)_{tors}$ part is well understood. In fact, when $L = \mathbb{Q}$, we have the following deep theorem:

Theorem 1.2. (Mazur Torsion theorem, 1978) Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{tors}$ is one of the following forms:

- $E(\mathbb{Q})_{tors} \cong \frac{\mathbb{Z}}{N\mathbb{Z}}$ with $1 \leq N \leq 10$ or $N = 12$.
- $E(\mathbb{Q})_{tors} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2N\mathbb{Z}}$ with $1 \leq N \leq 4$.

In other words, $\#E(\mathbb{Q})_{tors}$ is uniformally bounded by 16 for $L = \mathbb{Q}$. For other number fields, a similar result holds true which was fully proven by Merel in 1995. On the other hand, the rank is very mysterious and there are many unsolved conjectures about it even when $L = \mathbb{Q}$. Most prominent of those is the Birch and Swinnerton-Dyer (BSD) conjecture which was first made in 1965 [BSD65] and made precise in the subsequent years. In order to state it, first we define L-series associated to E/L.

Definition 1.3. If E has good reduction at $\mathfrak{P}$, we define,

$$L_{\mathfrak{P}}(E/L, T) := 1 - a_{\mathfrak{P}}T + q_{\mathfrak{P}}T^2 \text{ where } a_{\mathfrak{P}} := q_{\mathfrak{P}} + 1 - \#\tilde{E}\left(\mathbb{F}_{\mathfrak{P}}\right)$$

$L_{\mathfrak{P}}(E/L, T)$ is called the *local L-series* of E at $\mathfrak{P}$. If E has bad reduction at $\mathfrak{P}$, we define

$$L_{\mathfrak{P}}(E/L, T) := \begin{cases} 1 - T & \text{if } E \text{ has split multiplicative at } \mathfrak{P}. \\ 1 + T & \text{if } E \text{ has non-split multiplicative at } \mathfrak{P}. \\ 1 & \text{if } E \text{ has additive reduction at } \mathfrak{P} \end{cases} \tag{1.1}$$

The *(global) L-series* of E/L is defined by the Euler product

$$L(E/L, s) := \prod_{\mathfrak{P}} L_{\mathfrak{P}}\left(E/L, q_{\mathfrak{P}}^{-s}\right)^{-1} \tag{1.2}$$

The *analytic rank* of E/L is defined as the order of vanishing of $L(E/L, s)$ at $s = 1$.

Using Hasse-Weil bound, $L(E/L, s)$ is easily seen to be an analytic function on $Re(s) > \frac{3}{2}$.

[BSD Conjecture] Let $E/\mathbb{Q}$ be an elliptic curve and $L(E/\mathbb{Q}, s)$ be its L-function. Then

1. Algebraic rank of E is equal to its analytic rank. i.e.,
$$\text{rank}(E(\mathbb{Q})) = \text{ord}_{s=1} L(E/\mathbb{Q}, s) (= r \text{ say}) \tag{1.3}$$
2. The leading term in the Laurent expansion of $L(E/\mathbb{Q}, s)$ at $s = 1$ is given in terms of the arithmetic invariants of E. More precisely,
$$\frac{L^r(E/\mathbb{Q}, 1)}{r!} = \frac{\#Ш(E/\mathbb{Q})\Omega_E R_E}{(\#E(\mathbb{Q})_{tors})^2} \prod_p c_p \quad \text{where} \tag{1.4}$$
   (a) $Ш(E/\mathbb{Q})$ is the *Tate-Shafareviech group* of E,
   (b) R_E is the *regulator* of E,
   (c) Ω_E is a certain integer multiple of the *least real period of* E, and
   (d) local indicies c_p's are called the *Tamagawa factors* (or *fudge factors*) of E, defined by
   $$c_p := [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$$
   where $E_0(\mathbb{Q}_p)$ is the subgroup of $E(\mathbb{Q}_p)$ consisting of those points whose reduction modulo p (on a minimal model of E) is non-singular.

It is remarkable to note that when this conjecture first appeared in 1965, it was not even known whether $L(E/\mathbb{Q}, s)$ is defined at $s = 1$ (this is now known as a consequence of the Modularity theorem, fully proven in 2000's). Even now, it is not known whether $Ш(E/\mathbb{Q})$ is finite or not. Also note that the (2) part has striking resemblance with another well known formula in number theory:

[Analytic Class Number Formula] For K a number field, the Dedekind zeta function $\zeta_K(s)$ has meromorphic continuation to all of $\mathbb{C}$ with only one simple pole at $s = 1$ with residue
$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot \text{Reg}_K \cdot h_K}{w_K \cdot \sqrt{|D_K|}} \tag{1.5}$$
where h_K is the class number, Reg_K is the regulator of K, r_1- number of real embeddings, $2r_2$- number of non-real embeddings, w_k- number of roots of unity in K.

In this report, we will start with defining the regulator, the conductor, and the Tate-Shafarevich group of an EC (section 2). Then we will restrict our attention to the so-called CM ECs: ECs over $\mathbb{C}$ with endomorphism ring strictly larger than $\mathbb{Z}$. These curves have many beautiful properties (section 4). Then we will prove the analytic continuation the L-function of a CM EC, a result which was proved by Deuring in 1940's. At the end, we will define Heegner points on ECs and briefly outline the work to be done in the next semester (section 5).

§2. Arithmetic Invariants of an Elliptic Curve

In this section, we first define the regulator and conductor of an EC. Then we define the Tate-Shafarevich group. But in order to properly understand the Tate-Shafarevich group, we will first need to understand the *Weil-Châtelet group* of an EC (2.3). We will assume familarity with elementary group cohomology in (2.3) and (2.4) and will be based on [Sil86], Ch X.

§§2.1. The Regulator

The regulator of an elliptic curve is an important arithmetic invariant, which can be compared to the regulator of a number field. In order to define it, we first recall the properties of the canonical height function:

Notation: Let E be an elliptic curve over a number field K with algebraic closure $\bar{K}$.

Theorem 2.1. The canonical height $\hat{h}$ of Neron and Tate on E satisfies the following:

1. $\hat{h}(P+Q)+\hat{h}(P-Q)=2\hat{h}(P)+2\hat{h}(Q) \quad \forall P,Q\in E(\bar{K})$. **(Parallelogram Law)**
2. $\hat{h}([n]P)=n^2\hat{h}(P) \quad \forall P\in E(\bar{K}), \quad \forall n\in\mathbb{Z}$.
3. $\hat{h}$ gives rise to the **Neron-Tate height pairing**

$$\langle , \rangle : E(\bar{K})\times E(\bar{K}) \longrightarrow \mathbb{R}, \quad \langle P,Q\rangle = \hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q)$$

4. $\hat{h}(P)\geq 0$ for all $P\in E(\bar{K})$, and $\hat{h}(P)=0 \iff P$ is a torsion point.

By Mordell-Weil Theorem, $E(K)\otimes\mathbb{R}$ is a finite dimensional vector space. And we can consider $E(K)/E(K)_{\text{tors}}$ as a complete lattice in $E(K)\otimes\mathbb{R}$. The *regulator* of E/K is the volume of a fundamental domain of $E(K)/E(K)_{\text{tors}}$ w.r.t the Neron-Tate height pairing. More formally,

Definition 2.2. The $R_{E/K}$ *regulator* of E/K is defined as

$$R_{E/K} := \det\left(\langle P_i,P_j\rangle\right)_{1\leq i\leq r,1\leq j\leq r}$$

where $P_1,P_2,\ldots,P_r\in E(K)$ be a set of generators for $E(K)/E(K)_{\text{tors}}$.

§§2.2. The Conductor

The conductor of E/K is an arithmetic invariant which encodes the primes primes of bad reduction. Unfortunately, understanding it completely requires the knowledge of Néron models which is a difficult topic. But we can state the final result:

Definition 2.3. The *conductor* of E/K is an integral ideal defined by

$$N_{E/K} := \prod_v \mathfrak{p}_v^{f_v}$$

where v runs over all finite places and for a finite place v, f_v is defined as

$$f_v := \begin{cases} 0 & \text{if } E \text{ has good reduction at } v \\ 1 & \text{if } E \text{ has multiplicative reduction at } v \\ 2+\delta_v & \text{if } E \text{ has additive reduction at } v \end{cases}$$

where δ_v is a measure of the "wild ramification" in the action of the inertia group I_v on $T_\ell(E)$. If $\mathfrak{p}_v \nmid 2, 3$ then $\delta_v = 0$. (see [Sil86], C§16)

§§2.3. The Weil-Châtelet Group

The only ineffective part in determination of the Mordell-Weil group of an EC is the determination of the Weak Mordell-Weil group which basically depends on knowing the existence (or non-existence) of rational points on certain curves associated to the EC.

Definition 2.4. Let E/K be an elliptic curve. A *(principal) homogeneous space* for E/K is a smooth curve C/K together with a **simply transitive algebraic group action** of E on C defined over K. In other words, a homogeneous space for E/K is a pair (C, μ), where C/K is a smooth curve and $\mu : C \times E \longrightarrow C$ is a morphism over K having the following properties:

1. μ is a group action.
2. For all $p, q \in C$ there is a unique $P \in E$ such that $\mu(p, P) = q$.

Definition 2.5. Two homogeneous spaces C/K and C'/K for E/K are *equivalent* if there is an isomorphism $\theta : C \longrightarrow C'$ defined over K that is compatible with the action of E on C and C'. i.e., the following diagram commutes

$$\begin{array}{ccc} C \times E & \longrightarrow & C \\ \downarrow{\scriptstyle \theta \times id} & & \downarrow{\scriptstyle \theta} \\ C' \times E & \longrightarrow & C' \end{array}$$

The equivalence class containing E/K, acting on itself by translation, is called the *trivial class*. The set of equivalence classes of homogeneous spaces for E/K is called the *Weil-Châtelet group* for E/K denoted by $\mathrm{WC}(E/K)$. (see theorem 2.7 for the group structure)

Here are some interesting results about homogeneous spaces and the Weil-Châtelet group.

Theorem 2.6. Let C/K be a homogeneous space for E/K. Then

$$C/K \text{ is in the trivial class} \iff C(K) \text{ is not the empty set.}$$

Theorem 2.7. There is a natural bijection $\mathrm{WC}(E/K) \longrightarrow H^1(\mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K}), E)$.

§§2.4. The Tate-Shafarevich Group

Let K be a number field, M_K be a complete set of inequivalent absolute values on K, K_v is the completion of K at $v \in M_K$, and E/K, E'/K are two isogenous ECs with $\phi : E \longrightarrow E'$ an isogeny. We start with a short exact sequence (SES) of $G = \mathrm{Gal}(\bar{K}/K)$-modules

$$0 \longrightarrow E[\phi] \longrightarrow E(\bar{K}) \xrightarrow{[\phi]} E'(\bar{K}) \longrightarrow 0$$

Using Galois Cohomology, we obtain the following long exact sequence (LES) (connecting homomorphism is δ_E)

$$\begin{array}{l} 0 \longrightarrow E(K)[\phi] \longrightarrow E(K) \xrightarrow{\phi} E'(K) \curvearrowright \\ \quad \hookrightarrow H^1(G, E[\phi]) \longrightarrow H^1(G, E(\bar{K})) \longrightarrow H^1(G, E'(\bar{K})) \end{array}$$

We extract the following SES, which is called the *Kummer sequence* for E/K:

$$0 \longrightarrow \frac{E'(K)}{\phi(E(K))} \xrightarrow{\delta_E} H^1(G, E[\phi]) \xrightarrow{\psi} H^1(G, E(\bar{K}))[\phi] \longrightarrow 0$$

Remark 2.8. Note that by 2.7, the last term in above SES may be identified with the ϕ-torsion in the Weil-Châtelet group $\mathrm{WC}(E/K)$. Now the above SES has a very elegant interpretation:

$$\begin{array}{rcl} \text{Determining the group } E'(K)/\phi(E(K)) & \iff & \text{knowing its image under } \delta_E \\ & \iff & \text{knowing the kernel of the map } \psi \\ & \iff & \text{knowing whether a } K\text{-rational point exists or} \\ & & \text{not on each of the homogeneous spaces} \end{array}$$

This last equivalence is a consequence of the theorem 2.6. Note that (theoretically) it is easy to determine all the homogeneous spaces of a given EC and also easy to determine a point in $E'(K)/\phi(E(K))$ given a K-rational point on some homogeneous space.

So the only thing remains is to determine whether a K-rational point exists or not on a homogeneous space. Recall the *Hasse-Minkowski theorem* which is an example of the local-global principle. Here also, to introduce local fields into the picture, we do following: For each $v \in M_K$ we fix an extension of v to $\bar{K}$, which serves to fix an embedding $\bar{K} \subset \bar{K}_v$ and a decomposition group $G_v \subset \mathrm{Gal}(\bar{K}/K)$. Replacing K to K_v in above, we get

$$0 \longrightarrow \frac{E'(K_v)}{\phi(E(K_v))} \xrightarrow{\delta} H^1(G_v, E[\phi]) \longrightarrow H^1(G_v, E(\bar{K}_v))[\phi] \longrightarrow 0$$

The natural inclusions $G_v \subset \mathrm{Gal}(\bar{K}/K)$ and $E(\bar{K}) \subset E(\bar{K}_v)$ give restriction maps on cohomology. Thus we get the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E'(K)}{\phi(E(K))} & \xrightarrow{\delta_E} & H^1(G, E[\phi]) & \longrightarrow & \mathrm{WC}(E/K)[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_{v\in M_K} \frac{E'(K_v)}{\phi(E(K_v))} & \xrightarrow{\delta} & \prod_{v\in M_K} H^1(G_v, E[\phi]) & \longrightarrow & \prod_{v\in M_K} \mathrm{WC}(E/K_v)[\phi] & \longrightarrow & 0 \end{array}$$

Definition 2.9. Let $\phi : E/K \to E'/K$ be an isogeny. The *ϕ-Selmer group* of E/K is the subgroup of $H^1\left(\mathrm{Gal}(\bar{K}/K), E[\phi]\right)$ defined by

$$S^{(\phi)}(E/K) = \ker\left\{H^1\left(\mathrm{Gal}(\bar{K}/K), E[\phi]\right) \longrightarrow \prod_{v\in M_K} \mathrm{WC}\left(E/K_v\right)\right\} \tag{2.1}$$

The *Shafarevich-Tate group* of E/K is the subgroup of $\mathrm{WC}(E/K)$ defined by

$$Ш(E/K) = \ker\left\{\mathrm{WC}(E/K) \longrightarrow \prod_{v\in M_K} \mathrm{WC}\left(E/K_v\right)\right\} \tag{2.2}$$

Meaning of these groups: By theorem 2.6, the Selmer group contains those homogeneous spaces which has atleast one K_v-rational point for each valuation v and the Tate-Shafarevich group contains those homogeneous spaces in the Selmer group which does not have a K-rational point. So, the Tate-Shafarevich group measures the extent of failure of the local-global principle. This group is known to be non-trivial for a family of elliptic curves (see [Sil86], X.6.5).

The following is a fundamental conjecture about $Ш(E/K)$.

(Conjecture) The Tate-Shafarevich group of an elliptic curve is finite.

§3. Class Field Theory

We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. In particular, it is abelian. The **Kronecker-Weber theorem** gives a partial converse to this fact:

Theorem 3.1. If $K/\mathbb{Q}$ is an abelian extension, then $K \subset \mathbb{Q}(\zeta_n)$ for some n.

One can similarly ask about characterization of abelian extensions of other fields of arithmetic interest and this is answered in Class Field Theory(CFT), although very abstractly. In the next section, we will see how the Theory of Complex Multiplication can be used to obtain explicit description of abelian extensions of quadratic imaginary fields. Our main reference for this section is [Cox03], chapter VII.

Let L/K be a finite Galois extension of number fields, $\mathfrak{P}|\mathfrak{p}$ be a prime extension, and $\kappa = \mathcal{O}_K/\mathfrak{p}$, $\lambda = \mathcal{O}_L/\mathfrak{P}$ are the residue fields. Recall from Algebraic Number Theory that we have a *surjective* homomorphism

$$D_{\mathfrak{P}} \twoheadrightarrow \mathrm{Gal}\,(\lambda/\kappa)\,, \quad \sigma \longmapsto \tilde{\sigma}$$

where $D_{\mathfrak{P}} \subset \mathrm{Gal}(L/K)$ is the decomposition group associated to $\mathfrak{P}$. The kernel of this map is the inertia group associated to $\mathfrak{P}$, denoted by $I_{\mathfrak{P}}$.

Now suppose that $\mathfrak{P}|\mathfrak{p}$ is unramified. Then $I_{\mathfrak{P}} = 0$, i.e., the above map is an isomorphism. Since the residue fields are finite, λ/κ is cyclic, and therefore there exists an unique element $\left(\frac{L/K}{\mathfrak{P}}\right) \in D_{\mathfrak{P}}$, called the *Artin symbol*, which maps to the *Frobenious automorphism* of λ/κ.

Morover, if L/K is abelian then the Artin symbol for $\mathfrak{P}$ only depends on the prime below, $\mathfrak{p}$ and not on $\mathfrak{P}$. Therefore, it is denoted by $\left(\frac{L/K}{\mathfrak{p}}\right)$.

§§3.1. Main theorems of CFT

For a number field K, let I_K and P_K denote respectively the group of non-zero fractional and principal-fractional ideals of K.

Definition 3.2. A *modulus* in K is a formal product $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ over all primes $\mathfrak{p}$, finite or infinite, where $n_{\mathfrak{p}} \geq 0$ and at most finitely many are nonzero, $n_{\mathfrak{p}} \leq 1$ if $\mathfrak{p}$ is real infinite, and $n_{\mathfrak{p}} = 0$ if $\mathfrak{p}$ is complex infinite.

Given a modulus $\mathfrak{m}$, we can write it as $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$. We define

$$I_K(\mathfrak{m}) := \{\mathfrak{a} \in I_K : \mathfrak{a} \text{ is relatively prime to } \mathfrak{m}\}$$
$$P_{K,1}(\mathfrak{m}) := \langle \alpha\mathcal{O}_K : \alpha \in \mathcal{O}_K \text{ and } \alpha \equiv 1 \pmod{\mathfrak{m}_0}, \sigma(\alpha) > 0\rangle$$

Definition 3.3. A subgroup $H \subset I_K(\mathfrak{m})$ is called a *congruence subgroup* for $\mathfrak{m}$ if it satisfies

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$$

and the quotient $I_K(\mathfrak{m})/H$ is called a *generalized ideal class group* for $\mathfrak{m}$.

Let L/K be an abelian extension and $\mathfrak{m}$ be a modulus divisible by all primes of K, finite or infinite that ramify in L.

Definition 3.4. Then the homomorphism (extends by multiplicativity)

$$\Phi_{\mathfrak{m},L/K} : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K), \quad \mathfrak{p} \longmapsto \left(\frac{L/K}{\mathfrak{p}}\right)$$

is called the *Artin map* for L/K and $\mathfrak{m}$. (omit L/K if clear from context)

The following result regarding the Artin map is called the **Artin Reciprocity Theorem**:

Theorem 3.5.
1. The Artin map $\Phi_{\mathfrak{m}}$ is surjective.
2. If the exponents of the finite primes $\mathfrak{m}$ are sufficiently large, then $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$, and hence $\mathrm{Gal}(L/K)$ is a generalized ideal class group for the modulus $\mathfrak{m}$.

The above theorem is true for many moduli $\mathfrak{m}$ but there is one modulus which is better than all the others, called the *conductor* of L/K:

Theorem 3.6. (Conductor Theorem) There is a modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ such that
1. A prime of K, finite or infinite, ramifies in $L \iff$ it divides $\mathfrak{f}$.
2. Let $\mathfrak{m}$ be a modulus divisible by all primes of K which ramify in L. Then $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m} \iff \mathfrak{f}|\mathfrak{m}$.

Theorem 3.7. (Existence Theorem): Let $\mathfrak{m}$ be a modulus of K, and let H be a congruence subgroup for $\mathfrak{m}$, i.e., $P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$. Then there is a unique Abelian extension L of K, all of whose ramified primes, finite or infinite, divide $\mathfrak{m}$, such that kernel of Artin map $\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$ is H.

Given any modulus $\mathfrak{m}$, the Existence theorem shows that there is a unique abelian extension $K_{\mathfrak{m}}$ of K such that $P_{K,1}(\mathfrak{m}) = \ker(\Phi_{K_{\mathfrak{m}}/K,\mathfrak{m}})$. $K_{\mathfrak{m}}$ is called the *ray class field* for the modulus $\mathfrak{m}$.

Thus the ray class field $K_{\mathfrak{m}}$ is characterized by the property that it is an abelian extension of K and primes which split completely in it are precisely the primes in $P_{K,1}(\mathfrak{m})$.

Example 3.1. The ray class field for the modulus $\mathfrak{m} = 1$ is called the *Hilbert Class Field* H of K characterized by the property that it is everywhere unramified maximal abelian extension.

Theorem 3.8. Let $\mathfrak{p}$ be a prime in K. Then $\left(\frac{L/K}{\mathfrak{p}}\right) = 1 \iff \mathfrak{p}$ is principal.

§§3.2. The Idelic Approach to CFT

This subsection is based on [Sil94], chapter II.3.

Let K be a number field, and for each absolute value v on K, let R_v be the ring of integers of K_v if v is non-archimedean, and let $R_v = K_v$ otherwise. The idele group of K is the group

$$\mathbf{A}_K^* = \prod_{v \in M_K}{}' K_v^* \tag{3.1}$$

where prime indicates that the product is restricted relative to the R_v 's. This means that an element $s \in \prod K_v^*$ in the unrestricted product is in $\mathbf{A}_K^*$ if and only if $x_v \in R_v^*$ for all but finitely many v.

Definition 3.9. Let $s \in \mathbf{A}_K^*$ be an idele. We define the ideal of s to be the fractional ideal of K given by $(s) := \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}\, s_p}$.

If L/K is a finite extension, then there is a natural norm map from $\mathbf{A}_L^*$ to $\mathbf{A}_K^*$. This is a continuous homomorphism

$$\mathrm{N}_K^L : \mathbf{A}_L^* \longrightarrow \mathbf{A}_K^*, \quad x = (x_w) \longmapsto \left(\prod_{w|v} \mathrm{N}_{K_v}^{L_w} x_w \right)$$

. The idelic formulation of class field theory is given in terms of the reciprocity map described in the following theorem.

Theorem 3.10. Let K be a number field, and let K^{ab} be the maximal abelian extension of K. There exists a unique continuous homomorphism

$$\mathbf{A}_K^* \longrightarrow \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right), \quad s \longmapsto [s, K]$$

with the following property: Let L/K be a finite abelian extension, and let $s \in \mathbf{A}_K^*$ be an idele whose ideal (s) is not divisible by any primes that ramify in L. Then

$$[s, K]|_L = \left(\frac{L/K}{(s)}\right) \text{ where } \left(\frac{L/K}{\cdot}\right) \text{ is the Artin map.}$$

The homomorphism $[\cdot, K]$ is called the *reciprocity map* for K. The reciprocity map has the following additional properties:

1. The reciprocity map is surjective, and K^* is contained in its kernel.
2. The reciprocity map is compatible with the norm map,
$$[x, L]|_{K^{\mathrm{ab}}} = \left[\mathrm{N}_K^L x, K\right] \quad \text{for all } x \in \mathbf{A}_L^*$$
3. Let $\mathfrak{p}$ be a prime ideal of K, let $I_{\mathfrak{p}}^{ab} \subset \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)$ be the inertia group of $\mathfrak{p}$, let $\pi_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$ be a uniformizer at $\mathfrak{p}$, and let L/K be any ab. extension that is unramified at $\mathfrak{p}$. Then
$$[\pi_{\mathfrak{p}}, K]|_L = (\mathfrak{p}, L/K) = \text{ Frobenius for } L/K \text{ at } \mathfrak{p} \text{ and } \left[R_{\mathfrak{p}}^*, K\right] = I_{\mathfrak{p}}^{ab}$$

§4. Complex Multiplication

Let $E/\mathbb{C}$ be an elliptic curve. We begin by recalling an important theorem about $\mathrm{End}(E)$.

Theorem 4.1. ([Sil86], VI.5.2) Let ω_1 and ω_2 be generators for a lattice Λ associated to E. Then either $\mathrm{End}(E) = \mathbb{Z}$ or the field $\mathbb{Q}(\omega_2/\omega_1)$ is an imaginary quadratic extension of $\mathbb{Q}$, and $\mathrm{End}(E)$ is isomorphic to an order in $\mathbb{Q}(\omega_1/\omega_2)$.

Elliptic curves of latter type are our topic of discussion. We define them formally.

Definition 4.2. $E/\mathbb{C}$ is said to have *complex multiplication* (or CM) if $\mathbb{Z} \subsetneq \mathrm{End}(E)$.

We will see many nice properties of a CM elliptic curve E in section 4.1. Section 4.2 states the Main Theorem of Complex Multiplication which will be used in section 4.3 to associate a Grössencharacter to E, which in turn will be used to prove the analytic continuation of the L-series of E in section 4.4. This chapter is based on [Sil94], chapter II.

§§4.1. Properties of CM Elliptic Curves

Let $\mathcal{ELL}(\mathcal{O})$ denote the isomorphism classes of elliptic curves $E/\mathbb{C}$ with $\mathrm{End}(E) \cong \mathcal{O}$.

Let K be a imaginary quadratic field and $\mathcal{O}_K$ its ring of integers. In our discussion, we will restrict ourselves to only those EC which have CM by $\mathcal{O}_K$ i.e., the maximal order. This is not very serious restriction:

Theorem 4.3. Let E have CM by an order $\mathcal{O}$ in K. Then it is isogenous to an EC E' which have CM by $\mathcal{O}_K$. i.e., there is an isogeny $E \longrightarrow E'$.

Proof. Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice for E. Then $K = \mathbb{Q}(\omega_2/\omega_1)$ by theorem 4.1. Let $\lambda \in \Lambda$ be non-zero. Then $\lambda^{-1}\Lambda \subset K$ hence fractional ideal of K. So WLOG, we can assume $\Lambda \subset \mathcal{O}_K$. Clearly we have isogeny $\mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\mathcal{O}_K, \quad z \longmapsto z$. Take $E' = \mathbb{C}/\mathcal{O}_K$. □

Let $\mathcal{CL}(\mathcal{O}_K)$ denotes the ideal class group of $\mathcal{O}_K$. Our first result is that $\mathcal{ELL}(\mathcal{O}_K)$ is finite.

Theorem 4.4.

1. Let Λ be a lattice with $E_\Lambda \in \mathcal{ELL}(\mathcal{O}_K)$ and let $\mathfrak{a}, \mathfrak{b} \in J_K$.
   (a) $\mathfrak{a}\Lambda = \{a_1\lambda_1 + \ldots + a_r\lambda_r : a_i \in \mathfrak{a}, \lambda_i \in \Lambda\}$ is a lattice in $\mathbb{C}$.
   (b) The elliptic curve $E_{\mathfrak{a}\Lambda}$ satisfies $\mathrm{End}(E_{\mathfrak{a}\Lambda}) \cong \mathcal{O}_K$.
   (c) $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \iff \overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ in $\mathcal{CL}(\mathcal{O}_K)$.

   Hence there is well-defined *action* of $\mathcal{CL}(\mathcal{O}_K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ given by $\overline{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$.
2. This action is *simply transitive*. In particular, $|\mathcal{CL}(\mathcal{O}_K)| = |\mathcal{ELL}(\mathcal{O}_K)|$.

The proof of this theorem essentially depends on the fact that any isogeny $\phi : \frac{\mathbb{C}}{\Lambda_1} \longrightarrow \frac{\mathbb{C}}{\Lambda_2}$ between complex ECs is of the form $\phi(z) = \alpha z$ for some $\alpha \in \mathbb{C}$ with $\alpha\Lambda_1 \subset \Lambda_2$. Hence

$$\mathrm{End}(E_\Lambda) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$$

Because the action is simple transitive, there is a well defined map

$$F : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathcal{CL}(R_K)$$

characterized by the condition that (where $E \in \mathcal{ELL}(\mathcal{O}_K)$ is some chosen EC)

$$\sigma(E) = F(\sigma) * E \quad \text{for all } \sigma \in \mathrm{Gal}(\overline{K}/K).$$

This map is a homomorphism (easy) and independent of chosen EC E in $\mathcal{ELL}(R_K)$ (hard). By studying this map F (using Class Field Theory), we are able to prove the next result which says that if E has CM by $\mathcal{O}_K$ then it is defined over a number field, more precisely over the Hilbert class field H of K (3.1). In particular, it also says that $j(E)$ is an algebraic number (which is an amazing result in itself). j-invariants of EC by CM are called *singular modulli*.

Theorem 4.5. Let $E/\mathbb{C}$ has EM by $\mathcal{O}_K$. Then $K(j(E))$ is the Hilbert class field H of K.

The next result says that the coordinates of torsion points can be used to generate abelian extensions of H (not of K). The proof of this essentially depends on the fact that all endomorphisms of E are defined over H and that $E[m]$ is a free $\mathcal{O}_K/m\mathcal{O}_K$-module of rank 1.

Theorem 4.6. ([Sil94], II.2.3) Let

$$L = K(j(E), E_{tors})$$

be the field generated by the j-invariant of E and the coordinates of all of the torsion points of E. Then L is an abelian extension of $K(j(E))$.

To generate abelian extensions of K, we need to tweak the coordinates of points in E_{tors}. For this purpose, we introduce the Weber function.

Definition 4.7. For an elliptic curve $E/\mathbb{C}$, choose a lattice A and an isomorphism

$$f : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \quad z \longmapsto (\wp(z,\Lambda), \wp'(z,\Lambda))$$

then the *Weber function* $h(f(z))$ is defined by

$$h(f(z)) := \begin{cases} \frac{g_2(\Lambda)^2}{\Delta(\Lambda)}\wp(z,\Lambda)^2 & \text{if } g_3(\Lambda) = 0 \\ \frac{g_3(\Lambda)}{\Delta(\Lambda)}\wp(z,\Lambda)^3 & \text{if } g_2(\Lambda) = 0 \\ \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp(z,\Lambda) & \text{otherwise.} \end{cases} \tag{4.1}$$

where $\Delta(\Lambda) = g_2(\Lambda)^2 - 27g_3(\Lambda)^3 \neq 0$ is the usual modular discriminant.

Notation: $E[\mathfrak{a}] = \{P \in E : [\alpha]P = 0 \forall \alpha \in E\}$ is called the *group of* $\mathfrak{a}$*-torsion points* of E.

The next result is one of the central theorems in the Theory of Complex Multiplication. It is an analogue of the classical *Kronecker-Weber theorem* (3.1).

Theorem 4.8. ([Sil94], II.5.6) Let E has CM by $\mathcal{O}_K$, and let $h(f(z))$ be the Weber function as defined above. Let $\mathfrak{c}$ be an integral ideal of $\mathcal{O}_K$. Then the field

$$K(j(E), h(E[\mathfrak{c}]))$$

is the ray class field of K modulo $\mathfrak{c}$.

Proof. **(Sketch)** Let $L = K(j(E), h(E[\mathfrak{c}])) = H(h(E[\mathfrak{c}]))$. We want to prove that

$$\left(\frac{L/K}{\mathfrak{p}}\right) = 1 \iff \mathfrak{p} \in P_{K,1}(\mathfrak{c})$$

Suppose $\mathfrak{p} = \mu\mathcal{O}_K \in P_{K,1}(\mathfrak{c})$ is of degree 1. Then by 3.8, $\left(\frac{H/K}{\mathfrak{p}}\right) = 1$. Using CFT, we can find $\pi \in \mathcal{O}_K$ such that $\mathfrak{p} = \pi\mathcal{O}_K$ and reduction of $[\pi]$ modulo $\mathfrak{p}$, $\widetilde{[\pi]} = \varphi_p$ is p^{th}-power Frobenius map. Using properties of reduction map and the Weber function, we prove that $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$.

Suppose $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$. Then $\left(\frac{H/K}{\mathfrak{p}}\right) = 1$. Hence again we have $\pi \in \mathcal{O}_K$ such that $\mathfrak{p} = \pi\mathcal{O}_K$ and $\widetilde{[\pi]} = \varphi_p$. Again, using properties of reduction map and the Weber function, we can find $\xi \in \mathcal{O}^\times$ s.t. $[\pi - \xi]$ annhilates $E[\mathfrak{c}]$. Hence $\xi^{-1}\pi \equiv 1 \bmod \mathfrak{c}$ and $\mathfrak{p} = \pi\mathcal{O}_K = \xi^{-1}\pi\mathcal{O}_K$. □

One of the remarkable properties of CM elliptic curves is that their j-invariant is integral.

Theorem 4.9. (II.6.1) Let $E/\mathbb{C}$ be an EC with CM. Then $j(E)$ is an algebraic integer.

Proof. **(Sketch)** Define the following:

$$\begin{aligned}
\mathcal{D}_n &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad - bc = n \right\} \\
\mathcal{S}_n &:= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad = n, d > 0, 0 \le b < d \right\} \\
(j \circ \alpha)(\tau) &:= j\left(\frac{a\tau + b}{c\tau + d}\right) \text{ for } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \text{ with } \det(\alpha) > 0 \\
F_n(X) &:= \prod_{\alpha \in \mathcal{S}_n} (X - j \circ \alpha) = \sum_m s_m X^m
\end{aligned}$$

Then we can prove the following series of statements:

1. **Claim 1:** s_m is a modular function for $\mathrm{SL}_2(\mathbb{Z})$. Hence $s_m \in \mathbb{C}[j]$.
2. **Claim 2:** The Fourier expansion of s_m has coefficients in $\mathbb{Z}$. Hence $s_m \in \mathbb{Z}[j]$.

3. By Claim 2, $\prod_{\alpha\in\mathcal{S}_n}(X - j\circ\alpha) = F_n(j, X)$ where $F(Y, X) \in \mathbb{Z}[Y, X]$.
4. If n is not a perfect square, then the polynomial $H_n(X) = F_n(X, X)$ is non-constant and has leading coefficient ± 1.

Now if E has CM by full ring $\mathcal{O}_K$, then we can find an isogeny whose degree is not perfect square. Using point 4, integrality of $j(E)$ is proved. For arbitrary orders, we prove that $j(E)$ is integral over $\mathbb{Z}[j(E')]$ where E' has CM by $\mathcal{O}_K$ and use transitivity. □

Remark: Ramanujan calculated (without calculator) that

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999250072597\ldots \quad \textbf{(known as Ramanujan's Contant)}$$

which is almost an integer. This can be explained as follows: Since $\mathbb{Q}(\sqrt{-163})$ has class number 1 hence $j\left(\frac{1+\sqrt{-163}}{2}\right) \in \mathbb{Z}$. Also, recall that $j(\tau)$ has the q-expansion

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots \quad \text{where } q = e^{2\pi i\tau}$$

If we substitute $\tau = (1+\sqrt{-163})/2$, then

$$q = -e^{-\pi\sqrt{163}} \approx -3.809\cdot 10^{-18}$$

is very small. Thus the main term in $j(q)$ will be $1/q$ which means that $1/q$ should be "almost" an integer. Also all the other terms with positive power of q will be very small meaning $j(\tau)$ is almost an integer.

§§4.2. The Main Theorem of Complex Multiplication

Let $x \in \mathbb{A}_K^*$ be an idele and let $R = \mathcal{O}_K$. If $\mathfrak{a}$ is any (non-zero) fractional ideal of K, we define $x\mathfrak{a}$ to be the product $(x)\mathfrak{a}$. Using the equality $(x)_\mathfrak{p} = (x)R_\mathfrak{p} = x_\mathfrak{p}R_\mathfrak{p}$, we see that

$$(x\mathfrak{a})_\mathfrak{p} = (x)\mathfrak{a}R_\mathfrak{p} = x_\mathfrak{p}\mathfrak{a}R_\mathfrak{p} = x_\mathfrak{p}\mathfrak{a}_\mathfrak{p}$$

The following natural maps are isomorphism of abelian groups ([Sil94], II.8.1):

$$\frac{K}{\mathfrak{a}} \cong \bigoplus_\mathfrak{p} \frac{K_\mathfrak{p}}{\mathfrak{a}_\mathfrak{p}} \quad \text{and} \quad \frac{K}{x\mathfrak{a}} \cong \bigoplus_\mathfrak{p} \frac{K_\mathfrak{p}}{x_\mathfrak{p}\mathfrak{a}_\mathfrak{p}}$$

We define the *multiplication-by-x map on* $K/\mathfrak{a}$ to be multiplication of the $\mathfrak{P}$-primary component by $x_\mathfrak{p}$ i.e., it is defined by the commutativity of the following diagram:

$$\begin{array}{ccc} \frac{K}{\mathfrak{a}} & \xrightarrow{\quad x \quad} & \frac{K}{x\mathfrak{a}} \\ \downarrow\sim & & \downarrow\sim \\ \oplus_\mathfrak{p} \frac{K_\mathfrak{p}}{\mathfrak{a}_\mathfrak{p}} & \xrightarrow{(t_\mathfrak{p})\longmapsto(x_\mathfrak{p}t_\mathfrak{p})} & \oplus_\mathfrak{p} \frac{K_\mathfrak{p}}{x_\mathfrak{p}\mathfrak{a}_\mathfrak{p}} \end{array}$$

Now we are ready to state the main theorem of CM. It gives an analytic description of of the action of $\mathrm{Aut}(\mathbb{C})$ on $E(\mathbb{C})$. It is called so because we can deduce theorem 4.8 from it. Also it will help us associate a Grössencharacter to E (theorem 4.14) which will help us prove the analytic continuation of L-function of E (theorem 4.21).

Theorem 4.10. (Main Theorem of CM) Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ and $s \in \mathbb{A}_K^*$, an idele of K satisfying $[s, K] = \sigma|_{K^{ab}}$. Fix a complex analytic isomorphism

$$f : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C})$$

where $\mathfrak{a}$ is a fractional ideal of K. Then there exists a unique complex analytic isomorphism

$$f' : \mathbb{C}/s^{-1}\mathfrak{a} \xrightarrow{\sim} E^\sigma(\mathbb{C})$$

(depending on f and σ) so that the following diagram commutes:

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

§§4.3. The Associated Grössencharacter

Definition 4.11. A *Grössencharacter* on a number field L is a continuous homomorphism

$$\psi : \mathbb{A}_L^* \longrightarrow \mathbb{C}^*$$

with the property that $\psi(L^*) = 1$. It is said to be *unramified* at $\mathfrak{P}$ if $\psi(R_{\mathfrak{P}}^*) = 1$.

Let E/L be an EC with CM by the ring of integers $\mathcal{O}_K$ of K, and assume that $L \supset K$. In the next theorem, we take our first step in defining the Grössencharacter.

Theorem 4.12. Let $x \in \mathbb{A}_L^*$ be an idele of L, and let $s = N_K^L(x) \in \mathbb{A}_K^*$. Then there exists a unique $\alpha = \alpha_{E/L}(x) \in K^*$ with the following two properties:

1. $\alpha\mathcal{O}_K = (s)$, where $(s) \subset K$ is the ideal of s.
2. The following diagram commutes

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\alpha s^{-1}} & K/\mathfrak{a} \\ \downarrow f & & \downarrow f \\ E(L^{ab}) & \xrightarrow{[x,L]} & E(L^{ab}) \end{array}$$

for any fractional ideal $\mathfrak{a} \subset K$ and any analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \longrightarrow E(\mathbb{C})$.

Proof. Let $L' = L(E_{\text{tors}})$. Since $j(E) \in L$, it follows from 4.8 and 4.6 resp. that

$$K^{\text{ab}} \subset L' \subset L^{\text{ab}}$$

Choose an automorphism $\sigma \in \text{Aut}(\mathbb{C})$ such that $\sigma|_{L^{ab}} = [x, L]$. Then by (3.10), we have $\sigma|_{K^{\text{ab}}} = [s, K]$. So applying the main theorem of CM (4.10), we find an analytic isomorphism $f' : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$ and a commutative diagram as in 4.10.

Now $E^\sigma = E$, since σ fixes L. In particular, $\mathbb{C}/\mathfrak{a} \cong K/s^{-1}\mathfrak{a}$. Hence $\exists \beta \in K^*$ such that $\beta s^{-1}\mathfrak{a} = \mathfrak{a}$. Our commutative diagram then becomes

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

Note that $f'' \circ f^{-1}$ is an automorphism of E, say $f'' = [\xi] \circ f$ for some $\xi \in \mathcal{O}_K^*$. Now set $\alpha = \xi\beta$ and use the facts that $\sigma|_{L^{ab}} = [x, L]$ and $E_{\text{tors}} \subset E\left(L^{\text{ab}}\right)$, we get

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\alpha s^{-1}} & K/\mathfrak{a} \\ \downarrow f & & \downarrow f \\ E(L^{ab}) & \xrightarrow{[x,L]} & E(L^{ab}) \end{array}$$

which is exactly (ii). Further, we have an equality of ideals

$$\alpha s^{-1}\mathfrak{a} = \beta s^{-1}\mathfrak{a} = \mathfrak{a}, \quad \text{so} \quad \alpha\mathcal{O}_K = (s)$$

This proves that α satisfies both (i) and (ii), which completes the proof of the existence. It can be showed that such α is unique and independent of the choice of f. □

The above theorem gives us a well-defined map

$$\alpha_{E/L} : \mathbb{A}_L^* \longrightarrow K^* \subset \mathbb{C}^*$$

which is clearly a homomorphism. However, it is easy to see that $\alpha_{E/L}(L^*) \neq 1$, so $\alpha_{E/L}$ is not a Grössencharacter. More precisely, if $\beta \in L^*$ and $x_\beta \in \mathbf{A}_L^*$ is the corresponding idele, then $\left[x_\beta, L\right] = 1$ (because L^* is in the kernel of $[\cdot, L]$). Then it is easy to see that (using the formula $N_K^L(\alpha) = \prod_{w|v} N_{K_v}^{L_w}(\alpha)$ for any valuation v on K)

$$\alpha_{E/L}\left(x_\beta\right) = \mathrm{N}_K^L\beta \quad \text{for all } \beta \in L^*.$$

But we very close. We can tweak the function $\alpha_{E/L}$ to obtain a Grössencharacter (theorem 4.14). Before moving on, we first recall a criterion for good reduction.

Theorem 4.13. [Sil86],VII.7.1 **(Criterion of Neron-Ogg-Shafarevich)** Let K be a local field and E/K be an elliptic curve. Then E has good reduction at $K \iff I_v^{ab}$ acts trivially on $E[m]$ for infinitely many integers $m \geq 1$ that are relatively prime to $\text{char}(k)$.

Theorem 4.14. Let

$$\alpha_{E/L} : \mathbb{A}_L^* \longrightarrow K^*$$

be the map described in theorem 4.12. For any idele $s \in \mathbb{A}_K^*$, let $s_\infty \in \mathbb{C}^*$ be the component of s corresponding to the unique archimedean absolute value on K. Define a map

$$\psi_{E/L} : \mathbb{A}_L^* \longrightarrow \mathbb{C}^*, \quad \psi_{E/L}(x) = \alpha_{E/L}(x)\mathrm{N}_K^L(x^{-1})_\infty$$

1. $\psi_{E/L}$ is a Grössencharacter of L.
2. Let $\mathfrak{P}$ be a prime of L. Then $\psi_{E/L}$ is unramified at $\mathfrak{P} \iff E$ has good reduction at $\mathfrak{P}$.

Proof. **(a)** It is clear that $\psi_{E/L}$ is a homomorphism. We saw above that if $\beta \in L^*$, then $\alpha_{E/L}(x_\beta) = \mathrm{N}_K^L\beta$. On the other hand, untwisting the definitions we find

$$\mathbb{N}_K^L(x_\beta)_\infty = \prod_{\substack{\tau: L \hookrightarrow \mathbb{C} \\ \tau|_K = 1}} \beta^\tau = \mathrm{N}_K^L\beta$$

Therefore $\psi_{E/L}(x_\beta = 1$. This holds for all β, so $\psi_{E/L}(L^*) = 1$.

First we verify that $\alpha_{E/L}$ is **continuous.** Fix an integer $m \geq 3$. By 4.6, $L(E[m]) \subset L^{ab}$. Let

$$B_m = [\cdot, L]^{-1}(\mathrm{Gal}(\bar{L}/L(E[m])) \subset \mathbb{A}_L^*$$

be the open subgroup (open because reciprocity map is continuous). Let

$$W_m := \left\{s \in \mathbb{A}_K^* : s_\mathfrak{P} \in (\mathcal{O}_K)_\mathfrak{p}^* \quad \text{and} \quad s_\mathfrak{p} \equiv 1 \bmod m(\mathcal{O}_K)_\mathfrak{p} \text{ for all } \mathfrak{p}\right\} \quad \text{(open because } (\mathcal{O}_K)_\mathfrak{p}^* \text{ is open)}$$

$$U_m := B_m \cap \left\{x \in \mathbb{A}_L^* : \mathrm{N}_K^L x \in W_m\right\} \quad \text{(open because } N_K^L : \mathbb{A}_L^* \to \mathbb{A}_K^* \text{ is continuous)}$$

We are going to prove the **Claim:** $\alpha_{E/L}(x) = 1$ for all $x \in U_m$.

Let $x \in U_m$, $\alpha = \alpha_{E/L}(x)$, and fix an analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C})$. Then for any $t \in m^{-1}\mathfrak{a}/\mathfrak{a}$ we have $f(t) \in E[m]$, so

$$\begin{aligned} f(t) = f(t)^{[x,L]} &= f\left(\alpha N_K^L x^{-1} t\right) \\ &= f(\alpha t) \quad \text{since } t \in m^{-1}\mathfrak{a}/\mathfrak{a} \text{ and } \left(\mathrm{N}_K^L x\right)_\mathfrak{p} \in (1 + m(\mathcal{O}_K)_\mathfrak{p}) \cap (\mathcal{O}_K)_\mathfrak{p}^* \text{ for all } \mathfrak{p} \end{aligned}$$

Since f is an isomorphism, multiplication by α fixes $m^{-1}\mathfrak{a}/\mathfrak{a}$ or, equivalently,

$$(\alpha - 1)m^{-1}\mathfrak{a} \subset \mathfrak{a} \implies (\alpha - 1)\mathcal{O}_K \subset m\mathcal{O}_K \implies \alpha \in \mathcal{O}_K \quad \text{and} \quad \alpha \equiv 1 \,(\mathrm{mod}\, m\mathcal{O}_K)$$

On the other hand, for any prime $\mathfrak{p}$ of K we have

$$\begin{aligned} \mathrm{ord}_\mathfrak{p}\,\alpha &= \mathrm{ord}_\mathfrak{p}\left(\mathrm{N}_K^L x\right)_\mathfrak{p} \quad \text{(by 4.12(i))} \\ &= 1 \quad \text{(since the } \mathfrak{p}\text{-component of } \mathrm{N}_K^L x \in W_m \text{ is a unit.)} \end{aligned}$$

This holds for all $\mathfrak{p}$, so $\alpha \in \mathcal{O}_K^*$. But $\alpha \equiv 1 (\mathrm{mod}\, m\mathcal{O}_K)$ from above, so the only possibility is $\alpha = 1$ (using $m \geq 3$). This proves our claim. Hence,

$$\psi_{E/L}(x) = \mathrm{N}_K^L \left(x^{-1}\right)_\infty \qquad \text{for all } x \in U_m$$

proving that $\psi_{E/L}$ is continuous on U_m. Therefore $\psi_{E/L}$ is continuous on all of $\mathbb{A}_L^*$.

(b) Let $I_{\mathfrak{P}}^{ab} \subset \mathrm{Gal}(L^{ab}/L)$ be the inertia group for $\mathfrak{P}$. Then $\left[R_{\mathfrak{P}}^*, L\right] = I_{\mathfrak{P}}^{ab}$ by 3.10. Let $m \in \mathbb{Z}$ with $\mathfrak{P} \nmid m$. We know from 4.6 that $E[m] \subset E(L^{ab})$, so $I_{\mathfrak{P}}^{ab}$ will act on $E[m]$. Now

$$\begin{aligned} I_{\mathfrak{P}}^{ab} \text{ acts trivially on } E[m] &\iff f(t)^{[x,L]} = f(t) \text{ for all } x \in (\mathcal{O}_K)_{\mathfrak{P}}^* \text{ and all } t \in m^{-1}\mathfrak{a}/\mathfrak{a} \\ &\iff f\left(\alpha_{E/L}(x)\left(\mathrm{N}_K^L x^{-1}\right)t\right) = f(t) \text{ for all } x \in (\mathcal{O}_K)_{\mathfrak{P}}^* \text{ and all } t \in m^{-1}\mathfrak{a}/\mathfrak{a}. \end{aligned}$$

We make two observations. First,

$$\psi_{E/L}(x) = \alpha_{E/L}(x) \qquad \text{for all } x \in (\mathcal{O}_K)_{\mathfrak{P}}^*$$

since $x \in (\mathcal{O}_K)_{\mathfrak{P}}^*$ are all 1 for $\mathfrak{P}|\infty$. Second, the multiplication by $\mathrm{N}_K^L x^{-1}$ induces the identity map on $m^{-1}\mathfrak{a}/\mathfrak{a}$. This follows from a technical lemma ([Sil94], II.9.3) and the assumption that $\mathfrak{P} \nmid m$. Hence we find

$$\begin{aligned} I_{\mathfrak{P}}^{ab} \text{ acts trivially} &\iff f\left(\psi_{E/L}(x)t\right) = f(t) \text{ for all } x \in (\mathcal{O}_K)_{\mathfrak{P}}^* \text{ and all } t \in m^{-1}\mathfrak{a}/\mathfrak{a} \\ &\iff \psi_{E/L}(x) \equiv 1 \,(\mathrm{mod}\, m\mathcal{O}_K) \text{ for all } x \in (\mathcal{O}_K)_{\mathfrak{P}}^*, \text{ since } f : m^{-1}\mathfrak{a}/\mathfrak{a} \xrightarrow{\sim} E[m] \end{aligned}$$

Combining this with the criterion of Néron-Ogg-Shafarevich (4.13), we get

$$\begin{aligned} E \text{ has good redn. at } \mathfrak{P} &\iff \exists \text{ infinitely many } m \text{ with } \mathfrak{P} \nmid m \text{ s.t. } \psi_{E/L}(x) \equiv 1 \,(\mathrm{mod}\, m\mathcal{O}_K)\, \forall x \in (\mathcal{O}_K)_{\mathfrak{P}}^* \\ &\iff \psi_{E/L}(x) = 1 \text{ for all } x \in (\mathcal{O}_K)_{\mathfrak{P}}^* \quad \text{(since above is true for infinitely many } m \end{aligned}$$

And by definition this means that $\psi_{E/L}$ is unramified at $\mathfrak{P}$. □

§§4.4. The L-Series Attached to a CM Elliptic Curve

Let L be a number field and E/L be an EC with CM by $\mathcal{O}_K$.. In this section, we prove the analytic continuation (4.21) of the L-series of E. This is done is a slightly unusual way: We prove that $L(E/L, s)$ is equal to a certain Dirichlet series whose analytic continuation is already known (4.16) and then conclude the analytic continuation of $L(E/L, s)$.

Definition 4.15. Let $\psi : \mathbb{A}_L^* \longrightarrow \mathbb{C}^*$ be a Grössencharater and $\mathfrak{P}$ a prime of L. We define

$$\psi(\mathfrak{P}) := \begin{cases} \psi(\ldots, 1, 1, \pi, 1, 1, \ldots) & \text{if } \psi \text{ is unramified at } \mathfrak{P} \\ 0 & \text{otherwise} \end{cases}$$

The *Hecke L-series* attached to the Grössencharater ψ is defined by the Euler product

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

Theorem 4.16. Let $L(s,\psi)$ be the *Hecke L-series* attached to the Grössencharacter ψ. Then $L(s,\psi)$ has an analytic continuation to the entire complex plane. Further, there is a functional equation relating the values of $L(s,\psi)$ and $L(N-s,\overline{\psi})$ for some real number $N = N(\psi)$.

Now we set on to find the relation between elliptic curve invariants and its associated Grössencharacter. First, we prove the following proposition.

Proposition 4.17. Assume that $L \supset K$ and let $\mathfrak{P}$ be a prime of L at which E has good reduction, let $\widetilde{E}$ be the reduction of E modulo $\mathfrak{P}$, and let

$$\phi_{\mathfrak{P}} : E \longrightarrow \widetilde{E} \quad \text{be the associated } q_{\mathfrak{P}}\text{-power Frobenius map, and} \quad \psi_{E/L} : \mathbb{A}_L^* \longrightarrow \mathbb{C}^*$$

be the Grössencharacter (4.14) attached to E/L. Then the following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{[\psi_{E/L}(\mathfrak{P})]} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\phi_{\mathfrak{P}}} & \tilde{E} \end{array}$$

Remark: We have $\psi_{E/L}(\mathfrak{P}) = \alpha_{E/L}(\mathfrak{P}) \in \mathcal{O}_K$, so $[\psi_{E/L}(\mathfrak{P})] \in \mathrm{End}(E)$.

Proof. Let $x = (\ldots, 1, 1, \pi, 1, 1, \ldots) \in \mathbf{A}_L^*$ where $\mathfrak{P} = \pi\mathcal{O}_L$. Then as we just remarked,

$$\psi_{E/L}(\mathfrak{P}) = \psi_{E/L}(x) = \alpha_{E/L}(x) \in \mathcal{O}_K$$

The commutative diagram in 4.12 used to define $\alpha_{E/L}$ tells us that

$$f(t)^{[x,L]} = [\psi_{E/L}(x)]\, f\left(\mathrm{N}_K^L x^{-1} t\right) \quad \text{for all } t \in K/\mathfrak{a}$$

Fix some $m \in \mathbb{Z}$ with $\mathfrak{P} \nmid m$. Then ([Sil94], lemma II.9.3) says that $\left(\mathrm{N}_K^L x^{-1}\right) t = t$ for all $t \in m^{-1}\mathfrak{a}/\mathfrak{a}$, so we get

$$f(t)^{[x,L]} = [\psi_{E/L}(x)]\, f(t) \quad \text{for all } t \in m^{-1}\mathfrak{a}/\mathfrak{a}$$

Now we have $[x,L] = \left(\frac{L^{ab}/L}{\mathfrak{P}}\right)$ from 3.10 (iii), so $[x,L]$ mod $\mathfrak{P}$ is $\phi_{\mathfrak{P}}$. Hence we get,

$$\phi_{\mathfrak{P}}(\widetilde{f(t)}) = \widetilde{f(t)^{[x,L]}} = \left[\widetilde{\psi_{E/L}(x)}\right] \widetilde{f(t)} \quad \text{for all } t \in m^{-1}\mathfrak{a}/\mathfrak{a}$$

As t varies over $m^{-1}\mathfrak{a}/\mathfrak{a}$, $f(t)$ varies over all of $E[m]$. Let $L' = L(E[m])$ and $\mathfrak{P}'|\mathfrak{P}$ be a prime extension. By [AEC VII.3.1], (where k' is the residue field of $(\mathcal{O}_{L'})_{\mathfrak{P}'}$)

$$E(L'_{\mathfrak{P}'})[m] \longrightarrow \tilde{E}(k')$$

is injective. Since $L' \subset L'_{\mathfrak{P}'}$, $|E(L')[m]| = m^2$, and $|\tilde{E}(k')| \leq m^2$, we get that above map is bijection of m-torsion points. Hence $\widetilde{f(m^{-1}\mathfrak{a}/\mathfrak{a})}$ is all of $\tilde{E}[m]$.

Since this is true for all $m \in \mathbb{Z}$ with $m \nmid \mathfrak{P}$, and since an endomorphism of $\tilde{E}$ is determined by its effect on torsion (or even on ℓ-primary torsion for a fixed prime ℓ [AEC III.7.4]), we conclude that $\phi_{\mathfrak{P}} = \left[\widetilde{\psi_{E/L}(x)}\right]$. □

Now we give some properties of endomorphisms of ECs and give corollary of above.

Theorem 4.18. 1. ([Sil94], II.1.5) If E is an EC with CM by $\mathcal{O}_K$, then $\forall \alpha \in \mathcal{O}_K$, the endomorphism $[\alpha] : E \longrightarrow E$ has degree $|N_{\mathbb{Q}}^K(\alpha)|$.

2. ([Sil94], II.4.4) Let E be an EC with good reduction at prime $\mathfrak{P}$, then

$$\deg(\phi) = \deg(\tilde{\phi}) \quad \text{for any } \phi \in \mathrm{End}(E),$$

where $\tilde{\phi} : \tilde{E} \longrightarrow \tilde{E}$ is the reduction of ϕ modulo $\mathfrak{P}$.

Corollary 4.19. 1. $q_{\mathfrak{P}} = \mathrm{N}_{\mathbb{Q}}^L \mathfrak{P} = \mathrm{N}_{\mathbb{Q}}^K (\psi_{E/L}(\mathfrak{P}))$,

2. $\#\tilde{E}(\mathbb{F}_{\mathfrak{P}}) = \mathrm{N}_{\mathbb{Q}}^L \mathfrak{P} + 1 - \psi_{E/L}(\mathfrak{P}) - \overline{\psi_{E/L}(\mathfrak{P})}$,

3. $a_{\mathfrak{P}} = \psi_{E/L}(\mathfrak{P}) + \overline{\psi_{E/L}(\mathfrak{P})}$.

Proof. **(a)** We compute

$$\begin{aligned} \mathrm{N}_{\mathbb{Q}}^L \mathfrak{P} = \deg \phi_{\mathfrak{P}} &= \deg\left[\widetilde{\psi_{E/L}(\mathfrak{P})}\right] && \text{from 4.17} \\ &= \deg\left[\psi_{E/L}(\mathfrak{P})\right] && \text{from 4.18 (ii)} \\ &= \mathrm{N}_{\mathbb{Q}}^K (\psi_{E/L}(\mathfrak{P})) && \text{from 4.18 (i)} \end{aligned}$$

(b) Similarly, we compute

$$\begin{aligned} \#\tilde{E}(\mathbb{F}_{\mathfrak{P}}) = \#\ker(1 - \phi_{\mathfrak{P}}) &= \deg(1 - \phi_{\mathfrak{P}}) \\ &= \deg\left[1 - \widetilde{\psi_{E/L}(\mathfrak{P})}\right] && \text{from 4.17} \\ &= \deg\left[1 - \psi_{E/L}(\mathfrak{P})\right] && \text{from 4.18(ii)} \\ &= N_{\mathbb{Q}}^K (1 - \psi_{E/L}(\mathfrak{P})) && \text{from 4.18 (i)} \\ &= (1 - \psi_{E/L}(\mathfrak{P}))\left(1 - \overline{\psi_{E/L}(\mathfrak{P})}\right) \\ &= 1 - \psi_{E/L}(\mathfrak{P}) - \overline{\psi_{E/L}(\mathfrak{P})} + N_{\mathbb{Q}}^L \mathfrak{P} && \text{from (a)} \end{aligned}$$

(c) Obvious from (a), (b) and the definition of $a_{\mathfrak{P}}$. □

Now we prove the analytic continuation of $L(E/L, s)$ by relating it to Hecke L-series. But first we recall some results about reduction of ECs.

Theorem 4.20. ([Sil86], VI.5.5) Let F be a local field and E/F be an elliptic curve.

1. Let F'/F be a finite extension. If E has either good or multiplicative reduction over F, then it has the same reduction type over F'.
2. Then E has potential good reduction $\iff$ its j-invariant $j(E) \in \mathcal{O}_F$.

Theorem 4.21. (Deuring) Let E/L be an EC with CM by the ring of integers $\mathcal{O}_K$ of K.

1. Assume $K \subset L$. Let $\psi_{E/L} : \mathbb{A}_L^* \longrightarrow \mathbb{C}^*$ be the Grössencharacter attached to E/L. Then
$$L(E/L, s) = L(s, \psi_{E/L})L(s, \overline{\psi_{E/L}}).$$
2. Suppose $K \not\subset L$, and let $L' = LK$ and $\psi_{E/L'}$ be the Grössencharacter attached to E/L'. Then $L(E/L, s) = L(s, \psi_{E/L'})$.

Proof. By 4.9 and 4.20, we get that E has no multiplicative reduction. Hence E has only good or additive reduction. Now suppose E has good reduction at $\mathfrak{P}$. Then

$$\begin{aligned} L_{\mathfrak{P}}(E/L, T) &= 1 - a_{\mathfrak{P}}T + q_{\mathfrak{P}}T^2 \\ &= 1 - \left(\psi_{E/L}(\mathfrak{P}) + \overline{\psi_{E/L}(\mathfrak{P})}\right) T + \left(\mathrm{N}_{\mathbb{Q}}^{K}\psi_{E/L}(\mathfrak{P})\right) T^2 \text{ (by 4.19)} \\ &= (1 - \psi_{E/L}(\mathfrak{P})T)\left(1 - \overline{\psi_{E/L}(\mathfrak{P})}T\right) \end{aligned}$$

On the other hand, (4.14 b) says that $\psi_{E/L}$ is unramified at $\mathfrak{P} \iff E$ has good reduction at $\mathfrak{P}$, and the same is true for $\overline{\psi_{E/L}}$. Thus

$$\psi_{E/L}(\mathfrak{P}) = \overline{\psi_{E/L}(\mathfrak{P})} = 0 \quad \text{if } E \text{ has bad reduction at } \mathfrak{P}$$

so the formula given above for $L_{\mathfrak{P}}(E/L, T)$ is also true for primes of bad reduction. Therefore

$$\begin{aligned} L(E/L, s) = \prod_{\mathfrak{P}} L_{\mathfrak{P}}\left(E/L, q_{\mathfrak{P}}^{-s}\right)^{-1} &= \prod_{\mathfrak{P}} \left(1 - \psi_{E/L}(\mathfrak{P})q_{\mathfrak{P}}^{-s}\right)^{-1} \left(1 - \overline{\psi_{E/L}(\mathfrak{P})}q_{\mathfrak{P}}^{-s}\right)^{-1} \\ &= L\left(s, \psi_{E/L}\right) L\left(s, \overline{\psi_{E/L}}\right) \end{aligned}$$

The part (2) can be also proved in a similar way. □

Now we give the explicit analytic continuation of the L-function $L(E/L, s)$ when $L = \mathbb{Q}$.

Corollary 4.22. $L(E/\mathbb{Q}, s)$ extends to an entire function on $\mathbb{C}$ with functional equation

$$\Lambda(E/\mathbb{Q}, s) = w\Lambda(E/\mathbb{Q}, 2 - s)$$

where

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

Γ is the Gamma-function, and $w \in \{\pm 1\}$ is called the *sign* of the functional equation.

The sign of the functional equation will play an important role in the later sections.

§5. Future Work

We resume from where we left off in the introduction. So around 1970's, $L(E/\mathbb{Q}, s)$ was known to be defined at $s = 1$ only for CM ECs (theorem 4.22). So naturally, mathematicians first tried to prove BSD for CM ECs and John Coates and Andrew Wiles succeeded at it:

Theorem 5.1. (Coates-Wiles, 1978) Let $E/\mathbb{Q}$ be an elliptic curve having complex multiplication. Then $L(E, 1) \neq 0 \implies \text{rank}(E(\mathbb{Q})) = 0$.

Soon, another major breakthrough came through the collaboration of Benedict Gross and Don Zagier. They studied the so-called *Heegner points* on ECs which we will formally define in section 5.4. But first some preliminaries in sections 5.1 and 5.2. Heegner points have an interesting history which we will see in section 5.3. In section 5.5, we will give the statement of the theorems of Gross-Zagier and Kolyvagin.

§§5.1. Modular Curves

The main reference for this section is [DS05], Ch II.

Let $\mathcal{H} := \{\tau \in \mathbb{C} : \text{Im}\,\tau > 0\}$ denote the Poincare upper half plane.

Definition 5.2. For $N \in \mathbb{Z}_{\geq 1}$, we define

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : c \equiv 0 (\text{mod}\, N) \right\}$$

called the *Hecke congruence subgroup of level N*.

We define $Y_0(N) := \Gamma_0(N)\backslash\mathcal{H}$, the set of orbits of the action of $\Gamma_0(N)$ on $\mathcal{H}$. Let $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ be the completion of $\mathcal{H}$, where $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.

We topologize $\mathcal{H}^*$ as follows: A basic open set about a point of $\mathcal{H}$ is an open disc wholly within $\mathcal{H}$, and a basic open set about ∞ is

$$\mathcal{N}_M := \{\tau \in \mathcal{H} : \text{Im}\,\tau > M\} \text{ for each positive real number } M.$$

If $x = p/q \in \mathbb{P}^1(\mathbb{Q})$ is rational, a basic open set about x is of the form $D \cup \{x\}$, where D is an open disc in $\mathcal{H}$ of positive radius r and center $x + ir$. The resulting topology on $\mathcal{H}^*$ is Hausdorff, $\mathcal{H}$ is an open subset and Γ acts continuously.

Definition 5.3. $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$ is called the *modular curve of level N*.

Theorem 5.4. $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$ is a compact, connected, and Hausdorff space.

Morever, $X_0(N)$ can be given complex charts which makes it into a Riemann surface and this Riemann surface can be realized as the set of complex points of a projective curve defined

over $\mathbb{Q}$. Infact, there is an equation, called the *modular equation*, given by $F_N(j, j_N) = 0$ where $j(z)$ is the modular j-invariant and $j_N(z) := j(Nz)$ with $F_N(u, v) \in \mathbb{Z}[u, v]$. And

$$Z_0(N) : F_N(u, v) = 0 \tag{5.1}$$

is an irreducible plane model for $X_0(N)$. F_N also occured in the proof of the integrality of j-invariant of CM ECs (theorem 4.9).

Also $Y_0(N) \subset X_0(N)$ is also a Riemann surface (as $X_0(N) \backslash Y_0(N)$ is finite hence closed). $Y_0(N)$ has another interpretation which will be useful later:

$$\begin{aligned} Y_0(N) &= \{(E, \phi) \text{ upto isomorphism} : E/\mathbb{C} \text{ is an EC and } \phi \subset E \text{ is a cyclic subgroup of order } N\} \\ &= \{\phi : E \longrightarrow E' \text{ upto isomorphism} : \phi \text{ an isogeny with } \ker(\phi) \text{ cyclic of order } N\} \end{aligned}$$

where isomorphisms are defined in the obvious way.

§§5.2. Weil Curves and the Modularity Theorem

Let $E/\mathbb{Q}$ be an EC and $L(E/\mathbb{Q}, s) = \sum_n a_n n^{-s}$ be its L-series. Let $f_E(\tau) = \sum_n^\infty a_n q^n$ where $q = e^{2\pi i \tau}$. If f_E is a cusp form of weight 2 then E is called a *modular elliptic curve* or *a Weil curve*. The following theorem gives conditions for cusp forms to arise this way.

Theorem 5.5. Let f be a modular cusp form of weight 2 for the group $\Gamma_0(N)$. Assume further that f is a normalized newform and that f has rational Fourier coefficients. Then there exists an elliptic curve E defined over $\mathbb{Q}$ such that $f = f_E$.

In other direction, we have the following famous result which also gives the analytic continuation of $L(E/\mathbb{Q}, s)$ to all to the whole complex plane.

Theorem 5.6. (Modularity Theorem) Every elliptic curve $\mathbb{Q}$ is a Weil curve.

The following version of Modularity theorem is often useful.

Theorem 5.7. (**Modularity Theorem**, [DS05], VII.7.2) Let E be an elliptic curve over $\mathbb{Q}$. Then for some positive integer N there exists a surjective morphism over $\mathbb{Q}$ of curves

$$\Phi_{N,E} : X_0(N) \longrightarrow E(\mathbb{C})$$

The map $\Phi_{N,E}$ is called a *modular parametrization* of E. The positive integer N can be taken to be the conductor of E.

§§5.3. The Congruent Number & The Class Number 1 Problems

An amature German mathematician named Kurt Heegner in his [Hee52] paper was interested in solving an special case of the ancient Congruent number problem (CNP). Along the way, he also solved the famous Gauss' Class number 1 problem. Sadly, his solution to the Gauss' problem wasn't accepted at the time due to an alleged gap. It was only later, when

Harold Stark [Sta66] and Alan Baker [Bak71] independently solved it in 1966, Stark went back to the Heegner's proof and realised that it was (almost) correct.

Also later, Bryan Birch realized that while solving the CNP, Heegner had unknowingly found a remarkable way to explicitely construct certain rational points on certain elliptic curves which he called "Heegner Points" [Bir75]. Birch generalised the Heegner's results and formulated them in modern language (as points on modular curves). With N Stephens, he also did an extensive numerical computations of Heegner points on the family of curves $y^2 = x^3 - 1728e^3$ [BS81] and formulated a conjecture about Heegner points (see section 5.5).

Even though Heegner did not used elliptic curves in his paper, all of this was possible because of a relation between the CNP and elliptic curves which we now describe.

Definition 5.8. An integer n is called *congruent* if it is the area of some right triangle all of whose sides are rational numbers.

[Congruent Number Problem] Given a positive integer n, determine if it congruent or not.

Theorem 5.9. n is congruent $\iff$ rank of the elliptic curve $E_n : y^2 = x^3 - n^2x$ is positive.

Heegner proved the following result in his paper [Hee52].

Theorem 5.10. Let $p \in \mathbb{Z}_{\geq 1}$ be a prime number. If $p \equiv 5 \text{ or } 7 (\text{mod } 8)$ (resp. $p \equiv 3 \text{ or } 7 (\text{mod } 8)$) then p (resp. $2p$) is congruent.

§§5.4. Heegner Points

Let $\omega \in \mathcal{H}$ is an imaginary quadratic number. Then ω satisfies an equation

$$A\omega^2 + B\omega + C = 0$$

where $(A, B, C) = 1$. Denote the discriminant of ω as $\Delta(\omega) := B^2 - 4AC$ and let K be the imaginary quadratic field (IQF) $\mathbb{Q}(\omega)$. Also, fix a positive integer N. There are several equivalent ways of defining Heegner points but we choose the following:

Definition 5.11. Let $\omega \in \mathcal{H}$ is an imaginary quadratic number and A, B, C be as above. If

$$A \equiv 0 (\text{mod } N) \quad \text{and} \quad (\Delta(\omega), 4N) = 1$$

then $[\omega] \in X_0(N) = \Gamma_0(N) \backslash \mathcal{H}^*$ is called a *Heegner Point* (of *discriminant* $\Delta(\omega)$) on $X_0(N)$.

1. The discriminant $\Delta(\omega)$ of $[\omega]$ is well-defined since $\Gamma_0(N) \subset \text{GL}_2(\mathbb{Z})$. By abuse of notation, we will say that ω is a Heegner point.
2. If ω' is such that $[\omega'] = [\omega]$ and if $A \equiv 0 (\text{mod } N)$, then A' is also 0 modulo N.

3. Also note that if $(\Delta(\omega), 4N) = 1$ then

$$\begin{aligned} A \equiv 0 (\bmod N) &\iff \Delta(\omega) \equiv \beta^2 \bmod 4N \text{ for some } \beta \in \mathbb{Z} \\ &\iff \text{every prime } p \text{ dividing } N \text{ splits in } K \end{aligned}$$

Both forward implications are easy to see but backward ones require some work. Last condition is often called "*Heegner Hypothesis*" in literature.

The following gives an alternate characterization of Heegner points.

Theorem 5.12. A quadratic number ω is a Heegner point of $X_0(N) \iff \Delta(\omega) = \Delta(N\omega)$.

Proof. ($\implies$) Since ω satisfies

$$NA'\omega^2 + B\omega + C = 0 \quad \text{with } (NA', B, C) = 1$$

and therefore, $\Delta(\omega) = B^2 - 4NA'C$. Multiplying this by N, we get

$$A'(N\omega)^2 + B(N\omega) + CN = 0$$

It is easy to see that $(A', B, CN) = 1$. Therefore $\Delta(N\omega) = B^2 - 4NA'C = \Delta(\omega)$.

($\impliedby$) Let ω satisfy an equation

$$A\omega^2 + B\omega + C = 0 \quad \text{where } A, B, C \text{ are relatively prime.}$$

Multiplying this by N^2, we get

$$A(N\omega)^2 + BN(N\omega) + CN^2 = 0.$$

Let d be the gcd of A, BN and CN^2. Then $\Delta(N\omega) = \frac{N^2}{d^2}(B^2 - 4AC)$. Since $\Delta(\omega) = \Delta(N\omega)$, this implies $d = \pm N$ and therefore, $A \equiv 0 (\bmod N)$. □

We remarked at the end of section 5.1 that any point $\tau \in Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}$ can be interpreted as a pair of elliptic curves,

$$E = \frac{\mathbb{C}}{\langle 1, \tau \rangle}, \quad E' = \frac{\mathbb{C}}{\langle 1, N\tau \rangle}, \quad \text{together with the } N\text{-isogeny } E \to E'.$$

Then a Heegner point ω corresponds to a pair of N-isogenous ECs, each CM by the same order because $\Delta(\omega) = \Delta(N\omega)$. Infact, this property characterizes Heegner points and Birch defined them this way when he first introduced them in [Bir75].

Also recall that the image of ω on $X_0(N)$ may be represented on the plane model as

$$(j(\omega), j_N(\omega)) \in Z_0(N) \tag{5.2}$$

Given an elliptic curve $E/\mathbb{Q}$ of conductor N with a rational map

$$\Phi_{N,E} : X_0(N)(\mathbb{C}) \to E(\mathbb{C}) \tag{5.3}$$

defined over $\mathbb{Q}$ (5.7). If ω is a Heegner point then by equation 5.2 and 5.3, we get

$$\Phi_{N,E}(\omega) \in E\left(\mathbb{Q}\left(j(\omega), j_N(\omega)\right)\right).$$

Now by theorem 4.5, the Hilbert class field $H = \mathbb{Q}(\omega, j(\omega)) = \mathbb{Q}\left(\omega, j_N(\omega)\right)$ since $\Delta(\omega) = \Delta(N\omega)$. Therefore, $\mathbb{Q}\left(j(\omega), j_N(\omega)\right) \subset \mathbb{Q}(\omega, j(\omega)) = H$ and we have

$$\Phi_{N,E}(\omega) \in E(H).$$

Since H is Galois over $K = \mathbb{Q}(\omega)$, we can find a point in $E(K)$ using this point: Let $\Delta(\omega) = D$ and the class number $h = h(D)$. In order to obtain a complete set of H/K conjugates, we find h Heegner points $\omega_1, \ldots, \omega_h$, each satisfying

$$A_i\omega_i^2 + B_i\omega_i + C_i = 0 \quad \text{with} \quad \Delta(\omega_i) = B_i^2 - 4A_iC_i = D \equiv r^2 \bmod 4N,$$
$$A_i \equiv 0 (\bmod N) \quad \text{, and} \quad B_i \equiv r \bmod 2N.$$

Then we take the following sum to obtain a point in $E(K)$.

$$P_K = \mathrm{Tr}_K^H(\Phi_{N,E}(\omega_1)) = \Phi_{N,E}(\omega_1) + \cdots + \Phi_{N,E}(\omega_h)$$

In the next semester, we will see how this point can be used to construct a point in $E(\mathbb{Q})$.

§§5.5. The Theorems of Gross-Zagier and Kolyvagin

In 1982, Birch and Stephens [BS81] published a conjecture about the height of the rational point arising from the Heegner construction:

[Conjecture 5.1] If E is an elliptic curve over $\mathbb{Q}$ which is parametrized by modular functions, i.e. E is a Weil curve, and K is a complex quadratic field such that the Mordell-Weil group $E(K)$ of K-rational points of E has odd rank, then the "canonical" K-rational point of E which is given by Heegner's construction has Tate height measured by $L'_{E/K}(1)$.

Soon after, in 1983, Gross and Zagier proved this conjecture [Gro83].

Theorem 5.13. (Gross-Zagier, 1983) Let $E/\mathbb{Q}$ be a modular elliptic curve given by

$$E : y^2 = 4x^3 + ax + b \quad \text{and} \quad E^D : Dy^2 = 4x^3 + ax + b \text{ be a twist,}$$

where $D < 0$ is the discriminant of an imaginary quadratic field. Assume also that $(D, N) = 1$, where N is the conductor of E and that

$$D \equiv \beta^2 \pmod{4N} \text{ for some } \beta.$$

Let ϵ be the sign of the functional equation of $L(E/\mathbb{Q}, s)$ and let Ω_E and Ω_{E^D} denote the least positive real periods of the elliptic curves E and E^D, respectively, there are two cases:

- **Case 1:** $\epsilon = -1$. Then there exists a point $P_D \in E(\mathbb{Q})$ such that

$$L(E^D/\mathbb{Q}, 1)L'(E/\mathbb{Q}, 1) = c\Omega_{E^D}\Omega_E\hat{h}_E(P_D)$$

  where c is a nonzero rational number and $\hat{h}_E$ is the height function on $E(\mathbb{Q})$.

- **Case 2:** $\epsilon = 1$. Then there exists a point $P_D \in E^D(\mathbb{Q})$ such that

$$L(E/\mathbb{Q},1)L'(E^D/\mathbb{Q},1) = c\Omega_{E^D}\Omega_E\hat{h}_{E^D}(P_D)$$

  where c is as above and $\hat{h}_{E^D}$ is the height function on $E^D(\mathbb{Q})$.

In both cases, the point P_D will be explicitely constructed from the point P_K discussed above. Victor Kolyvagin [Kol89] made a further breakthrough by proving:

Theorem 5.14. (Kolyvagin, 1988) If P_K is a point of infinite order, then the following are true:

1. $\operatorname{rank} E(K) = 1$.
2. The index of P_K in $E(K)$, $[E(K) : \langle P_K \rangle]$, annihalates $Ш(E/K)$. Hence $Ш(E/K)$ is finite.

Morover, refining Kolyvagin's method and combining it with Gross-Zagier, we get

Theorem 5.15. (Gross-Zagier, Kolyvagin) Let $E/\mathbb{Q}$ be a modular elliptic curve. And suppose that $\operatorname{ord}_{s=1} L(E/\mathbb{Q},s) = r$ with $r \in \{0,1\}$. Then

- $\operatorname{rank}(E(\mathbb{Q})) = r$.
- $Ш(E/\mathbb{Q})$ is finite with an upper bound on its size consistent with the BSD formula .

The above result can be extended to all elliptic curves over $\mathbb{Q}$ using the Modularity theorem.

In the next semester, we will see the proof of the above theorems (5.13 and 5.14).

References

[Bak71] Alan Baker. "On the class number of imaginary quadratic fields". In: *Bulletin of the American Mathematical Society* 77.5 (1971), pp. 678–684.

[Bir75] BJ Birch. "Heegner points of elliptic curves". In: *Symposia Mathematica*. Vol. 15. 1975, pp. 441–445.

[BS81] BJ Birch and N Stephens. "Heegner's construction of points on the curve $y^2 = x^3 - 1728e^3$". In: *Séminaire de Théorie des Nombres* 82 (1981-82), pp. 1–19.

[BSD65] Bryan John Birch and Henry Peter Francis Swinnerton-Dyer. "Notes on elliptic curves. II." In: (1965).

[Cox03] David A Cox. *primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. John Wiley & Sons, 2003.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. GTM 228, Springer-Verlag, New York, 2005.

[Gro83] Benedict Gross. "Don Zagier Points de Heegner et drives de fonctions L.(French) [Heegner points and derivatives of L-functions] C. R". In: *Acad. Sci. Paris Sr. I Math* 297 (1983), pp. 85–87.

[Hee52] Kurt Heegner. "Diophantische analysis und modulfunktionen". In: *Mathematische Zeitschrift* 56.3 (1952), pp. 227–253.

[Kol89] Victor Alexandrovich Kolyvagin. *Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a subclass of Weil curves*. Vol. 32. 3. IOP Publishing, 1989, p. 523.

[Sil86] Joseph Silverman. *Arithmetic of Elliptic Curves*. GTM 106, Springer-Verlag, New York, 1986.

[Sil94] Joseph Silverman. *Advanced Topics in Arithmetic of Elliptic Curves*. GTM 151, Springer-Verlag, New York, 1994.

[Sta66] Harold Stark. "On complex quadratic fields with class number equal to one". In: *Transactions of the American Mathematical Society* 122.1 (1966), pp. 112–119.