AN INTRODUCTION TO ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION AND THEIR IWASAWA THEORY

JOHN COATES

1. 1st Lecture

The elliptic curve $E/\mathbb{Q}$ is a curve of genus 1 over $\mathbb{Q}$, with a given $\mathbb{Q}$-rational point $\mathcal{O}$. It is written as

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathbb{Z}.$$

And $E(\mathbb{Q})$ is the group of $\mathbb{Q}$-rational points of E.

Theorem 1.1. *(Mordell) $E(\mathbb{Q})$ is a finitely generated abelian group.*

So $E(\mathbb{Q}) = \mathbb{Z}^{g_{E/\mathbb{Q}}} \oplus$ (finite group). In practice, we can find $g_{E/\mathbb{Q}}$ in every numerical case.

Example 1.2. Let $E : y^2 = x^3 - 17x$. Then $g_{E/\mathbb{Q}} = 2$ and $E(\mathbb{Q})$ is generated by $(-1, 4), (\frac{17}{4}, \frac{17}{8}), \infty, (0, 0)$. Here $(-1, 4), (\frac{17}{4}\frac{17}{8})$ are of infinite order and $(0, 0)$ is of order 2.

Conjecture 1.3. *Let N be any square free integer≥ 1 with $N \equiv 5, 6, 7$ mod 8. Prove that for the curve*

$$E : y^2 = x^3 - N^2x$$

we always have $g_{E/\mathbb{Q}} \geq 1$.

Note that in this case $g_{E/\mathbb{Q}} \geq 1$ if and only if there is a point (u, v) with $u, v \in \mathbb{Q}$ and $v \neq 0$. We have lots of numerical data. But it is difficult to find $g_{E/\mathbb{Q}}$ theoretically. It is because Fermat and Mordell's argument of infinite descent is a cohomological argument.

Pick any prime number p. $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ and $\mathbb{Z}_p \subset \mathbb{Q}_p$ is a ring of p-adic integers.

Definition 1.4. E_{p^∞} is the group of all points in $E(\bar{\mathbb{Q}})$ of p-power order.

It can be written

$$E_{p^\infty} = \lim_{\rightarrow}(\mathbb{Z}/p^n\mathbb{Z})^2 = (\mathbb{Q}_p/\mathbb{Z}_p)^2$$

as an abelian group. And $G_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ operates on E_{p^∞} because E is defined over $\mathbb{Q}$. We consider the Galois representation

$$\rho_p : G_{\mathbb{Q}} \to Aut(E_{p^\infty}) = GL_2(\mathbb{Z}_p).$$

Descent Theory gives

$$i_{E/\mathbb{Q},p} : E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \text{Ш}_{E/\mathbb{Q},p}.$$

Here $\mathbb{Q}_p/\mathbb{Z}_p = (\mathbb{Q}/\mathbb{Z})(p)$, $E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \backsimeq (\mathbb{Q}_p/\mathbb{Z}_p)^{g_{E/\mathbb{Q}}}$ and $\text{Ш}_{E/\mathbb{Q},p}$ is the p^∞-Selmer group of $E/\mathbb{Q}$.

Definition 1.5. $\text{Ш}_{E/\mathbb{Q},p} = Ker(H^1(G_{\mathbb{Q}}, E_{p^\infty}) \to \prod_q H^1(G_{\mathbb{Q}_q}, E(\bar{\mathbb{Q}}_q)))$. Here $E_{p^\infty} \hookrightarrow E(\bar{\mathbb{Q}}_q)$ for q any prime or $q = \infty$ and $G_{\mathbb{Q}_q} = Gal(\bar{\mathbb{Q}}_q, \mathbb{Q}_q)$. And $Coker(i_{E/\mathbb{Q},p}) = (E/\mathbb{Q})(p)$.

Definition 1.6. $\text{Ш}(E/\mathbb{Q})$ is the Tate-Shafravich group of $E/\mathbb{Q}$ defined by

$$\text{Ш}(E/\mathbb{Q}) = Ker(H^1(G_{\mathbb{Q}}, E(\bar{\mathbb{Q}})) \to \prod_q H^1(G_{\mathbb{Q}_q}, E(\bar{\mathbb{Q}})_q).$$

The following is the key fact which is the classical consequences of algebraic number theory:

$$\text{Ш}_{E/\mathbb{Q},p} = (\mathbb{Q}_p \times \mathbb{Z}_p)^{s_{E/\mathbb{Q},p}} \otimes \text{finite group}$$

for some integer $s_{E/\mathbb{Q},p} \geq 0$. And hence

$$\text{Ш}(E/\mathbb{Q})(p) = (\mathbb{Q}_p/\mathbb{Z}_p)^{t_{E/\mathbb{Q},p}} \otimes \text{finite group}.$$

The conclusion is that $s_{E/\mathbb{Q},p} = g_{E/\mathbb{Q}} + t_{E/\mathbb{Q},p}$. If for some p, we can calculate $s_{E/\mathbb{Q},p}$ and show that $t_{E/\mathbb{Q},p} = 0$ then we have found $g_{E/\mathbb{Q}}$.

Conjecture 1.7. $t_{E/\mathbb{Q},p} = 0$ *for every* p.

Conjecture 1.8. $\text{Ш}(E/\mathbb{Q})$ *is finite.*

Theorem 1.9. *(T. and V. Dokchitser) Parity of* $s_{E/\mathbb{Q},p}$ *is independent of* p.

For example, in the case of $y^2 = x^3 - N^2x$ for $N \equiv 5, 6, 7 \bmod 8$ $s_{E/\mathbb{Q},p}$ is always odd for all p.

In theory, classical number theory gives an upper bound for $s_{E/\mathbb{Q},p}$ for all p.

1.1. **Connection with L-functions.** This is done by Birch and Swinnerton-Dyer. Let N_E be the conductor of E. Note that primes which divide N_E are precisely the primes of bad reduction.

$L(E/\mathbb{Q}, s)$ is defined in $Re(s) > \frac{3}{2}$ by the Euler product

$$L(E/\mathbb{Q}, s) = \prod_{q|N_E} (1 - \epsilon_q q^{-s})^{-1} \times \prod_{(q,N_E)=1} (1 - a_q q^{-s} + q^{1-2s})^{-1}$$

where

$$\epsilon_q = \begin{cases} 0 & \text{if } E \text{ has an additive reduction at } q, \\ 1 & \text{if } E \text{ has a split multiplicative reduction at } q, \\ -1 & \text{if } E \text{ has a non-split multiplicative reduction at } q, \end{cases}$$

and if $(q, N_E) = 1$ then $N_q = q + 1 - a_q$. Here N_q is the number of points on $E \bmod q$ over $\tilde{E}/\mathbb{F}_q$.

Example 1.10. Let $E : y^2 = x^3 - x$ be an elliptic curve. Then $N_E = 32, \epsilon_2 = 0$. If $q < 100$ and $q \equiv 3 \bmod 4$ then $a_q = 0$. And for $q \not\equiv 3 \bmod 4$ we have a following table:

q	5	13	17	29	37	41	53	61	73	89	97
a_q	-2	6	2	-10	-2	10	14	-10	-6	10	18

Definition 1.11. $\Lambda(E/\mathbb{Q}, s) := (2\pi)^{-2s}\Gamma(s)L(E/\mathbb{Q}, s)$.

Theorem 1.12. *(Deuring-Weil, Wiles et all)* $\Lambda(E/\mathbb{Q}, s)$ *is entire and satisfies*

$$\Lambda(E/\mathbb{Q}, s) = \omega_E N_E^{1-s} \Lambda(E/\mathbb{Q}, 2 - s)$$

where $\omega_E = \pm 1$.

Definition 1.13. $r_{E/\mathbb{Q},\infty} := ord_{s-1} L(E/\mathbb{Q}, s)$.

Then note that $\omega_E = (-1)^{r_{E/\mathbb{Q},\infty}}$.

Conjecture 1.14. $r_{E/\mathbb{Q},\infty} = g_{E/\mathbb{Q}}$.

Also, they conjectured an exact formula for $\#(Ш(E/\mathbb{Q}))$ in terms of coefficients of $(s-1)^{r_{E/\mathbb{Q},\infty}}$ in each of $L(E/\mathbb{Q},s)$. In most cases, it is predicted that $Ш(E/\mathbb{Q})=0$ especially if $g_{E/\mathbb{Q}} \geq 2$.

Theorem 1.15. *(T. and V. Dokchitser)* $s_{E/\mathbb{Q},p} \equiv r_{E/\mathbb{Q},\infty}$ *mod* 2 *for every* p.

Theorem 1.16. *(Gross-Zagier-Kolyvagin) If* $r_{E/\mathbb{Q},\infty} \leq 1$, *then* $r_{E/\mathbb{Q},\infty} = g_{E/\mathbb{Q}}$ *and* $Ш(E)$ *is finite.*

Corollary 1.17. *If* $r_{E/\mathbb{Q}} \geq 2$ *then* $r_{E/\mathbb{Q},\infty} \geq 2$.

But we do not know the followings:
(i) We do not know $Ш(E/\mathbb{Q})$ is finite for a single $E/\mathbb{Q}$ with $g_{E/\mathbb{Q}} \geq 2$,
(ii) It is unknown how to prove inequalities such as $g_{E/\mathbb{Q}} \leq r_{E/\mathbb{Q},\infty}$.

2. **2nd Lecture**

The BSD conjecture is about the relation between $Ш(E/\mathbb{Q})$ and the behavior of $L(E/\mathbb{Q},s)$ at $s=1$. But if $r_{E/\mathbb{Q},\infty} \geq 2$ then there is no theoretical connection!

2.1. **Iwasawa theory.** Pick a prime p. Is there a p-adic analogue of $L(E/\mathbb{Q},s)$, say $L_p(E/\mathbb{Q},s)$ for $s \in \mathbb{Z}_p$?

We will consider the following field extensions:

$$\begin{array}{cc} \mathbb{Q}(\mu_{p^\infty}) & \mathbb{Q}(E_{p^\infty}) \\ | & | \\ \mathbb{Q} & \mathbb{Q} \end{array}$$

Remark 2.1. For every $E/\mathbb{Q}$, $End_{\mathbb{Q}}(E)=\mathbb{Z}$.

Definition 2.2. We say that $E/\mathbb{Q}$ has complex multiplication if $End_{\overline{\mathbb{Q}}}(E) \neq \mathbb{Z}$.

Example 2.3.
(1) Let $E: y^2=x^3-Dx$ be an elliptic curve and let $D \in \mathbb{Z}, D \neq 0$. Then $End_{\overline{\mathbb{Q}}}(E)=\mathbb{Z}[i]$ where $i^4=1, [i](x,y):=(-x,iy)$.
(2) Let $E: y^2=x^3+D$ be an elliptic curve and let $D \in \mathbb{Z}, D \neq 0$. Then $End_{\overline{\mathbb{Q}}}(E)=\mathbb{Z}[\rho]$ where $\rho^3=1, [\rho](x,y):=(\rho x,y)$.

It is the fact that $K = End_{\bar{\mathbb{Q}}}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic field of class number 1. Let's consider a finite extension F of $\mathbb{Q}$ and its extension field E.

Definition 2.4. E has CM if $End_{\bar{\mathbb{Q}}}(E) \neq \mathbb{Z}$.

It is always true that if F has CM, then $K = End_{\bar{\mathbb{Q}}}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic field. But in general K doesn't have class number 1.

Remark 2.5. If $End_F(E) \neq \mathbb{Z}$, then $K = End_F(E) \otimes \mathbb{Q}$ is embedded in F.

The following theory is mainly due to several contributors, like Hecke/Tate, Deuring/Weil, Eisenstein/Kronecker.

2.2. **Abelian nature of the p-adic representaions of E/F with CM.** Let $[F : \mathbb{Q}] < \infty$, and E/F be an elliptic curve with $End_F(E) \neq \mathbb{Z}$. Let p be any prime number. Then we have a Galois representation

$$\rho_p : G_F := Gal(\bar{F}/F) \longrightarrow Aut(E_{p^\infty}) = GL_2(\mathbb{Z}_p).$$

Theorem 2.6. *If $End_F(E) \neq \mathbb{Z}$, then $\rho_p(G_F)$ is abelian.*

Now consider the case when k is any field (for us $k = F$ or a finite field). Let A/k be any elliptic curve and assume that $p \neq char(k)$. Define A_{p^n} by

$$A_{p^n} := ker(A(k^{sep}) \to^{p^n} A(k^{sep})) \cong (\mathbb{Z}/p^n\mathbb{Z}).$$

Definition 2.7.

$$T_p(A) := \varprojlim A_{p^m} \cong_{\mathbb{Z}_p - module} \mathbb{Z}_p^2,$$
$$V_p(A) := T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Note that $V_p(A)$ is a $\mathbb{Q}_p$-vector space of dimension 2. Furthermore, we have the following exact sequanece:

$$0 \to T_p(A) \to V_p(A) \to A_{p^\infty} \to 0.$$

Let $G_k = Gal(k^{sep}/k)$, $\rho_p : G_k \to Aut(T_p(A))(= GL_2(\mathbb{Z}_p))$, and $End_k(A)$ the ring of k-endomorphisms of A. Then we have a homomorphism $End_k(A) \to End_{\mathbb{Q}_p}(V_p(A))$. This is not injective in general, but we know the following:

Proposition 2.8. *(see Silverman) The map* $End_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p \to End_{\mathbb{Q}_p}(V_p(A))$ *is injective.*

Now we impose a hypothesis on A/k: We are given an imaginary quadratic field K and an injective ring homomorphism $i : K \to End_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. This homomorphism is not necessarily surjective. We identify K with $i(K)$.

Definition 2.9. $R := K \cap End_k(A)$. Then R is an order in K.

Definition 2.10. $R_p := R \otimes_{\mathbb{Z}} \mathbb{Z}_p$, $K_p := K \otimes_{\mathbb{Q}} \mathbb{Q}_p = R \otimes_{\mathbb{Z}} \mathbb{Q}_p$

We can view K_p as a subset of $End_{\mathbb{Q}_p}(V_p(A))$ using the identification.

Theorem 2.11. *Under the above hypothesis, we know*

(1) $V_p(A)$ *is a free* K_p*-module of rank 1.*
(2) $\phi \in K_p$ *maps* $T_p(A)$ *into itself* $\Leftrightarrow \phi \in R_p$.

Remark 2.12. It is not always true that $T_p(A)$ is free of rank 1 over R_p.

Proof (1) First note that K_p operates faithfully on $V_p(A)$ and both K_p and $V_p(A)$ are vector spaces of dimension 2 over $\mathbb{Q}_p$. Then there are two cases:

(a) K_p is a field, which is equivalent to saying that there is one prime in K over p. Then $V_p(A)$ must have dimension 1 over K_p.
(b) $K_p = \mathbb{Q}_p \times \mathbb{Q}_p$. Let $e_1 = (1,0), e_2 = (0,1)$. We claim that $V_p(A) = e_1V_p(A) \oplus e_2V_p(A)$. This is because $e_iV_p(A)$ $(i = 1, 2)$ is nonzero therefore is of dimension ≥ 1 and they have nothing in common. Then let α_i be the $\mathbb{Q}_p$-basis of $e_iV_p(A)$, where $i = 1, 2$. Finally we get $V_p(A) = K_p(\alpha_1 + \alpha_2)$, which is free over K_p of rank 1.

(2) Let φ in K_p with $\varphi(T_p(A)) \subset T_p(A)$. Then $p^N\varphi \in R_p$, $p^N\varphi \equiv \psi \bmod p^N R_p$ for $\psi \in R$. Since $p^N\varphi T_p(A) \subset p^N T_p(A)$, $\psi T_p(A) \subset p^N A$. We consider the following exact sequence:

$$0 \to T_p(A) \to V_p(A) \to A_{p^\infty} \to 0.$$

Then we can consider the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_p(A) & \longrightarrow & V_p(A) & \longrightarrow & A_{p^\infty} & \longrightarrow & 0 \\ & & \downarrow p^N & & \downarrow p^N & & \downarrow p^N & & \\ 0 & \longrightarrow & T_p(A) & \longrightarrow & V_p(A) & \longrightarrow & A_{p^\infty} & \longrightarrow & 0. \end{array}$$

From this we can make a following exact sequence:

$$\begin{aligned} 0 &\to Ker(p^N : T_p(A) \to T_p(A)) \to Ker(p^N : V_p(A) \to V_p(A)) \to A_{p^N} \\ &\to T_p(A)/p^N T_p(A) \to 0. \end{aligned}$$

Since $p^N : V_p(A) \to V_p(A)$ is an isomorphism, $Ker(p^N : V_p(A) \to V_p(A) = 0$. So we have

$$T_p(A)/p^N T_p(A) \backsimeq A_{p^N}.$$

This implies that $\psi(A_{p^N}) = 0$. By standard lemma, $\psi = p^n\eta,\ \eta \in End_k(A)$ and $p^N\varphi \equiv p^N\eta \bmod p^N R_p$. Therefore we have $\varphi \in R_p$. □

3. **3rd Lecture**

Corollary 3.1. *The commutant of R in the following cases is valid:*

(1) In $End(V_p(A))$ is K_p.
(2) In $End(T_p(A))$ is R_p.
(3) In $End_k(A) \otimes \mathbb{Q}$ is K.
(4) In $End_k(A)$ is R.

Proof (1) It follows from (1) in Theorem2.11 since every element of $End(V_p(A))$ which commutes with R commutes with $K_p = R \otimes \mathbb{Q}_p$.
(2) It follows from that $R_p = K_p \cap End(T_p(A))$.
(3) Note that $\mathbb{Q}_p \otimes End_k(A) \hookrightarrow End(V_p(A))$. And the dimension over $\mathbb{Q}$ of commutant of R in $\mathbb{Q} \otimes End_k(A)$ is at most $[K_p : \mathbb{Q}_p] = [K : \mathbb{Q}] = 2$.
(4) It is by the definition of R:

$$R = K \cap End_k(A) \otimes \mathbb{Q}. \quad \square$$

Corollary 3.2. *Let $\rho_p : G_{k^s} = Gal(k^s/k) \to Aut(T_p(A))$. Then $\rho_p(G_{k^s}) \subset R_p^*$. In particular, $\rho_p(G_{k^s})$ is abelian.*

Proof Take σ in G_{k^s}. Then $\rho_p(\sigma)$ commutes with R, because $R \subset End_k(A)$. Hence by (2) of Theorem2.11 it lies in R_p. □

Let $F/\mathbb{Q}$ be a finite extension and let E/F be an extension with $End_F(E) \neq \mathbb{Z}$. And $K = End_F(E) \otimes \mathbb{Q}$ is an imaginary quadratic field.

Let v be a place of F and let k_v be the residue field of v and $N_v = \#(R_v)$. Assume that E has a good reduction at v. Let $\tilde{E}_v/k_v$ be an elliptic curve over k_v. And we define the Frobenius endomorphism $\varphi_v \in End_{k_v}(\tilde{E}_v)$ by

$$\varphi_v(x, y) = (x^{N_v}, y^{N_v}).$$

The reduction modulo v gives a ring homomorphism:

$$\begin{aligned} i_v &: End_F(E) \hookrightarrow End_{k_v}(\tilde{E}_v) \\ i_v &: K \hookrightarrow End_{k_v}(\tilde{E}_v) \otimes \mathbb{Q}. \end{aligned}$$

Remark 3.3. ρ_v belongs to center of $End_{k_v}(\tilde{E}_v)$.

Theorem 3.4. *For each v where E has a good reduction, there exists a unique π_v in $K = End_F(E) \otimes \mathbb{Q}$ such that $i_v(\pi_v) = \varphi_v$.*

Note that $i_v(\pi_v) \in R_v = K \cap End_{k_v}(\tilde{E}_v)$ and that this does not imply $\pi_v \in End_F(E)$.

Example 3.5. Let $K = \mathbb{Q}(\sqrt{-11})$, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\beta$, $\beta = (1 + \sqrt{-11})/2$, $\mathcal{O} = \mathbb{Z} + 3\mathcal{O}_K$. And let $F = K(\sqrt{33}) = K(\sqrt{-3}) = K(j(\mathcal{O}))$. $E : y^2 + y = x^3 + a_2x^2 + a_4x + a_6$ is an elliptic curve and $\pi_v = \pm\beta$. We consider E/F. Then $\Delta(E)$ is a unit in F. Let v be any prime of F above $\beta\mathcal{O}_K$. Then v is totally ramified in F/K and $\pi_v \notin \mathcal{O} = End_F(E)$.

Let S be the set of primes of F where E has a bad reduction. And let I_S be the free abelian group on primes of F not in S. We define $\psi_{E/f} : I_S \to K^*$. $\psi_{E/F}$ is a group homomorphism and $\psi_{E/F}(v) = \pi_v$.

Our goal is to show that there exists an integral ideal $\mathcal{F}$ of F, divisible precisely by primes in S, such that $\psi_{E/F}((\alpha)) = N_{F/K}\alpha$ and $ord_v(\alpha - 1) \geq ord_v(\mathcal{F})$ for all $v|\mathcal{F}$.

Example 3.6. Let $E : y^2 = x^3 - 17x$ be an elliptic curve with $g_{E/\mathbb{Q}} = 2$ and let $K = \mathbb{Q}(i)$. Then $End_K(E) = \mathbb{Z}[i]$ and $S = \{\mathcal{P}_2, \mathcal{P}_{17}, \mathcal{P}_{17}^*\}$ where $\mathcal{P}_2 = (1 + i), \mathcal{P}_{17} = (1 + 4i), \mathcal{P}_{17}^* = (1 - 4i)$. For $v \notin S$, $\pi_v \in \mathbb{Z}[i]$ and $(\pi_v) = v$.

4. **4th Lecture**

Let $[F:\mathbb{Q}] < \infty$ and E/F be an elliptic curve. We assumed $End_F(E) \neq \mathbb{Z}$ and $K = \mathbb{Q} \otimes_{\mathbb{Z}} End_F(E)$ is an imaginary quadratic field. Then $End_F(E)$ acts on F-vector space of holomorphic differentials on E and this gives an embedding $K \hookrightarrow F$.

Definition 4.1. Let S be a set of primes in F where E has bad reduction. For v not in S, we consider $\tilde{E}_v/k_v$, where k_v is the residue field of v and $i_v : K = \mathbb{Q} \otimes_{\mathbb{Z}} End_F(E) \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} End_{k_v}(\tilde{E}_v) \ni \varphi_v$ such that $\varphi_v(x,y) = (x^{Nv}, y^{Nv})$.

Theorem 4.2. *For v not in S, there exists unique $\pi_v \in K$ with $i_v(\pi_v) = \varphi_v$.*

Theorem 4.3. *Assume v is not in S and $(char(k_v), [\mathcal{O}_K : End_F(E)]) = 1$. Then $\pi_v \mathcal{O}_K = N_{F/K} v$.*

Lemma 4.4. *If v is not in S, then we have*

$$N_{K/\mathbb{Q}}\pi_v = Nv, Tr_{K/\mathbb{Q}}\pi_v = Nv + 1 - \#(\tilde{E}_v(k_v)).$$

Let $l \neq char(k_v)$. Then we have natural reduction module v map

$$V_l(E) \simeq V_l(\tilde{E}_v).$$

Then we have the following commutative diagram

$$\begin{array}{ccc} K = \mathbb{Q} \otimes_{\mathbb{Z}} End_F(E) & \longrightarrow & End_{\mathbb{Q}_l}(V_l(E)) \\ \downarrow i_v & \circlearrowright & \downarrow \wr \\ \mathbb{Q} \otimes_{\mathbb{Z}} End_{k_v}(\tilde{E}_v) & \longrightarrow & End_{\mathbb{Q}_l}(V_l(\tilde{E}_v(k_v))) \end{array}$$

and $\varphi_v \in \mathbb{Q} \otimes_{\mathbb{Z}} End_{k_v}(\tilde{E}_v)$ satisfies $\varphi_v \circ \hat{\varphi_v} = Nv$ and $\varphi_v + \hat{\varphi_v} = Nv + 1 - \#(\tilde{E}_v(k_v))$. Hence π_v is always an algebraic integer in K, i.e. $\pi_v \in \mathcal{O}_K$.

Let $p_v = chark_v$. We have a tower of fields:

$$\begin{array}{cc} F & v \\ | & \\ K & w \\ | & \\ \mathbb{Q} & p_v. \end{array}$$

Lemma 4.5. *Assume that v is not in S and $(p_v, [\mathcal{O}_K : End_F(E)]) = 1$. Then we always have* $\mathrm{ord}_w(\pi_v) > 0$.

Proof Let $w = \frac{dx}{2y+a_1x+a_3}$. Then for $\alpha \in End_F(E)$, $w \circ \alpha = \alpha w$. For $n \geq 1$, $(n, p_v) = 1$ with $n\pi_v \in End_F(E)$ we have $w \circ n\pi_v = n\pi_v w$. We reduce this modulo v, to get $\widetilde{w} \circ \widetilde{n\pi_v} = n\tilde{\pi}_v\tilde{w}$, where $\widetilde{w}$ is the differential on the reduced curve and $\widetilde{n\pi_v} = i_v(n\pi_v)$. Note that $i_v(n\pi_v) = n\varphi_v$. Then $\tilde{w} \circ \widetilde{n\pi_v} = n\varphi_v$ because $n\varphi_v$ is purely inseparable. Hence $n\pi_v = 0$ in k_v. Because $(p_v, [\mathcal{O}_K : End_F(E)]) = 1$, $\tilde{\pi}_v = 0$, i.e. $\mathrm{ord}_w(\pi_v) > 0$. □

(i) Suppose that there exists unique w of K above p_v. Then $(\pi_v) = w^a$. From an equation we can see $a = [k_v : k_w]$. Then $N_{F/K}v = w^{[k_v:k_w]}$ and $N_{K/\mathbb{Q}}v = p_v^{[k_v:\mathbb{F}_{p_v}]}$.

(ii) Next assume that p_v splits in K, i.e. there are two primes w, w^* above p_v. Then $(\pi_v) = w^a(w^*)^b$. We know by above lemma $a > 0$. We must show $b = 0$. Actually once we prove this we can prove the second theorem.

Assume $b > 0$. We want to get a contradiction. Let π_v^* be the conjugate of π_v over $\mathbb{Q}$. Then $p_v | \pi_v^n + (\pi_v^*)^n$, for all $n \geq 1$. Let $k_{v,n}$ be an extension field of k_v of degree n. Then we have

$$\tilde{E}_v(k_{v,n}) = (Nv)^n + 1 - \#(\pi_v^n + (\pi_v^*)^n),$$

from which we conclude $\tilde{E}_v(\bar{k_v})(p_v) = 0$, i.e. it has no p_v-torsion.

Now we will show this is not true. We have for some r $(w^*)^r = (\beta)$, where $\beta \in \mathcal{O}_K$. Choose $(n, p_v) = 1$ such that $\lambda = n\beta \in End_F(E)$. Let $E_\lambda := ker(E(\bar{F}) \to E(\bar{F}))$.

Claim: $E_\lambda(p_v) \neq 0$ and the reduction modulo v is injective on E_λ.
Note that from these we see $\tilde{E}_v(\bar{k_v})(p_v) \neq 0$, which contradicts the above observation, hence proves the theorem.

Note that the p^r-division points in the formal group of E at v^* are in E_λ. Let's look at the formal group of E at v then λ gives an endomorphism of formal group $t = \frac{-x}{y}$, and

$$\frac{[\lambda](t)}{t} = \lambda + \sum_{n=0} b_n t^{n-1} \in \mathcal{O}_{F_v}[[t]].$$

The point is that λ is an element of $\mathcal{O}_{F_v}^{\times}$, so it has no zeros in the maximal ideal of $\bar{\mathcal{O}}_{F_v}$. Therefore no points in E_λ can lie on $\hat{E}$.

Let $\psi_{E/F} : I_S \to K^{\times}$, $\psi_{E/F}(v) = \pi_v$. We will show: there exists some integral ideal f of F divisible by places in F, so other places perhaps such that ??

There are some facts: $\psi_{E/F}((\alpha)) = N_{F/K}(\zeta_\alpha), \zeta_\alpha \in K, \mathrm{ord}_v(\alpha - 1) \geq \mathrm{ord}_v(f)$, $\forall v | f$.

5. **5th Lecture**

Let F be an extension field of $\mathbb{Q}$ and E/F be an elliptic curve with $End_F(E) \neq \mathbb{Z}$ and $K = \mathbb{Q} \otimes_{\mathbb{Z}} End_F(E) \hookrightarrow F$. S is the set of primes where E has bad reduction and I_S is the free abelian group on primes not in S. And

$$\psi_{E/F} : I_S \to K^*, \ \psi_{E/F}(v) = \pi_v.$$

Theorem 5.1. *There exists an ideal $\mathcal{G}$ of F, divisible at least by primes in S, such that, for all $\alpha \in F^*$ with $ord_v(\alpha - 1) \geq ord_v(\mathcal{G})$ for all v dividing $\mathcal{G}$, we have*

$$\psi_{E/F}((\alpha)) = N_{F/K}\alpha.$$

Corollary 5.2. *$\psi_{E/F}$ is a grossencharacter of F in sense of Hecke.*

Proof of Theorem5.1 Let $S' = S \cup \{v : char(k_v) divides [\mathcal{O}_K : End_F(E)]\}$. For $v \notin S'$ $(\psi_{E/F}(v)) = N_{F/K}v$. Then $\in I_{S'}$ implies that $(\psi_{E/F}()) = N_{F/K}$. We assume that for $= (\alpha)$ $(\psi_{E/F}(\alpha)) = N_{F/K}((\alpha)) = (N_{F/K}\alpha)$ by definition. They are ideals in K. But K is an imaginary quadratic field. So this implies that

$$\psi_{E/F}((\alpha)) = \zeta_\alpha N_{F/K}\alpha, \ \zeta_\alpha \in \mu_K.$$

For a prime l and $E_{l^m} \in E(\bar{\mathbb{Q}})$ $F(E_{l^n})/F$ is abelian. Pick l to be any prime number such that

(1) $(l, \#(\mu_K)) = 1$.
(2) $(l, S') = 1$.
(3) l is unramified in K.

Let $S'_l = S' \cup \{v \ of \ F | \ v | l\}$.

Lemma 5.3. *The extension $F(E_l)/F$ is unramified outside of S'_l.*

Proof $w \notin S'_l$ implies that $\tilde{E}_w/k_w$ is a good reduction. □

The crucial remark is that reduction mod w is injective on E_l. For $w \notin S'_l$, σ_w is its Frobenius element in $Gal(F(E_l)/F)$.

Lemma 5.4. *Assume $w \notin S'_l$. Then, for any P in E_l, $\sigma_w(P) = \psi_{E/F}(w)(P)$.*

Proof We have to check that $\widetilde{\sigma_w(P)} = \widetilde{\psi_{E/F}(w)}(P)$ where $\tilde{}$ means a reduction mod w. Let $P = (\alpha, \beta)$. Then $\widetilde{\sigma_w(P)} = \widetilde{\sigma_w}(\tilde{P}) = (\alpha^{Nw}, \beta^{Nw})$. And $\widetilde{\psi_{E/F}(w)}(P) = \varphi_w(\tilde{P}) = (\alpha^{Nw}, \beta^{Nw})$. If $(\mathfrak{a}, S'_l) = 1$, then $\sigma_{\mathfrak{a}} \in Gal(F(E_l)/F)$. This implies that $\sigma_{\mathfrak{a}}(P) = \psi_{E/F}(\mathfrak{a})(P)$ for all $P \in E_l$. □

Artin's law for $F(E_l)/F$ implies that there is an ideal $\mathcal{G}$ divisible by all primes in S'_l, such that when $\alpha \in F^*$ satisfies $ord_w(\alpha - 1) \geq ord_v(\mathcal{G})$ for all $\alpha | \mathcal{G}, \sigma(\alpha) = 1$. $\sigma(\alpha) = 1$ implies that $\psi_{E/F}((\alpha))(P) = P$ for all $P \in E_l$. Here, $E_l \cong \mathcal{O}_K/l\mathcal{O}_k$. So $\psi_{E/F}((\alpha)) \equiv 1 \bmod l$. Since $v|l$ implies $v|\mathcal{G}$, $\alpha \equiv 1 \bmod v$ for all $v|l$. This implies that $N_{F/K}\alpha \equiv 1 \bmod l$. This concludes that $\zeta_\alpha \equiv 1 \bmod l$. Therefore $\zeta_\alpha = 1$ since $(l, \#(\mu_K)) = 1$. □

There is $\mathcal{G}$ such that $\mathcal{G}$ is divisible by all primes in S. And $ord_v(\alpha - 1) \geq ord_v(\mathcal{G})$ for all $v|\mathcal{G}$ implies that $\psi_{E/F}((\alpha)) = N_{F/K}\alpha$ and $F_A^*/F^* \xrightarrow{\psi_{E/F}} \mathbb{C}^*$.

Theorem 5.5. *(Deuring) The conductor of $\psi_{E/F}$ is divisible precisely by the set of primes of F where E has bad reduction.*

Corollary 5.6. *Let K be an imaginary quadratic field. There is no E/K with $End_K(E) \neq \mathbb{Z}$ having good reduction everywhere.*

Proof Suppose there is such a curve. Then $\psi_{E/F}((\alpha)) = \alpha$ for all $\alpha \in \mathcal{O}_K$. There is no such homomorphism. □

Example 5.7. Let $E : y^2 = x^3 - x$ be an elliptic curve and $K = \mathbb{Q}(i)$. Then $End_K(E) = \mathbb{Z}[i]$. And $\psi_{E/F}$ is the unique bad prime in $\mathcal{P}_2 = (1 + i)$. $\mathcal{F} = \mathcal{P}_\alpha^n$ must have $n \geq 3$. $\alpha \equiv 1 \bmod \mathcal{F}$, $\psi_{E/K}((\alpha)) = \alpha$ implies that $\mathcal{F} = \zeta_2^3$. For $\zeta \in \mu_K$ *zeta* $\equiv 1 \bmod \mathcal{P}_2^2$ implies that $\zeta = 1$ and $n \geq 3$. $\psi_{E/F} : I_s \to K^* \to \mathbb{C}^*$.

Hecke showed that

$$\begin{aligned} L(\psi_{E/K}(s)) &= \prod_{(v,s)=1} (1 - \frac{\psi_{E/F}(v)}{(Nv)^s})^{-1}, \\ L(\bar{\psi}_{E/K}(s)) &= \prod_{(v,s)=1} (1 - \frac{1 - \bar{\psi}_{E/F}(v)}{N(v)^s})^{-1}. \end{aligned}$$

Definition 5.8. (Hasse, Weil-Deuring) E with $End_F(E) \neq \mathbb{Z}$ has no place of multiplicative reduction. Define

$$L(E/F, s) := \prod_{(v,s)=1} (1 - a_v(Nv)^{-s} + (Nv)^{1-2s})^{-1}$$

where $a_v = Nv + 1 - \#(\tilde{E}_v(k_v))$.

Euler showed that for $v \notin S$,

$$\begin{aligned} \psi_{E/F}(v)\overline{\psi_{E/F}(v)} &= Nv, \\ \psi_{E/F}(v) + \overline{\psi_{E/F}(v)} &= a_v. \end{aligned}$$

Theorem 5.9. $L(E/F, s) = L(\psi_{E/F}, s)L(\bar{\psi}_{E/F}, s)$.

6. **6th Lecture**

Let E/K be an elliptic curve where K is an imaginary quadratic field, such that $End_K(E) = \mathcal{O}_K$. K has necessarily class number 1, which means that it has the minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \ a_i \in \mathcal{O}_K.$$

Let us fix an embedding $K \hookrightarrow \mathbb{C}$, consider the invariant differential $w = \frac{dx}{2y+a_1x+a_3}$, and let $\mathcal{L}$ be its period lattice. Then $\mathcal{L}$ is an $\mathcal{O}_K$-module of rank 1, which is denoted by $\mathcal{L} = \Omega_\infty\mathcal{O}_K, \Omega_\infty \in \mathbb{C}^\times$. Consider any ideal $\mathcal{G}$ of $\mathcal{O}_K$.

Definition 6.1. $E_\mathcal{G} := ker(E(\bar{K}) \to^g E(\bar{K}), \mathcal{G} = (g))$.

This is the $\mathcal{O}_K$-module and $\mathcal{G}^{-1}\mathcal{L}/\mathcal{L} = \mathcal{G}^{-1}\Omega_\infty\mathcal{O}_K/\Omega_\infty\mathcal{O}_K$, hence $E_\mathcal{G} \cong \mathcal{O}_K/\mathcal{G}$.

Definition 6.2. $K(E_\mathcal{G})$=the adjoin to K coordinates of points on $E_\mathcal{G}$.

Then we have $Gal(E_{\mathcal{G}}/K) \hookrightarrow Aut_{\mathcal{O}_K}(\mathcal{O}_K/\mathcal{G}) = (\mathcal{O}_K/\mathcal{G})^\times$. Let $\mathcal{G}$ be an integral ideal of $\mathcal{O}_K$.

Definition 6.3. Let $R_{\mathcal{G}}$:= the ray class field of K modulo $\mathcal{G}$.

Then $Gal(R_{\mathcal{G}}/K)$ is the ray class group of K modulo $\mathcal{G}$, and is isomorphic to $(\mathcal{O}_K/\mathcal{G})^\times/\tilde{\mu}_K$.

Lemma 6.4. *For all $\mathcal{G}$, $R_{\mathcal{G}} \subset K(E_{\mathcal{G}})$ is given by*

$$K(x(p)^{\frac{\#(\mu_K)}{2}}, p \text{ is a primitive element of } E_{\mathcal{G}}).$$

Definition 6.5. $\mathbf{f}$ is a conductor of $\psi_K = \psi_{E/K} = Grossencharacter$ of E over K.

Lemma 6.6. *Let $\mathcal{G}$ be an integral ideal of K which is divisible by $\mathbf{f}$. Then $K(E_{\mathcal{G}}) = R_{\mathcal{G}}$. In particular $Gal(K(E_{\mathcal{G}})/K)$ has order $\#(\mathcal{O}_K(\mathcal{G})^\times)/\#(\mu_K)$.*

Example 6.7. Consider $E : y^2 = x^3 - x, K = \mathbb{Q}(i)$. Then $\mathbf{f} = \mathcal{P}_2^3$, where $\mathcal{P}_2 = (1+i)$. Then $[K(E_{\mathbf{f}}) : K] = (\mathbb{Z}[i]/\mathcal{P}_2^3)^\times/4 = 1$. Hence we have $K(E_{\mathbf{f}}) = K(E_{(1+i)^3})$.

Proof First note that $R_{\mathcal{G}} \subset K(E_{\mathcal{G}})$. Consider $\sigma_{\mathfrak{a}} \in Gal(K(E_{\mathcal{G}})/K)$, where $\mathfrak{a}$ is an integral ideal prime to $\mathcal{G}$. We show that $\sigma_{\mathfrak{a}}$ fixes $R_{\mathcal{G}}$ implies $\mathfrak{a} = (\alpha), \alpha \equiv 1 \ mod\ \mathcal{G}$. $\sigma_{\mathfrak{a}}(P) = \psi_E(\mathfrak{a})(P) = \alpha(P) = P$, which completes the proof. □

Example 6.8. Consider $E : y^2 = x^3 - Dx, K = \mathbb{Q}(i), D \geq 1$, where D is a fourth power free.

It is the fact that if we let Δ be the product of the distinct primes dividing D, then $\mathbf{f}$ is $(1+i)^3\Delta\mathbb{Z}[i]$ when $D \equiv 1(mod 4)$, and $(1+i)^4\Delta\mathbb{Z}[i]$ otherwise.

(1) If D=17 then $y^2 = x^3 - 17x, \mathbf{f} = (1+i)^3 \cdot 17 \cdot \mathbb{Z}[i] = \mathcal{P}_2^3 \cdot \mathcal{P}_{17} \cdot \mathcal{P}_{17}^*$. Then $\#((\mathbb{Z}[i]/\mathbf{f})^\times) = 4 \cdot 16^2$ and $\#Gal(K(E_{\mathbf{f}}/K)) = 16^2 = 256$.
(2) If $D = 226$ then we have $\mathbf{f} = (1+i)^4 \cdot 2 \cdot 113 \cdot \mathbb{Z}[i] = (1+i)^6 \cdot 113 \cdot \mathbb{Z}[i] = \mathcal{P}_2^6 \cdot \mathcal{P}_{113} \cdot \mathcal{P}_{113}^*$, and $[K(E_{\mathbf{f}}) : K] = 8 \cdot (112)^2$.

Consider ψ_E^n where $(n, \#(\mu_K)) = 1$ such that ψ_E^n has a conductor $\mathbf{f}$.

Remark 6.9. In general, ψ_E^n may have conductor smaller than $\mathbf{f}$. If $\#(\mu_K)|n$, then ψ_E^n has conductor $\mathbf{f} = \mathcal{O}_K$.

How do we analytically continue $L(\bar{\psi}_K^n; s) = \sum_{(\mathfrak{a},\mathbf{f})=1} \frac{\bar{\psi}_E(\mathfrak{a})^n}{(N\mathfrak{a})^s}$?

6.1. **Kronecker-Eisenstein series.**

Definition 6.10. L is any lattice in $\mathbb{C}$. We define

$$H_K(z, s, L) := \sum_{w \in L} \frac{(\bar{z} + \bar{w})^k}{|z + w|^{2s}}.$$

This is a holomorphic function in s when $Re(s) > 1 + \frac{k}{2}$ and in fact $\Gamma(s)H_K(z, s, L)$ can be analytically continued to $\mathbb{C}$.

Definition 6.11. Suppose that $\mathbf{f}$ is the conductor of ψ_E. We define B to be the set of integral ideal of K prime to $\mathbf{f}$, with $Gal(K(E_\mathbf{f})/K) = \{\sigma_p : p \in B\}$ where $F = (\mathbf{f})$.

We will see the following theorem in the next lecture.

Theorem 6.12. *For all integer $n \geq 1$, with $(n, \#(\mu_K)) = 1$, we have*

$$L(\bar{\psi}_E^n, s) = \frac{|\Omega_\infty / f|^{2s}}{(\overline{\Omega_\infty / f})^n} \sum_{v \in B} H_n(\frac{\psi_E(v)\Omega_\infty}{f}, s, L).$$

7. **7th Lecture**

Let E/K be an elliptic curve and $End_K(E) \cong \mathcal{O}_K, K \hookrightarrow \mathbb{C}$. Let ψ_E be the Grossencharacter of E/K and $\mathfrak{f}$ be the conductor of ψ_E. And $\mathfrak{L} = \Omega_\infty \mathcal{O}_K$.

Let $k \geq 1$, L be any lattice in $\mathbb{C}$ and $(n, \#(\mu_K)) = 1$. Then $H_n(z, s, L) = \sum_{w \in L} \frac{(\bar{z} + \bar{w})^n}{|z + w|^{2s}}$ is holomorphic in s when $Re(s) > 1 + \frac{n}{2}$.

Theorem 7.1. *For all integers $n \geq 1$ with $(n, \#(\mu_K)) = 1$, we have*

$$L(\bar{\psi}_E^n, s) = \frac{|\Omega_\infty / f|^{2s}}{(\Omega_\infty / f)^n} \sum_{b \in \mathcal{B}} H_n(\frac{\psi_E(b)\Omega_\infty}{f}, s, \mathfrak{L})$$

where f is a generator of $\mathfrak{f}$.

This is the key observation. Consider the field extension $K(E_\mathfrak{f}) = R_\mathfrak{f}$ of K. Then $\#(\Delta) \cong (\mathcal{O}/\mathfrak{f})^*/\tilde{\mu}_K$. For $b \in \mathcal{B}, \sigma_b \in Gal(K(E_\mathfrak{f})/K)$. Look at the ideal $(\psi_E(b)+c)$ where b runs over $\mathcal{B}$ and c runs over $\mathfrak{f}$. Those are all integral ideals of K, prime to $\mathfrak{f}$, precisely once. Then

$$\begin{aligned} L(\bar{\psi}_E^n, s) &= \sum_{(\mathfrak{a},\mathfrak{f})=1} \frac{\bar{\psi}^n(\mathfrak{a})}{(N\mathfrak{a})^s} \\ &= \sum_{b\in\mathcal{B}} \sum_{c\in\mathfrak{f}} \frac{\bar{\psi}_E^n((\psi_E(b)+c))}{|\psi_E(b)+c|^{2s}}. \end{aligned}$$

Note that $(\psi_E(b)+c) = (\psi_E(b))(1+\frac{c}{\psi_E(b)}) = b(1+\frac{c}{\psi_E(b)})$. So $\psi_E((\psi_E(b)+c)) = \psi_E(b)(1+\frac{c}{\psi_E(b)}) = \psi_E(b)+c$ as $c \in \mathfrak{f}$. From this we have

$$\begin{aligned} L(\bar{\psi}_E^n, s) &= \sum_{b\in\mathcal{B}} \sum_{c\in\mathfrak{f}} \frac{(\overline{\psi_E(b)+c})^n}{|\psi_E(b)+c|^{2s}} \\ &= \frac{|\Omega_\infty/\mathfrak{f}|^{2s}}{(\Omega_\infty/\mathfrak{f})^{2n}} \sum_{b\in\mathcal{B}} \sum_{w\in\alpha} \frac{(\overline{\frac{\psi_E(b)\Omega_\infty}{\mathfrak{f}}+w})^n}{|\frac{\psi_E(b)\Omega_\infty}{\mathfrak{f}}+w|^{2s}}. \end{aligned}$$

Remark that $H_n(\frac{\psi_E(b)\Omega_\infty}{f}, s, \mathcal{L})$ converges $Re(s) > 1+\frac{n}{2}$. If $s = n$, then $n > 1+\frac{n}{2}$ if and only if $n > 2$. And it is equivalent $n > 1$ since $(n, \#(\mu_K)) = 1$.

Assume that $n > 2$. Then $H_n(z, n, L = \sum_{w\in L} \frac{1}{(z+w)^n}$. The Weierstrass $mathcalP$-function $\mathcal{P}(z, L)$ satisfies the following relation:

$$\mathcal{P}'(z, L)^2 = 4\mathcal{P}^3(z, L) - g_2(L)\mathcal{P}(z, L) - g_3(L).$$

This gives a map $\mathbb{C}/L \to \epsilon(C)$ defined by $z \bmod L \mapsto (\mathcal{P}(z, L), \mathcal{P}'(z, L))$. So $H_n(z, n, L) = \frac{(-1)^n}{(n-1)!}\mathcal{P}^{(n-2)}(z, L)$. Then the elliptic curve E/K has the following coordinates:

$$\begin{aligned} x &= \mathcal{P}(z, \mathcal{L}) - \frac{a_1^2 + 4a_2}{12}, \\ y &= \frac{1}{2}(\mathcal{P}'(z, \mathcal{L}) - a_1(\mathcal{P}(z, \mathcal{L}) - \frac{a_1^2 + 4a_2}{12}) - a_3). \end{aligned}$$

Corollary 7.2. *Assume* $n > 1, (n, \#(\mu_K)) = 1$. *Then*

$$\begin{aligned}\Omega_\infty^{-n} L(\bar{\psi}_E^n, n) &= -\frac{f^{-n}}{(n-1)!}\sum_{b\in\mathcal{B}} \mathcal{P}^{(n-2)}(\frac{\psi_E(b)\Omega_\infty}{f}, \mathcal{L}) \\ &= -\frac{f^n}{(n-1)!} Tr_{K(E_\mathfrak{f})/K}(\mathcal{P}^{(n-2)}(\frac{\Omega_\infty}{f}, \mathcal{L})) \in K.\end{aligned}$$

Note that $\mathcal{P}^{(n-2)}(z, \mathcal{L}) = D_n(\mathcal{P}(z, \mathcal{L}))\mathcal{P}'(z, \mathcal{L})$ where $D_n(T) \in K[T]$.

Remark 7.3. $(\mathcal{P}(\frac{\Omega_\infty}{f}, \mathcal{L}), \mathcal{P}'(\frac{\Omega_\infty}{f}, \mathcal{L}))^{\sigma_b} = (\mathcal{P}(\frac{\psi_E(b)\Omega_\infty}{f}, \mathcal{L}), \mathcal{P}'(\frac{\psi_E(b)\Omega_\infty}{f}, \mathcal{L}))$.

Proposition 7.4. $L(\bar{\psi}_E^n, n) \neq 0$ *because the Euler product for* $n \geq 1$ *is*

$$L(\bar{\psi}_E^n, n) = \prod_{(v,\mathfrak{f})=1} (1 - \frac{\bar{\psi}_E^n(v)}{(Nv)^n})^{-1}.$$

Let L be any lattice. We will consider the analytic continuation of $H_1(z, s, L)$ to $Re(s) > \frac{1}{2}$. Recall that $H_1(z, s, L) = \sum_{w\in L} \frac{(\bar{z}+\bar{w})}{|z+w|^{2s}}$.

Definition 7.5. $\Phi(z, s, L) = \frac{\bar{z}}{|z|^{2s}} + \sum_{w\in L\setminus\{0\}} \{\frac{\bar{z}+\bar{w}}{|z+w|^{2s}} - \frac{\bar{w}}{|w|^{2s}}(1 - \frac{sz}{w} - \frac{(s-1)\bar{z}}{\bar{w}})\}$.

This converges for $Re(s) > \frac{1}{2}$. And $\Phi(z, s, L) = H_1(z, s, L) + sz\sum_{\substack{w\in L\\ w\neq 0}} w^{-2}|w|^{-2s} + (s-1)\bar{z}\sum_{w\in L} \frac{1}{|w|^{2s}}$ for $Re(s) > \frac{3}{2}$. Note that $\sum_{\substack{w\in L\\ w\neq 0}} \bar{w}|w|^{2-2s} = 0$. In this way, we see that $H_1(z, s, L)$ can be continued analytically to $Re(s) > \frac{1}{2}$.

Note that $\Phi(z, 1, L) = \zeta(z, L)$ and $\mathcal{P}(z, L) = -\frac{d}{dz}\zeta(s, L)$. And $\sum_{w\in L} \frac{1}{|w|^{2s}}$ has a simple pole at $s = 1$ with the residue $\frac{1}{A(L)}$ where $A(L) = \frac{\bar{u}v - \bar{v}u}{2\pi i} > 0$ for $L = \mathbb{Z}u + \mathbb{Z}v, Im(v/u) > 0$. Let $s_2(L) = \lim_{\substack{t\to 0\\ t>0}} \sum_{\substack{w\in L\\ w\neq 0}} w^{-2}|w|^{-2t}$.

Theorem 7.6. $H_1(z, 1, L) = \zeta(s, L) - zs_2(L) - \bar{z}A(L)^{-1}$.

It is not holomorphic in z. Eisenstein defined

$$E_1^*(z, L) := \zeta(z, L) - zs_2(L) - \bar{z}A(L)^{-1}.$$

Theorem 7.7. $\Omega_\infty^{-1} L(\bar{\psi}_E, 1) = f^{-1} \sum_{b \in \mathcal{B}} E_1^*(\psi_E(b)\Omega_\infty^{-1}/f, \mathcal{L})$.

Then we have the following questions: Does it belong to $K(E_\mathfrak{f})$? And if it is true then does it belong to $E_1^*(\frac{\Omega_\infty}{f})^{\sigma_b}$. In fact, these are true.

8. **8th Lecture**

Let E/K be an elliptic curve with $End_K(E) = \mathcal{O}_K$, ψ_K, $\mathbf{f} = (f)$.

Theorem 8.1. *We have*

$$\Omega_\infty^{-1} L(\bar{\psi}_E, s) = f^{-1} \sum_{v \in B} E_1^*(\psi_E(1_E)^{\frac{\Omega_\infty}{f}}, \mathcal{L}) = f^{-1} Tr_{K(E_f)/K}(E_1^*(\frac{\Omega_\infty}{f}, \mathcal{L})),$$

where $E_1^*(z, \mathcal{L}) = \zeta(z, \mathcal{L}) \cdot z s_2(\mathcal{L}) \bar{z} A(\mathcal{L})^{-1}$, *and* $A(\mathcal{L}) = \frac{1}{2\pi i} \Omega_\infty \overline{\Omega_\infty} \sqrt{d_K}$.

Consider $f_a(T) = \frac{(1+T)^{-a/2} - (1+T)^{a/2}}{(1+T)^{-1/2} - (1+T)^{1/2}}$, where $(a, p) = 1 \in \mathbb{Z}_p[[T]]$. Then if ζ_n is a primitive p^{n+1}th root of 1,

$$f_a(\zeta_n - 1) = \frac{\zeta_n^{-a/2} - \zeta_n^{a/2}}{\zeta_n^{-1/2} - \zeta_n^{1/2}}.$$

Moreover,

$$\frac{d}{dz} \log f(e^z - 1) = \sum_{n=2}^{\infty} \zeta(1-n)(1-a^n) \frac{z^{n-1}}{(n-1)!}.$$

Example 8.2. Let $K = \mathbb{Q}(i)$, $E : y^2 = x^3 - Dx, D \geq 1$, fourth power free. Take $\lambda = 2 + i$. Then $\#(E_\lambda) = 5 = N\lambda$. Let V be a primitive λ-division point on E. We claim that $x(V)^2 \in K = \mathbb{Q}(i)$.

Consider the tower of fields

$$\begin{array}{c} K(x(V)^2) \\ | \\ K. \end{array}$$

Note that $K(x(V)^2)$ is the ray class field of K mod λ and the Galois group $\mathbb{Z}[i]/(2+i))^\times/\tilde{\mu}_4$ is of order 1, which completes the proof.

In fact $x(V)^2 = \frac{P}{1+2i}$ and $J(P) = (x^2 - x(V)^2)^{-1}$. What is the p-adic analogue of $L(\bar{\psi}_E, s)$? We use p-adic interpolation of certain "special values".

Theorem 8.3. *For all integers $n \geq 1$ and $m \geq 0$, we have*

$$(2\pi i)^m \Omega_\infty^{-(n+m)} L(\bar{\psi}_E^{n+m}, n) \in K.$$

Let p be a prime in K. Then we have an embedding $K \hookrightarrow K_p$. Consider the map:

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \to & K_p \\ (n, m) & \mapsto & (2\pi i)^m \Omega_\infty^{-(n+m)} L(\bar{\psi}_E^{n+m}, n). \end{array}$$

Does this extend to some nice continuous function on $\mathbb{Z}_p \times \mathbb{Z}_p$?

(1) When there is just one prime of $K/\mathbb{Q}$ above p, unknown.
(2) When $p\mathcal{O}_K = \mathcal{P}\mathcal{P}^*$, $\mathcal{P}$ is not equal to $\mathcal{P}^*$, there is a beautiful function!

Henceforth, we assume that

(1) $(p, \#(\mu_K)) = 1$.
(2) $(\mathcal{P}, f) = 1$.
(3) $p\mathcal{O}_K = \mathcal{P}\mathcal{P}^*$.

For example, $y^2 = x^3 - Dx, D \geq 1$ fourth power-free, $(p, D) = 1$, $\mathcal{P} \equiv 1 (mod 4)$.

Let $\Omega_\infty \in \mathbb{C}$, and $\hat{E}^{\mathcal{P}}$ be the formal group of E at $\mathcal{P}$, $t = -x/y$. And $\hat{G}_m$, $f(U, V) = (1 + U)(1 + V) - 1 = U + V + VU$. Let I be the completion with respect to the $1|p$ of the ring of integers of the maximal unramified extension of $\mathbb{Q}_p = K_{\mathcal{P}}$.

Theorem 8.4. *(Tate) There exists an isomorphism $\delta_{\mathcal{P}} : \hat{G}_m \to \hat{E}^{\mathcal{P}}$ defined over I, given by a formal power series $t = \delta_p(u) \in I[[u]]$ such that $t = \Omega_{\mathcal{P}^n} + \cdots$.*

Note that $\delta_{\mathcal{P}}$ is an isomorphism if and only if $\Omega_{\mathcal{P}} \in I^\times$.

Theorem 8.5. *Assume that Ω_∞ and $\Omega_{\mathcal{P}}$ are fixed. Then there exists a unique power series $H_{\mathcal{P}}(T) \in I[[T]]$ such that for all integers $n \geq 1$ with $n \equiv 1 \, mod (p-1)$ we have*

$$\Omega_{\mathcal{P}}^{-n} H_{\mathcal{P}}((1 + p)^n - 1) = \Omega_\infty^{-n} (n - 1)! L(\bar{\psi}_E^n, n)(1 - \frac{\psi_E^n(\mathcal{P})}{N\mathcal{P}}).$$

Note that since $(1 + p)^s - 1 \in p\mathbb{Z}_p$, for all $s \in \mathbb{C}$, the left hand side is convergent.

Definition 8.6. $L_{\mathcal{P}}(E, s) := H_{\mathcal{P}}((1 + p)^s - 1)$ for all $s \in \mathbb{Z}_p$.

Then we have the naive question: Does $L_{\mathcal{P}}(E,s)$ behave like $L(\bar{\psi}_E,s)$?

Let $E/\mathbb{Q}$ be elliptic curve and $g_{E/\mathbb{Q}}$ be the rank of $E(\mathbb{Q})$. Note that

$$Ш(E/\mathbb{Q})(p) = (\mathbb{Q}_p/\mathbb{Z}_p)^{t_{E/\mathbb{Z},p}} \oplus (finite\ group).$$

Theorem 8.7. *$L_{\mathcal{P}}(E,s)$ has a zero at $s=1$ of order at least $g_{E/\mathbb{Q}} + t_{E/\mathbb{Q},p}$. Moreover, if the order of the zero at $s=1$ is $g_{E/\mathbb{Q}}$, there exists an exact formula for the order of p-primary subgroup in terms of the coefficients of $(s-1)^{g_{E/\mathbb{Q}}}$.*

Example 8.8. Let $E: y^2 = x^3 - 17x$, $g_{E/\mathbb{Q}} = 2$. For $p \equiv 1 \bmod 4$, p not 17 check numerically that for all such $p < 29700$. $L_{E,\mathcal{P}}(s)$ has zero at $s=1$ of order 2, and $Ш(E/\mathbb{Q})(p) = 0$.

Definition 8.9. $r_{E/\mathbb{Q},\mathcal{P}} := \mathrm{ord}_{s=1} L_{\mathcal{P}}(E,s)$.

Theorem 8.10. *For every $\epsilon > 0$, we have $r_{E/\mathbb{Q},\mathcal{P}} \leq (1-\epsilon)p$ for all sufficiently large p which split in K.*

9. **9th Lecture**

Let E/K be an elliptic curve with $(p, \#(\mu_K)) = 1, (p, \mathfrak{f}) = 1, p\mathcal{O}_K = \mathcal{P}\mathcal{P}^*$.

9.1. **Arithmetic of E over K.** Consider $\mathbb{Z}_p$-extension of K. Classfield theory tells us that F_∞ is the completion of all $\mathbb{Z}_p$-extension of K with $Gal(F_\infty/K) \cong \mathbb{Z}_p^2$.

Let $E_{\mathcal{P}^n} = Ker(E(\bar{K}) \to^{\pi^n} E(\bar{K})), \pi = \psi_E(\mathcal{P})$. And $E_{\mathcal{P}^\infty} = \bigcup_{n\geq 1} E_{\mathcal{P}^n} = \mathbb{Q}_p/\mathbb{Z}_p$. Then we see that $E_{p^\infty} = E_{\mathcal{P}^\infty} \oplus E_{\mathcal{P}^{*\infty}}$. Consider the field extension

$$\begin{array}{c} K(E_{\mathcal{P}^\infty}) \\ | \\ K_{\mathcal{P}} \\ | \\ K. \end{array}$$

Then $Gal(K(E_{\mathcal{P}^\infty})/K) \hookrightarrow^{\chi_p} \mathbb{Z}_p^* = Aut(E_{\mathcal{P}^\infty})$. Note that since $(\mathcal{P}, \mathfrak{f}) = 1$, χ_p is an isomorphic and $\mathcal{P}$ is totally ramified in $K(E_{\mathcal{P}^\infty})$.

Definition 9.1. K_∞ is the unique $\mathbb{Z}_p$-extension of K contained in $K(E_{\mathfrak{P}^\infty})$. In fact, K_∞ is the unique $\mathbb{Z}_p$-extension of K unramified outside $\mathcal{P}$.

Let M be any algebraic extension of K.

Definition 9.2.

$$\begin{aligned} Sel_{\mathfrak{P}}(E/M) &= Ker(H^1(Gal(\bar{K}/K), E_{\mathfrak{P}^\infty}) \\ &\quad \to \prod_w H^1(Gal(\bar{M}_w/M_w), E(\bar{M}_w))). \end{aligned}$$

Note that $Sel_{\mathfrak{P}}(E/M) = Sel_p(E/M) \cap H^1(Gal(\bar{K}/K), E_{\mathfrak{P}^\infty})$. And $X_{\mathfrak{P}}(E/M) = Hom(Sel_{\mathfrak{P}}(E/M), \mathbb{Q}_p, \mathbb{Z}_p)$. This is compact and discrete. In particular, let $\Gamma = Gal(K_\infty/K)$. Then Γ acts on $Sel_{\mathfrak{P}}(E/K_\infty)$ and $X_{\mathfrak{P}}(E/K_\infty)$. They are $\mathbb{Z}_p$-modules and hence modules over $\Lambda(\Gamma) = \lim_{\leftarrow U} \mathbb{Z}_p[\Gamma/U]$. Recall that $\Lambda(\Gamma) \cong \mathbb{Z}_p[[T]]$ given by $\gamma \mapsto 1 + T$ where γ is the topological generator. We choose γ so that $\chi_{\mathfrak{P}}(\gamma) = 1 + p$.

9.2. **Main Conjecture.** This gives a precise relation between $\Lambda(\Gamma)$-module $X_{\mathfrak{P}}(E/K_\infty)$ and $H_{\mathfrak{P}}(T), L_{\mathfrak{P}}(E, s)$, i.e. this gives the relation between the algebraic structure and L-function.

Theorem 9.3. *$X_{\mathfrak{P}}(E/K_\infty)$ is a finitely generated torsion $\Lambda(\Gamma)$-module.*

Recall that $\Lambda[T] = \mathbb{Z}_p[[T]]$. It is not a principal ideal domain. In particular, the maximal ideal $m = (p, T)$ is not principal. Let Y be any finitely generated torsion $\Lambda(T)$-module. Then there is always an exact sequence of $\Lambda(\Gamma)$-modules of the following form:

$$0 \to \bigoplus_{i=1}^{r} \Lambda(\Gamma)/f_i\Lambda(\Gamma) \to Y \to D \to 0, \#(D) < \infty.$$

In fact, $f_i \neq 0$ because it is a torsion module.

Definition 9.4. $char_\Gamma(Y) = f_1 \cdots f_r \Lambda(T)$.

Consider $char_{\mathbb{Z}_p[[T]]}(X_{\mathfrak{P}}(E/K_\infty)) = B_{\mathfrak{P}}(T)\mathbb{Z}_p[[T]]$. This is the definition of $B_{\mathfrak{P}}(T)$.

Conjecture 9.5. *(Main Conjecture)* $H_{\mathfrak{P}}((1 + p)T - 1)\mathfrak{I}[[T]] = B_{\mathfrak{P}}(T)\mathfrak{I}[[T]]$.

This conjecture is true. Note that $H_{\mathfrak{P}}((1+p)T-1)\mathfrak{I}[[T]]$ is coming from $L_{\mathfrak{P}}(E,s)$ and $B_{\mathfrak{P}}(T)\mathfrak{I}[[T]]$ is coming from $X_{\mathfrak{P}}(E/K_\infty)$.

Theorem 9.6. *$B_{\mathfrak{P}}(T)$ has a zero at $T=0$ of order $\geq g_{E/\mathbb{Q}}+t_{E/\mathbb{Q},p}$.*

Proof There is a natural surjection of $\mathbb{Z}_p[[T]]$-modules from $X_{\mathfrak{P}}(E/K_\infty) \twoheadrightarrow (\mathbb{Z}_p[[T]]/(T))^{g_{E/\mathbb{Q}}+t_{E/\mathbb{Q},p}}$. Consider

$$\begin{array}{ccccc} K_\infty & Sel(E/K_\infty) & \subset & H^1(Gal(\bar{K}/K_infty), E_{\mathfrak{P}^\infty}) \\ | & \uparrow & & \uparrow \\ K & Sel_{\mathfrak{P}}(E/K) & \subset & H^1(Gal(\bar{K}/K), E_{\mathfrak{P}^\infty}). \end{array}$$

This is injective because $E_{\mathfrak{P}^\infty}(K_\infty)=0$. So we have $X_{\mathfrak{P}}(E/K_\infty) \to X_{\mathfrak{P}}(E/K) \to X_{\mathfrak{P}}(E/K)/X_{\mathfrak{P}}(E/K)_{tor} = \mathbb{Z}_p^{g_{E/\mathbb{Q}}+t_{E/\mathbb{Q},p}}$.