Modularity Theorem of Elliptic Curves and Eichler-Shimura Relation

Wenrong Zou, Yulin Peng
Advisor: Bingchen Lin

March, 2023

Contents

Abstract

Modular forms is a significant part of the main theorem in this article. In the first section, we will explain the definition and basic propties of modular forms, and then its simple connection with elliptic curves. And the second section will explain the Hecke operators, which not only important in the theorem of modular forms itself, but also select modular forms we need in the main theroem, whcih illustrate the deep connection between modular forms and elliptic curves. What's more, we will discuss the differential forms on the elliptic curve. In the last section, we will give two proofs of Eichler-Shimura Relation.

1 Basic definition of modular forms

A modular form is a holomorphic function on the upper half complex plane $\mathcal{H}$, which have two positive integer parametes: weight k and level N. We concentrate on level 1 first for simplicity.

Let $\mathrm{SL}_2(\mathbb{Z})$ be the group of 2×2 matrix with determinant 1 and integer entries. $\forall \tau \in \mathcal{H}, \gamma \in \mathrm{SL}_2(\mathbb{Z})$ we define $\gamma(\tau) = \frac{a\tau+b}{c\tau+d}$, where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. A modular form of level 1 can be viewed as defined on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$, which means that $\forall \tau \in \mathcal{H}$ we can know the value of $\gamma(\tau), \forall \gamma$ form the value of τ.

Definition 1.1 (Modular forms of level 1)**.** A *modular form of level 1 and weight k* is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ with the following propties:

1. $f(\gamma(\tau)) = (c\tau + d)^k f(\tau), \forall \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\forall \tau \in \mathcal{H}$.
2. f is holomorphic at ∞.

The set of all modular forms of level 1 and weight k is denoted by $M_k(\mathrm{SL}_2(\mathbb{Z}))$.

Remark 1.1.

1. To make $f(\infty)$ well defined, we first notice that we have $f(\tau + 1) = f(\tau)$ if we choose $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in property 1, so take the *Fourier expansion* we have

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f) q^n, \quad q = e^{2\pi i \tau}.$$

So $q \to 0 \Leftrightarrow Im(\tau) \to \infty$, and then we define f is holomorphic at ∞ if and only if $\lim_{Im(\tau)\to\infty} f(\tau)$ exists or equally $f(\tau)$ is bounded as $Im(\tau) \to \infty$.

2. If we choose $\gamma = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ in property 1, we have $f(\gamma(\gamma(\tau))) = (-1)^k f(\tau)$, so when k is odd, $M_k(\mathrm{SL}_2(\mathbb{Z})) = 0$.

And then we can define the *cusp forms*:

Definition 1.2 (Cusp forms)**.** A cusp form of weight k is a modular form of weight k and $a_0 = 0$ in its Fourier expansion or equally $\lim_{Im(\tau)\to\infty} f(\tau) = 0$.

The set of all cusp forms of level 1 and weight k is denoted by $S_k(\mathrm{SL}_2(\mathbb{Z}))$.

The name cusp form comes from the conception of cusp point, it's ∞ for $\mathrm{SL}_2(\mathbb{Z})$.

Example 1.1.

1. The zero function on $\mathcal{H}$ is a modular form of every weight, and every constant function on $\mathcal{H}$ is a modular form of weight 0.
2. For nontrivial examples, let $k > 2$ be an even integer and define the Eisenstein series of weight k to be a 2-dimensional analog of the Riemann zeta function $\zeta(k) = \sum_{d=1}^{\infty} 1/d^k$,

$$G_k(\tau) = \sum_{(c,d)'} \frac{1}{(c\tau + d)^k}, \quad \tau \in \mathcal{H},$$

where the primed summation sign means to sum over nonzero integer pairs $(c, d) \in \mathbb{Z}^2 - \{(0, 0)\}$. We can prove that G_k is holomorphic on $\mathcal{H}$ and its terms may be rearranged (Ferd, p4). For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, compute that

$$\begin{aligned} G_k(\gamma(\tau)) &= \sum_{(c',d')'} \frac{1}{\left(c'\left(\frac{a\tau+b}{c\tau+d}\right) + d'\right)^k} \\ &= (c\tau + d)^k \sum_{(c',d')'} \frac{1}{((c'a + d'c)\tau + (c'b + d'd))^k}. \end{aligned}$$

But as (c', d') runs through $\mathbb{Z}^2 - \{(0,0)\}$, so does $(c'a + d'c, c'b + d'd) = (c', d')\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and so the right side is $(c\tau + d)^k G_k(\tau)$, showing that G_k is weakly modular of weight k. Finally, G_k is bounded as $\mathrm{Im}(\tau) \to \infty$, so it is a modular form.

To define the modular forms for general level, we need the conception of congruence subgroup. Let $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$ denote the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with all matrix of the form

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}(modN), \qquad \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}(modN), \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}(modN)$$

respectively, where $*$ denotes any integer $modN$. It's easy to see that $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$, and when $N|M, \Gamma_i(M) \supset \Gamma_i(N), \forall i$.

Definition 1.3 (Congruence subgroups)**.** A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup of level N* if it contains $\Gamma(N)$ for some N.

Remark 1.2.

1. $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$ are congruence subgroups of level N.
2. If $N|M$ and Γ is a congruence subgroup of level N, then it's a congruence subgroups of level M.

A modular form of level N satisfied similar propties of Definition1.1, but we need to konw the cusp points for general congruence subgroups first. We expend the action $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ to $\mathcal{H} \cup \mathbb{Q} \cup \infty$ as the following:

1. $\forall q \in \mathbb{Q}$, we define $\gamma(q) = \frac{aq+b}{cq+d}$ is another rational number if $cq + d \neq 0$ and $\gamma(q) = \infty$ otherwise.
2. For ∞, we define $\gamma(\infty) = a/c$ if $c \neq 0$ and $\gamma(\infty) = \infty$ otherwise.

As Γ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$, we can restrict this action on Γ, and the orbits of this restriction on $\mathbb{Q} \cup \infty$ is the cusp points of Γ.

As the level 1 case, the modular form of level N need to be holomorphic at all cusp forms, to make the value of f on $\mathbb{Q}$ well defined, we define an action of $\mathrm{SL}_2(\mathbb{Z})$ on holomorphic functions on $\mathcal{H}$ by:

$$(f[\gamma]_k(\tau)) = j(\gamma, \tau)^{-k} f(\gamma(\tau)), \quad \forall \gamma \in \mathrm{SL}_2(\mathbb{Z}), \quad \tau \in \mathcal{H},$$

where $j(\gamma, \tau) = c\tau + d$.

Lemma 1.1. *For this action, $\forall \gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$, we have:*

1. $j(\gamma\gamma', \tau) = j(\gamma, \gamma'(\tau))j(\gamma', \tau)$,
2. $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$,
3. $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$,
4. $Im(\gamma(\tau)) = \frac{Im(\tau)}{|j(\gamma,\tau)|^2}$,
5. $\frac{d\gamma(\tau)}{d\tau} = \frac{1}{j(\gamma,\tau)^2}$.

So this is a well defined action, it's easy to see that if $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ then $f[\gamma]_k = f$. For a cusp point q differ form ∞ of Γ, $\exists \gamma \in \mathrm{SL}_2(\mathbb{Z})$ s.t. $\gamma(q) = \infty$, so we can define $f(q)$ to be $f[\gamma]_k(\infty)$. With all these preparation, we can finally define the general modular forms:

Definition 1.4 (Modular forms)**.** A *modular form of weight k respect to* Γ *(so has level N)* is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ with the following propties:

1. $f(\gamma(\tau)) = (c\tau + d)^k f(\tau), \forall \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $\forall \tau \in \mathcal{H}$, where Γ is a congruence subgroup of level N,
2. $f[\alpha]_k$ is holomorphic at $\infty, \forall \alpha \in \mathrm{SL}_2(\mathbb{Z})$.

   If in additon,
3. $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k, \forall \alpha \in \mathrm{SL}_2(\mathbb{Z})$,

then f is a cusp form of weight k respect to Γ.

The set of all modular (resp. cusp) forms of weight k with respect to Γ denoted $M_k(\Gamma)$ (resp. $S_k(\Gamma)$).

Example 1.2. 1. All modular forms of level 1 is a modular forms of any level, so the examples in Example1.1 are examples here too.

2. For a generation of Example1.1, we extend k to $k = 2$, $G_2(\tau)$ is not a modular form, but

$$G_{2,N}(\tau) = G_2(\tau) - G_2(N\tau)$$

   is a modular form of level N and weight 2 (Fred, p18).

We need the following quite none-trivial theorem letter, for its proof, see (Fred, p85-p91).

Theorem 1.1 (finite dimension)**.** *The space $M_k(\Gamma)$ (and then $S_k(\Gamma)$) of any level as a complex vector space has finite dimension.*

2 Connection between modular forms and elliptic curves

In this section, we want to represent the definition domain of modular forms by the set related to elliptic curves. And then we can look modular forms as a function defined on the space of elliptic curves. To do this, we need the following definition first:

Definition 2.1 (Modular curve)**.** For any congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, acting on the upper half plane $\mathcal{H}$ from the left, the modular curve $Y(\Gamma)$ is defined as the quotient space of orbits under Γ ,

$$Y(\Gamma) = \Gamma\backslash\mathcal{H} = \{\Gamma\tau : \tau \in \mathcal{H}\}.$$

The modular curves for $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma(N)$ are denoted:

$$Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}, \quad Y_1(N) = \Gamma_1(N)\backslash\mathcal{H}, \quad Y(N) = \Gamma(N)\backslash\mathcal{H}.$$

And then there is a bijection of spaces as following:

Theorem 2.1 (Moduli space and Modular curve)**.** *Let N be a positive integer. The moduli space for $\Gamma_0(N)$ is*

$$\mathrm{S}_0(N) = \{[E_\tau, \langle 1/N + \Lambda_\tau\rangle] : \tau \in \mathcal{H}\}.$$

Two points $[E_\tau, \langle 1/N + \Lambda_\tau\rangle]$ and $[E_{\tau'}, \langle 1/N + \Lambda_{\tau'}\rangle]$ are equal if and only if $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Thus there is a bijection $\psi_0 : \mathrm{S}_0(N) \xrightarrow{\sim} Y_0(N)$, $[\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle] \mapsto \Gamma_0(N)\tau$.

Remark 2.1. The element in the space $\mathrm{S}_0(N)$ is called the enhanced elliptic curve.

Especially when $N = 1$, the above gives a bijecton between all elliptic curves and the modular space of $\mathrm{SL}_2(\mathbb{Z})$.

And then we can define the correspondence of functions, we define the functions on $\mathrm{S}_0(N)$ first.

Definition 2.2. A complex-valued function F of the enhanced elliptic curves for $\Gamma_0(N)$ is degree-k homogeneous with respect to $\Gamma_0(N)$ if for every nonzero complex number m,

$$F(\mathbb{C}/m\Lambda, mC) = m^{-k}F(\mathbb{C}/\Lambda, C).$$

The correspondence is as following:

Theorem 2.2. *There is a bijection of degree-k homogeneous function with respect to* $\Gamma_0(N)$ *on* $S_0(N)$ *and modular forms of weight k with respect to* $\Gamma_0(N)$ *by:*

$$f(\tau) = F\left(\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle\right).$$

The modular form f is called the corresponding dehomogenized function of F.

Remark 2.2.

1. Especially when $N = 1$, the above gives a bijecton between all degree-k homogeneous functions with respect to $SL_2(\mathbb{Z})$ on all elliptic curves and all modular forms with level 1 and weight k.
2. f is weight-k invariant with respect to $\Gamma_0(N)$. To see this, let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, and for any $\tau \in \mathcal{H}$, let $m = (c\tau + d)^{-1}$. Then, using the condition $(c, d) \equiv (0, 1)(\mathrm{mod}N)$ at the third step,

$$\begin{aligned} f(\gamma(\tau)) &= F\left(\mathbb{C}/\Lambda_{\gamma(\tau)}, \langle 1/N + \Lambda_{\gamma(\tau)}\rangle\right) = F\left(\mathbb{C}/m\Lambda_\tau, \langle m(c\tau + d)/N + m\Lambda_\tau\rangle\right) \\ &= m^{-k}F\left(\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle\right) = (c\tau + d)^k f(\tau). \end{aligned}$$

With all the preparation on the last two section, we can eventually study the mian tool to deal with modular forms: Hecke operators.

3 Hecke operators

3.1 L-series of a modular form

Let f be a cusp form of weight $2k$ for $\Gamma_0(N)$. It can be expressed

$$f(s) = \sum_{n\geq 1} c(n)q^n, \quad q = e^{2\pi iz}, \quad c(n) \in \mathbb{C}.$$

The L-series of f is the Dirichlet series

$$L(f, s) = \sum_{n\geq 1} c(n)n^{-s}, \quad s \in \mathbb{C}.$$

There is an estimate that $|c(n)| \leq Cn^k$ for some constant C, so its Dirichlet series is convergent for $\Re > k + 1$.

The *Mellin transform* can give us an alternative definition of the L-series of a modular form by integral.

Definition 3.1 (Mellin transform)**.** Let $f = \sum_{n\geq 1} c(n)q^n$ be a cusp form, the Mellin transform of f is:

$$g(s) = \int_0^\infty f(iy)y^s \frac{dy}{y}.$$

Remark 3.1. Ignoring problem of convergence, we have:

$$\begin{aligned} g(s) &= \int_0^\infty \sum_{n=1}^\infty c(n) e^{-2\pi n y} y^s \frac{dy}{y} \\ &= \sum_{n=1}^\infty c(n) \int_0^\infty e^{-t} (2\pi n)^{-s} t^s \frac{dt}{t} \quad (t = 2\pi n y) \\ &= (2\pi)^{-s} \Gamma(s) \sum_{n=1}^\infty c(n) n^{-s} \\ &= (2\pi)^{-s} \Gamma(s) L(f, s). \end{aligned}$$

So this gives an alternative definition of $L(f, s)$.

3.2 Connection with the L-series of an elliptic curves

By the definition, for an elliptic curve E over $\mathbb{Q}$,

$$L(E, s) = \prod_{p \text{ good}} \frac{1}{1 - a_p p^{-s} + p^{1-s}} \prod_{p \text{ bad}} \frac{1}{1 - a_p p^{-s}},$$

where a_p can be defined by E and whether a prime number p is good or bad can be read from the conductor N of E.

We can expand this product and get the Dirichlet series:

$$L(E, s) = \sum_{n \geq 1} a_n n^{-s}.$$

It has the following propties:

1. $E \sim E'$ as elliptic curves, if and only if $L(E, s) = L(E', s)$.
2. It has an Euler product representation, by definition.
3. Conjecturally it can be extended analytically on the whole complex plane satisfies the functional equation
$$\Lambda(E, s) = \omega_E \Lambda(E, 2 - s), \quad \omega_E = \pm 1,$$
where $\Lambda(E, s) = N^{s/2} (2\pi)^{-s} \Gamma(s) L(E, s)$.

Our aim now is to find modular forms which can have a L-function equals to a L-function of an elliptic curve. We do this by finding modular forms which have L-functions satisfied the above three properties. We can know from the last section that the first property can be fit automatically.

The Hecke operators, which will be defined on next subsection, can help us to find those modular forms satisfied the second property. We give its stretch first.

Property 3.1. For general f, $L(f, s)$ has an Euler product of the form:

$$L(f, s) = \prod_{gcd(p,N)=1} \frac{1}{1 - c(p) p^{-s} + p^{2k-1-s}} \prod_{p|N} \frac{1}{1 - c(p) p^{-s}},$$

if and only if:

$$(*) \begin{cases} c(mn) = c(m)c(n), & \text{if } \gcd(m, n) = 1; \\ c(p) \cdot c\left(p^r\right) = c\left(p^{r+1}\right) + p^{2k-1} c\left(p^{r-1}\right), & r \geq 1, \text{ if } p \text{ is prime to } N; \\ c\left(p^r\right) = c(p)^r, r \geq 1, & \text{if } p \mid N. \end{cases}$$

This can be proved by expand directly. And Hecke proved the following theorems.

Theorem 3.1 (Hecke)**.** *The Hecke operators $T(n)$, $n \in \mathbb{N}$ to be defined letter have the following properties:*

1. $T(mn) = T(m)T(n)$, *if* $\gcd(m, n) = 1$;
2. $T(p) \cdot T(p^r) = T\left(p^{r+1}\right) + p^{2k-1}T\left(p^{r-1}\right), r \geq 1,$ *if p is prime to N;*
3. $T(p^r) = T(p)^r, r \geq 1,$ *if* $p \mid N$;
4. *all $T(n)$ commute.*

Theorem 3.2 (Hecke)**.** *Let $f \in S_{2k}(\Gamma_0(N))$ be a simultaneously eigenvector for all $T(n)$, let $T(n)f = \lambda(n)f$ and let*

$$f(s) = \sum_{n\geq 1} c(n)q^n, \quad q = e^{2\pi iz}.$$

Then $c(n) = \lambda(n)c(1)$.

Remark 3.2. By the above theorems and properties, let $f(s) = \sum_{n\geq 1} c(n)q^n$ with $c(1) = 1$ be the one in the above theorem, then

$$L(f, s) = \prod_{gcd(p,N)=1} \frac{1}{1 - c(p)p^{-s} + p^{2k-1-s}} \prod_{p|N} \frac{1}{1 - c(p)p^{-s}}.$$

So our aim in the following subsections is to define the Hecke operators and find the simultaneously eigenvectors.

For the third property, we define an operator first:

$$W_N : S_k(\Gamma_0(N)) \to S_k(\Gamma_0(N)), \quad f \mapsto (\tau \mapsto i^k N^{-k/2}\tau^{-k} f(\frac{-1}{N\tau})).$$

It's easily to see that $W_N^2 = 1$, so decomposite by the eigenspaces we have:

$$S_k(\Gamma_0(N)) = S_k(\Gamma_0(N))^{+1} \oplus S_k(\Gamma_0(N))^{-1}.$$

Theorem 3.3 (Hecke)**.** *Let $f \in S_{2k}(\Gamma_0(N))^{\epsilon}$, where $\epsilon = \pm 1$. Then $L(f, s)$ can be extended analytically on the whole complex plane satisfies the functional equation:*

$$\Lambda(f, s) = \epsilon(-1)^k \Lambda(f, k - s),$$

where $\Lambda(f, s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f, s)$.

Remark 3.3. We know by the Mellin transform that $\Lambda(f, s) = N^{s/2}g(s)$, by some tricks we can extend the integral in $g(s)$ to the whole complex plane, so $\Lambda(f, s)$ can be extended analytically by Mellin transform.

For $k = 2$, this is exactly the functional equation that the L-function of an elliptic curve has. So we archive the third aim.

3.3 Definition of Hecke operators

In Section 2, we have explained the bijection from moduli space to modular curve, and then get a bijection of degree-k homogeneous function with respect to $\Gamma_0(N)$ on $S_0(N)$ and modular forms of weight k with respect to $\Gamma_0(N)$. To define Hecke operators, we concentrate on $N = 1$ first. To define an operator on $S_{2k}(\Gamma_0(1)) = S_{2k}(\mathrm{SL}_2(\mathbb{Z}))$, we first define a operator on $\mathcal{L}$, the space of all elliptic curves, or equally, on $\mathcal{D}$, the free alelian group generated by $\mathcal{L}$.

For $n \geq 1$, we define:

$$T(n) : \mathcal{D} \to \mathcal{D}, \Lambda \mapsto \sum_{(\Lambda:\Lambda')=n} \Lambda'$$

and

$$R(n) : \mathcal{D} \to \mathcal{D}, \Lambda \mapsto n\Lambda.$$

And we can prove by some easy properties of elliptic curves that:

Proposition 3.1. *1.* $T(mn) = T(m) \circ T(n)$, *if* $\gcd(m, n) = 1$;

2. $T(p) \circ T(p^r) = T\left(p^{r+1}\right) + pR(p) \circ T\left(p^{r-1}\right)$.

And by using these two properties repeatedly, we can get:

Corollary 3.4. *For any m, n,*

$$T(m) \circ T(n) = \sum_{d|gcd(m,n)} d \cdot R(d) \circ T(mn/d^2).$$

It's easy to see that $R(n)$ are commute to all other operators, and by the above corollary, we have:

Corollary 3.5. *All $T(n), R(n), n \geq 1$ are commute to each other.*

For a function $F : \mathcal{L} \to \mathbb{C}$, it equals a function $F : \mathcal{D} \to \mathbb{C}$ by extend linearity. The action of $T(n), R(n), n \geq 1$ on it is defined by:

$$(T \cdot F)(\Lambda) = F(T\Lambda), \quad T = T(n) \text{ or } R(n), n \geq 1.$$

And if F is degree-k homogeneous function with respect to $\Gamma_0(1)$, then by definition: $R(n) \cdot F = n^{-2k}F$. Composing this with the above properties, we have immediatly:

Proposition 3.2. *Let F be of degree-k homogeneous with respect to $\Gamma_0(1)$, then so dose $T(n) \cdot F$, and*

1. $T(mn) \cdot F = T(m) \cdot T(n) \cdot F$, *if* $\gcd(m, n) = 1$;

2. $T(p) \cdot T(p^r) \cdot F = T\left(p^{r+1}\right) \cdot F + p^{1-2k} T\left(p^{r-1}\right) \cdot F$.

And then we can finally define the Hecke operators for $N = 1$.

Definition 3.2. Let $f \in S_{2k}(\Gamma_0(1))$, and let F be the correspondence function on $\mathcal{L}$, we define Hecke operators $T(n), n \geq 1$ on $S_{2k}(\Gamma_0(N))$ to be:

$$(T(n) \cdot f)(z) = n^{2k-1}(T(n) \cdot F)(\Lambda(z, 1)),$$

which is the correspondence function of $n^{2k-1}T(n) \cdot F$.

For the general case $N \neq 1$, all things are similar, except in the second property of Proposition3.2, where it holds only when $gcd(p, N) = 1$, and when $p|N$, it is $T(p^r) \cdot F = T(p)^r \cdot F, r \geq 1$.

The Theorem3.1 follows easily from Proposition3.2. And for a proof of Theorem3.2, see (Milne, p202-p203).

3.4 The spectral theorem and Petersson inner product

In Subsection2, we conclude that our aim in these subsections is to define the Hecke operators and find the simultaneously eigenvectors, we have achieve the first part in the last subsection, for the second part, we need a theorem form linear algebra first, which the proof of it can be find on (Milne, p204).

Theorem 3.6 (Spectral theorem)**.** *Let V be a finite dimension complex vector space with a positive-definite hermitian form $<,>$. Let $\alpha_1, \alpha_2, ...$ be a sequence ofcommuting self-adjiont linear maps $V \to V$; then V has a basis of consisting of vectors that are eigenvectors for all α_i.*

So to find the simultaneously eigenvectors, we need a hermitian form on $S_{2k}(\Gamma_0(N))$ first. We define it by a special integral, to define this integral, we need the measure defined by: $\mu(U) = \iint_U \frac{dxdy}{y^2}$ for any open set U in the complex plane.

Proposition 3.3. *For any open set U in the complex plane, we have $\mu(\gamma U) = \mu(U), \forall \gamma \in \mathrm{SL}_2(\mathbb{R})$.*

This can be proved by a direct computation. And then we define the hermitian form, which is called *Petersson inner product*.

Definition 3.3 (Petersson)**.** Let $f, g \in S_{2k}(\Gamma_0(N))$, then

$$< f, g >= \iint_D f\overline{g}y^{2k}\frac{dxdy}{y^2},$$

is the Petersson inner product of f, g, where D is the fundamental area of $\Gamma_0(N)$ (i.e. a connect set of represent elements of $Y_0(N)$).

Remark 3.4. We can prove easily that $f\overline{g}y^{2k}$ is invariant under $\Gamma_0(N)$, so it is well defined on D.

Theorem 3.7 (Petersson)**.** *The above integral converges provided at least one of f or g is a cusp form. It therefore defines a positive-definite hermitian form on the vector space $S_{2k}(\Gamma_0(N))$ of cusp forms. The Hecke operators $T(n)$ are self-adjoint for all n relatively prime to N.*

Proof. Fairly straightforward calculus, see [3]. □

Remark 3.5. By composing Theorem1.1, Theorem3.6, and Theorem3.7, we have a decomposition:

$$S_{2k}(\Gamma_0(N)) = \oplus V_i$$

of $S_{2k}(\Gamma_0(N))$ into a direct sum of orthogonal subspaces V_i, each of which is a simultaneous eigenspace for all $T(n)$ with $gcd(n, N) = 1$.

Unfortunately, W_N dosen't commute with the $T(p)s$, $p|N$, while both of them commute with the $T(p)s$, $gcd(p, N) = 1$. To find the modular forms which satisfy this property, we need the last constraint: new forms.

3.5 Oldforms, Newforms and Eigenforms

The problem left by the last subsection has a simple remedy. If $M \mid N$, then $\Gamma_0(M) \supset \Gamma_0(N)$, and so $\mathcal{S}_{2k}(\Gamma_0(M)) \subset \mathcal{S}_{2k}(\Gamma_0(N))$. Recall that the N turns up in the functional equation for $L(f, s)$, and so it is not surprising that we run into trouble when we mix fs of level N with fs that are really of level $M \mid N$, $M < N$.

The way out of the problem is to define a cusp form that is in some subspace $\mathcal{S}_{2k}(\Gamma_0(M))$, $M \mid N$, $M < N$, to be old. The old forms form a subspace $\mathcal{S}_{2k}^{\mathrm{old}}(\Gamma_0(N))$ of $\mathcal{S}_{2k}(\Gamma_0(N))$, and the orthogonal complement

$\mathcal{S}_{2k}^{\text{new}}(\Gamma_0(N))$ is called the space of new forms. It is stable under all the operators $T(n)$ and W_N, and so $\mathcal{S}_{2k}^{\text{new}}$ decomposes into a direct sum of orthogonal subspaces W_i,

$$\mathcal{S}_{2k}^{\text{new}}(\Gamma_0(N)) = \bigoplus W_i$$

each of which is a simultaneous eigenspace for all $T(n)$ with $\gcd(n, N) = 1$. Since the $T(p)$ for $p \mid N$ and W_N each commute with the $T(n)$ for $\gcd(n, N) = 1$, each stabilizes each W_i. And then we have the following theorem.

Theorem 3.8 (Atkin-Lehner 1970)**.** *The spaces W_i in the above decomposition all have dimension* 1.

We take the modular form with $c(0) = 1$ in W_i, then it is naturally the eigenvector of $T(p)$ for $p \mid N$ and W_N. So they are exactly the modular forms we need, which is called Eigenforms.

4 Meromorphic Differentials

4.1 Automorphic Forms

Let $\hat{\mathbb{C}}$ denote the Riemann sphere $\mathbb{C} \cup \{\infty\}$. Recall that for an open subset $V \subset \mathbb{C}$, a function $f : V \to \hat{\mathbb{C}}$ is meromorphic if it is the zero function or it has a Laurent series expansion truncated from the left about each point $\tau \in V$,

$$f(t) = \sum_{n=m}^{\infty} a_n (t - \tau)^n \text{ for all } t \text{ in some disk about } \tau,$$

with coefficients $a_n \in \mathbb{C}$ and $a_m \neq 0$. The starting index m is the order of f at τ, which also means "order of vanishing" and denoted $\nu_\tau(f)$; the zero function is defined to have order $\nu_\tau(f) = \infty$. The function f is holomorphic at τ when $\nu_\tau(f) \geqslant 0$, it vanishes at τ when $\nu_\tau > 0$, and it has a pole at τ whe $\nu_\tau(f) < 0$. The set of meromorphic functions on V forms a field.

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Recall the weight-$k$ operator,

$$(f[\gamma]_k)(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau)), \quad j(\gamma, \tau) = c\tau + d \text{ for } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

As we mentioned before, a meromorphic function $f : \mathbb{H} \to \hat{\mathbb{C}}$ is called weakly modular of weight k with respect to Γ if $f[\gamma]_k = f$ for all $\gamma \in \Gamma$. To discuss meromorphy of f at ∞, let h be the smallest positive integer such that $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \in \Gamma$. Thus f has period h. If also f has no poles in some region $\{\tau \in \mathbb{H} : \mathrm{Im}(\tau) > c\}$ then f has a Laurent series on the corresponding punctured disk about 0,

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n q_h^n \text{ if } \mathrm{Im}(\tau) > 0, \text{ where } q_h = e^{2\pi i \tau / h}.$$

Then f is meromorphic at ∞ if this series truncates from the left, starting at some $m \in \mathbb{Z}$ where $a_m \neq 0$, or if $f = 0$. The order of f ar ∞, denoted $\nu_\infty(f)$, is again defined as the starting index m except when $f = 0$, in which case $\nu_\infty(f) = \infty$. Now automorphic forms are defined the same way as modular forms except with meromorphy in place of holomorphy.

Definition 4.1. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let k be an integer. A function $f : \mathbb{H} \to \hat{\mathbb{C}}$ is an automorphic form of weight k with respect to Γ if

(1) f is meromorphic,
(2) f is weight-k invariant under Γ,
(3) $f[\alpha]_k$ is meromorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

The set of automorphic forms of weight k with respect to Γ is denoted $\mathcal{A}_k(\Gamma)$.

Setting $k = 0$ in the definition shows that $\mathcal{A}_0(\Gamma)$ is the field of meromorphic functions on $X(\Gamma)$, denoted $\mathbb{C}(X(\Gamma))$.

4.2 Meromorphic Differentials

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The transformation rule for automorphic forms of weight k with respect to Γ,

$$f(\gamma(\tau)) = j(\gamma, \tau)^k f(\tau),\ \gamma \in \Gamma$$

does not make such forms Γ-invariant. On the other hand, we have obtained that $d\gamma(\tau) = j(\gamma, \tau)^{-2} d\tau$ for $\gamma \in \Gamma$ so that at least formally the differential

$$f(\tau)(d\tau)^{k/2}$$

is truly Γ-invariant. The aim of this section is to define differentials on the Riemann surface $X(\Gamma)$. The first step is to define differentials locally. Let V be any open subset of $\mathbb{C}$ and let $n \in \mathbb{N}$ be any natural number.

Definition 4.2. The meromorphic differentials on V of degree n are

$$\Omega^{\otimes n}(V) = \{f(q)(dq)^n : f \text{ is meromorphic on } V\}$$

where q is the variable on V.

These form a vector space over $\mathbb{C}$ under the natural definitions of addition and scalar multiplication, $f(q)(dq)^n + g(q)(dq)^n = (f + g)(dq)^n$ and $c(f(q)(dq)^n) = (cf)(dq)^n$. The sum over all degrees,

$$\Omega(V) = \oplus_{n \in \mathbb{N}} \Omega^{\otimes n}(V)$$

naturally forms a ring under the definition $(dq)^n (dq)^m = (dq)^{n+m}$

Theorem 4.1. *Let $k \in \mathbb{N}$ be even and let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The map*

$$\begin{aligned} w : \mathcal{A}_k(\Gamma) &\longrightarrow \Omega^{\otimes k/2}(X(\Gamma)) \\ f &\longmapsto (\omega_j)_{j \in J} \end{aligned}$$

where $(w_j)_{j \in J}$ pulls back to $f(\tau)(d\tau)^{k/2} \in \Omega^{\otimes k/2}(\mathbb{H})$, is an isomorphism of complex vector spaces.

Proof. The map ω is defined since we have just constructed $\omega(f)$. Clear ω is $\mathbb{C}$-linear and injective. And ω is surjective because every $(\omega_j) \in \Omega^{\otimes k/2}(X(\Gamma))$ pulls back to some $f(\tau)(d\tau)^{k/2} \in \Omega^{k/2}(\mathbb{H})$ with $f \in \mathcal{A}(\Gamma)$. □

For k positive and even, $\mathcal{A}_k(\Gamma)$ takes the form $\mathbb{C}(\mathbb{X}(\lneq))f$ where $\mathbb{C}(X(\Gamma))$ is the field of meromorphic functions on $X(\Gamma)$ and f is any nonzero element of $\mathcal{A}_k(\Gamma)$.

$$\mathcal{A}_k(\Gamma) = \mathbb{C}(X(\Gamma))f = \{f_0 f : f_0 \in \mathbb{C}(X(\Gamma))\}$$

Now we focus on the specific case, the weight 2 cusp forms $\mathcal{S}_2(\Gamma)$ are isomorphism as a complex vector space to the degree 1 holomorphic differentials on $X(\Gamma)$, denoted $\Omega^1_{hol}(X(\Gamma))$.

5 Elliptic Curves

5.1 Elliptic curves in arbitrary characteristic

Definition 5.1. Let $\bar{\mathbf{k}}$ be an algebraic closure of the field $\mathbf{k}$. When a Weierstrass equation E has nonzero discriminant Δ it is called nonsingular and the set

$$E = \{(x, y) \in \bar{\mathbf{k}}^2 \text{ satisfying } E(x, y)\} \cup \{\infty\}$$

is called an elliptic curve over $\mathbf{k}$.

Definition 5.2. For any algebraic extension $\mathbf{K}/\mathbf{k}$ the set of $\mathbf{K}$-points of E is a subgroup of E,

$$E(\mathbf{K}) = \{P \in E - \{0_E\} : (x_P, y_P) \in \mathbf{K}^2\} \cup \{0_E\}$$

Let N be a positive integer. The structure theorem for the N-torsion subgroup $E[N] = ker([N])$ of an elliptic is

Theorem 5.1. *Let E be an elliptic curve over $\mathbf{k}$ and let N be a positive integer. Then*

$$E[N] \cong \prod E[p^{e_p}] \text{ where } N = \prod p^{e_p}$$

Also,

$$E[p^e] \cong (\mathbb{Z}/p^e\mathbb{Z})^2 \text{ if } p \neq \text{char}(\mathbf{k})$$

Thus $E[N] \cong (\mathbb{Z}/p^e\mathbb{Z})^2$ if $\text{char}(\mathbf{k}) \nmid N$. On the other hand, if $p \nmid= \text{char}(\mathbf{k})$, $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ or $E[p^e] = \{0\}$ for all $e \geqslant 1$.

In particular, if $\text{char}(\mathbf{k}) = p$ then either $E[p] \cong \mathbb{Z}/p\mathbb{Z}$, in which case E is called ordinary, or $E[p] = \{0\}$ and E is supersingular.

Proposition 5.1. *Let E be a Weierstrass equation over $\mathbf{k}$. Then*
(a) E describes an elliptic curve $\iff \Delta \neq 0$,
(b) E describes a curve with a node $\iff \Delta = 0$ and $c_4 \neq 0$,
(c) E describes a curve with a cusp $\iff \Delta = 0$ and $c_4 = 0$.

5.2 The reduction of elliptic curves over $\mathbb{Q}$

In this part, we will discuss reduction of elliptic curves over $\mathbb{Q}$ modulo a prime p. Consider a general Weierstrass equation E defined over $\mathbb{Q}$,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_1, \ldots, a_6 \in \mathbb{Q}$$

and consider admissible changes of variable over $\mathbb{Q}$. In particular the change of variable $(x, y) = (u^2x', u^3y')$ gives a Weierstrass equation E' with coefficients $a_i' = a_i/u^i$.

For any prime p and any nonzero rational number r let $\nu_p(r)$ denote the power of p appearing in r, i.e., $\nu_p(p^e \cdot m/n) = e \in \mathbb{Z}$ where $p \nmid mn$. Also define $\nu_p(0) = +\infty$. This is the p-adic valuation, we have the following properties:

$$\nu_p(rr') = \nu_p(r)\nu_p(r')$$
$$\nu_p(r + r') \geqslant \min\{\nu_p(r), \nu_p(r')\} \text{ with equality if } \nu_p(r) \neq \nu_p(r'),$$

but occurring now in the context of number fields rather than function fields. For each prime p let $\nu_p(E)$ denote the smallest power of p appearing in the discriminant of any integral Weierstrass equation equiavlent to E, the minimum of a set of nonnegative integers,

$$\nu_p(E) = \min\{\nu_p(\Delta(E')) : E' \text{integral, equivalent to } E\}.$$

Definition 5.3. Define the global minimal discriminant of E to be

$$\Delta_{\min}(E) = \prod_p p^{\nu_p(E)}.$$

This is a fintie product since $\nu_p(E) = 0$ for all $p \nmid \Delta(E)$. E is isomorphic over $\mathbb{Q}$ to an integral model E' with discriminant $\Delta(E') = \Delta_{\min}(E)$. This is the global minimal Weierstrass equation E', the model of E to reduce modulo primes. From now on we freely assume when convenient that elliptic curves over $\mathbb{Q}$ are given in this form.

The field $\mathbb{F}_p$ of p elements can be viewed as $\mathbb{Z}/p\mathbb{Z}$. That is, $\mathbb{F}_p$ is the image of a surjective homomorphism from the ring of rational integer$\mathbb{Z}$, reduction modulo $p\mathbb{Z}$,

$$\tilde{}: \mathbb{Z} \longrightarrow \mathbb{F}_p, \quad \tilde{n} = n + p\mathbb{Z}$$

This map reduces a global minimal Weierstrass equation E to a Weierstrass equation $\tilde{E}$ over $\mathbb{F}_p$, and this defines an elliptic curve over $\mathbb{F}_p$ if and only if $p \nmid \Delta_{\min}(E)$. The reduction of E modulo p (also called the reduction of E at p) is

Definition 5.4. 1. The reduction of E is called *good [nonsingular, stable]* if $\tilde{E}$ is again an elliptic curve,
(a) *ordinary* if $\tilde{E}[p] \cong p\mathbb{Z}$
(b) *supersingular* if $\tilde{E} = \{0\}$
2. The reduction of E is called *bad [singular]* if $\tilde{E}$ is not an elliptic curve, in which case it has only one singular point,
(a) *multiplicative [semistable]* if $\tilde{E}$ has a node,
(b) *additive [unstable]* if $\tilde{E}$ has a cusp.

Putting E into global minimal form provides an almost complete description of a related integer N_E called the algebraic conductor of E. The global minimal discriminant and the algebraic conductor are divisible by the same primes,

$$p \nmid \Delta_{\min}(E) \Longleftrightarrow p \nmid N_E,$$

so that E has good reduction at all primes p not dividing N_E. More specifically, the algebraic conductor takes the form $N_E = \prod_p p^{f_p}$ where

$$f_p = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p, \\ 1 & \text{if } E \text{ has multiplicative reduction at } p, \\ 2 & \text{if } E \text{ has additive reduction at } p \text{ and } p \notin \{2,3\}, \\ 2+\delta_p & \text{if } E \text{ has additive reduction at } p \text{ and } p \in \{2,3\}. \end{cases}$$

Here $\delta_2 \leqslant 6$ and $\delta_3 \leqslant 3$.

We have already discuss the reduction of a Weierstrass equation E over $\mathbb{Q}$ to $\tilde{E}$ over $\mathbb{F}_p$, we have not yet discussed reducing the points of the curve $\tilde{E}$. This will be done in the next subsection.

Definition 5.5. Let E be an elliptic curve over $\mathbb{Q}$. Assume E is in reduced form. Let p be a prime and let $\tilde{E}$ be the reduction of E modulo p. Then

$$a_p(E) = p + 1 - |\tilde{E}(\mathbb{F}_p)|.$$

Proposition 5.2. *Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime such that E has good reduction modulo p. Let $\varphi_{p,*}$ and φ_p^* be the forward and reverse maps of* $\mathrm{Pic}^0(\tilde{E})$ *induced by φ_p. Then*

$$a_p(E) = \varphi_{p,*} + \varphi_p^* \text{ as endomorphisms of } \mathrm{Pic}^0(\tilde{E}).$$

Proposition 5.3. *Let E be an elliptic curve over $\mathbb{Q}$, and let p be a prime such that E has good reduction at p. Then the reduction is*

$$\begin{cases} \textit{ordinary} & \textit{if } a_p(E) \not\equiv 0 (\mathrm{mod}\ p), \\ \textit{supersingular} & \textit{if } a_p(E) \equiv 0 (\mathrm{mod}\ p). \end{cases}$$

5.3 Reduction of the points on Elliptic curves

So far we have reduced a Weierstrass equation, but not the points themselves of the elliptic curve. To reduce the points, we first show more generally that for any positive integer n the maximal ideal $\mathfrak{p}$ determines a reduction map

$$\tilde{}: \mathbf{P}^n(\overline{\mathbb{Q}}) \longrightarrow \mathbf{P}^n(\overline{\mathbb{F}_p})$$

Proposition 5.4. *Let E be an elliptic curve over $\overline{\mathbb{Q}}$ with good reduction at $\mathfrak{p}$. Then:*

(a) The reduction maps on N-torsion,

$$E[N] \longrightarrow \tilde{E}[N],$$

is surjective for all N.

(b) Any isogenous E/C where C is a cyclic subgroup of order p also has good reduction at $\mathfrak{p}$. Furthermore, if E has ordinary reduction at $\mathfrak{p}$ then so does E/C, and if E has supersingular reduction at $\mathfrak{p}$ then so does E/C.

5.4 Reduction of algebraic curves and maps

Theorem 5.2. *Let C be a nonsingular projective algebraic curve over $\mathbb{Q}$ with good reduction at p. Then the reduction map $C \longrightarrow \widetilde{C}$ is surjective.*

Theorem 5.3. *Let C and C' be nonsingular projective algebraic curves over $\mathbb{Q}$ with good reduction at p, and let C' have positive genus. For any morphism $h : C \longrightarrow C'$ the following diagram commutes:*

$$\begin{array}{ccc} C & \xrightarrow{h} & C' \\ \downarrow & & \downarrow \\ \widetilde{C} & \xrightarrow{\tilde{h}} & \widetilde{C'} \end{array}$$

Also, $\deg(\tilde{h}) = \deg(h)$.

Corollary 5.4. *Let C' have positive genus. Then*

(a) If $h : C \longrightarrow C'$ surjects then so does $\tilde{h} : \widetilde{C} \longrightarrow \widetilde{C'}$.

(b) If also $k : C' \longrightarrow C''$ and C'' has positive genus then

$$\widetilde{k \circ h} = \tilde{k} \circ \tilde{h}.$$

(c) If h is an isomorphism then so is $\tilde{h}$.

Theorem 5.5. *Let C be a nonsingular projective algebraic curve over $\mathbb{Q}$ with good reduction at p. The map on degree-0 divisors induced by reduction,*

$$\mathrm{Div}^0(C) \longrightarrow \mathrm{Div}^0(\widetilde{C}), \qquad \sum n_P(P) \mapsto \sum n_P(\widetilde{P}).$$

sends principal divisors to principal divisors and therefore further induces a surjection of Picard groups,

$$\mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}^0(\widetilde{C}), \qquad [\sum n_P(P)] \mapsto [\sum n_P(\widetilde{P})].$$

Let C' also be a nonsingular projective algebraic curve over $\mathbb{Q}$ with good reduction at p, and let C' have positive genus. Let $h : C \longrightarrow C'$ be a morphism over $\mathbb{Q}$, and let $h_* : \mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}^0(C')$ and $\tilde{h}_* : \mathrm{Pic}^0(\widetilde{C}) \longrightarrow \mathrm{Pic}(\widetilde{C'})$ be the induced forward maps of h and h. Then the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Pic}^0(C) & \xrightarrow{h_*} & \mathrm{Pic}^0(C') \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{C}) & \xrightarrow{\tilde{h}_*} & \mathrm{Pic}^0(\widetilde{C'}) \end{array}$$

Theorem 5.6. *Let*

$$\varphi : E \longrightarrow E'$$

be an isogeny over $\overline{\mathbb{Q}}$ of elliptic curves over $\overline{\mathbb{Q}}$. Then there is a reduction

$$\tilde{\varphi} : \widetilde{E} \longrightarrow \widetilde{E'}$$

with the properties

(a) $\tilde{\varphi}$ is an isogeny.

(b) If $\psi : E' \longrightarrow E''$ is also an isogeny then $\widetilde{\psi \circ \varphi} = \tilde{\psi} \circ \tilde{\varphi}$.

(c) The following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\tilde{\varphi}} & \widetilde{E'} \end{array}$$

(d) $\deg(\tilde{\varphi}) = \deg(\varphi)$

5.5 Igusa's Theorem

Let $\mathfrak{p}$ be a maximal ideal of $\overline{\mathbb{Q}}$ lying over p. An elliptic curve E over $\overline{\mathbb{Q}}$ with good reduction at $\mathfrak{p}$ has $j(E) \in \overline{\mathbb{Z}}_{(\mathfrak{p})}$, so this reduces at $\mathfrak{p}$ to $\widetilde{j(E)}$ in $\overline{\mathbb{F}}_p$. We avoid $j = 0, 1728$ in the image. Denote this with a prime in the notation i.e., the suitable restriction of the moduli space $\mathrm{S}_1(N)$ over $\mathbb{Q}$ is

$$\mathrm{S}_1(N)'_{\mathrm{gd}} = \{[E, Q] \in \mathrm{S}_1(N) : E \text{has good reduction at } \mathfrak{p},\ \widetilde{j(E)} \notin \{0, 1728\}\}$$

In characteristic p, let $\widetilde{\mathrm{S}}_1(N)$ denote the moduli space over $\overline{\mathbb{F}}_p$, i,e., it consists of equivalence classes $[E, Q]$ where E is an elliptic curve over $\overline{\mathbb{F}}_p$ and $Q \in E$ is a point of order N and the equivalence relatio is isomorphism over $\overline{\mathbb{F}}_p$. Again avoid $j = 0, 1728$ by defining

$$\widetilde{\mathrm{S}}(N)' = \{[E, Q] \in \widetilde{\mathrm{S}}_1(N) : j(E) \notin \{0, 1728\}\}$$

The resulting reduction map is

$$\mathrm{S}_1(N)'_{\mathrm{gd}} \longrightarrow \widetilde{\mathrm{S}}(N)', \qquad [E_j, Q] \mapsto [\widetilde{E}_j, \widetilde{Q}].$$

This is a surjection.

Let $\sigma_{1,N} \in \mathbb{F}_p(j)[x]$ be the minimal polynomial of x-coordinate $x(Q)$. Define a field

$$\mathbf{K}_1(N) = \mathbb{F}_p(j)[x] / \langle \sigma_{1,N} \rangle$$

We have the result that $\mathbf{K}_1(N) \cap \overline{\mathbb{F}}_p = \mathbb{F}_p$, so $\mathbf{K}_1(N)$ is a function field over $\mathbb{F}_p$.

Theorem 5.7 (Igusa' Theorem)**.** *Let N be a positive integer and let p be a prime with $p \nmid N$. The modular curve $X_1(N)$ has good reduction at p. There is an isomorphism of functions fields*

$$\mathbb{F}_p(\widetilde{X}_1(N)) \longrightarrow \mathbf{K}_1(N).$$

Moreover, reducing the modular curve is compatible with reducing the moduli space in that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{S}_1(N)'_{\mathrm{gd}} & \xrightarrow{\psi_1} & X_1(N) \\ \downarrow & & \downarrow \\ \widetilde{\mathrm{S}}_1(N)' & \xrightarrow{\tilde{\psi}_1} & \widetilde{X}_1(N). \end{array}$$

Here the top row is the map $[E_j, Q] \mapsto (j, x(Q))$ to the planar model followed by the birational equivalence to $X_1(N)$, and similarly for the bottom row but in characteristic p.

The diagram extends to divisor groups, restricts to degree 0 divisors, and takes principal divisors to principal divisors, giving a modified diagram as below:

$$\begin{array}{ccc} \mathrm{Div}^0(\mathrm{S}_1(N)'_{\mathrm{gd}}) & \longrightarrow & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Div}^0(\widetilde{\mathrm{S}}(N)') & \longrightarrow & \mathrm{Pic}^0(\widetilde{X}_1(N)) \end{array} \tag{1}$$

6 Statement of the main theorem

Theorem 6.1 (Eichler-Shimura)**.** *Let $f = \sum c(n)q^n$ be a normalized newform on $\Gamma_0(N)$. If all $c(n) \in \mathbb{Z}$, then exist an elliptic curve E_f of conductor N such that $L(E_f, s) = L(f, s)$*

First, we want to know how to get a elliptic curve from a cusp form, then we consider the relation between L-function of cusp form and elliptic curve.

7 Get an Elliptic curve from a cusp form

A differential one-form on an open subset of $\mathbb{C}$ is simply an expression $\omega = f dz$, with f a meromorphic function. Given a smooth Given a smooth curve γ

$$t \mapsto z(t) : [a, b] \to \mathbb{C},\ [a, b] = \{t \in \mathbb{R} | a \leqslant t \leqslant b\}$$

we can form the integral $\int_\gamma \omega = \int_a^b f(z(t)) \cdot z'(t) \cdot dt \in \mathbb{C}$ Now consider a compact Riemann surface X. If ω is a differential one-form on x and (U_i, z_i) is a coordinate neighbourhood for X, then $\omega | U_i = f_i(z_i) dz_i$. If (U_j, z_j) is a second coordinate neighbourhood, so that $z_j = w(z_j)$ on $U_i \cap U_j$, then

$$f_i(z_i) dz_i = f_j(w(z_i)) w'(z_i) dz_i$$

on $U_i \cap U_j$. Thus, to give a differential one-form on X is to give differential one-forms $f_i dz_i$ on each U_i, satisfying the above equation on the overlaps. For any (real) curve $\gamma : I \to X$ and differential one-form ω on X, the integral $\int_\gamma \omega$ make sense.

Definition 7.1. A differential one-form is holomorphic if it is represented on the coordinated neighbourhoods by forms $f dz$ with f holomorphic.

7.1 Jacobian variety of a Riemann surface

Consider a Riemann surface with genus 1 and a nonzero holomorphic differential one-form ω. We choose a point $P_0 \in X$ and try to define a map

$$P \mapsto \int_{P_o}^{P} \omega : X \to \mathbb{C}$$

This is not well-defined because the value of the integral depends on the path we choose from P_0 to P −− nonhomotopic paths may give different answers. From the result in the Algebraic Topology, if we choose a basis $\{\gamma_1, \gamma_2\}$ for $H_1(X, \mathbb{Z})$ (equivalently, a basis for $\pi_1(X, P_0)$), then the integral is well-defined modulo the lattice Λ in $\mathbb{C}$ generated by

$$\int_{\gamma_1} \omega, \int_{\gamma_2} \omega.$$

In this way, we obtain an isomorphism

$$P \mapsto \int_{P_0}^{P} \omega : X \to \mathbb{C}/\Lambda$$

Jacobi and Abel made a similar construction for any compact Riemann surface X. It is an important fact that the holomorphic differential one-form on a Riemann surface of genus g form a complex vector space $\Omega^1(X)$ of dimension g. Now we suppose that X is a Riemann sufrce with genus g, and let $\omega_1, \ldots, \omega_g$ be a basis for the vector space $\Omega^1(X)$ of holomorphic one-forms on X. Choose a point $P_0 \in X$. Viewing X as a sphere with g handles where g is the genus of X, let $A_1, \ldots, A_g$ be longitudinal loops around each handle like arm-bands, and let $B_1, \ldots, B_g$ be latitudinal loops arod each handle like equators.Then consider the (first) homology group of X,

$$H_1(X, \mathbb{Z}) = \mathbb{Z} \int_{A_1} \oplus \cdots \oplus \mathbb{Z} \int_{A_g} \oplus \mathbb{Z} \int_{B_1} \oplus \cdots \oplus \mathbb{Z} \int_{B_g} \cong \mathbb{Z}^{2g}$$

Similarily, there is a map

$$P \mapsto (\int_{P_0}^{P} \omega_1, \ldots, \int_{P_0}^{P} \omega_g) : X \to \mathbb{C}^g/\Lambda$$

is well-defined. The quotient $\mathbb{C}^g/\Lambda$ is a comples manifold, called the jacobian variety $\mathrm{Jac}(X)$ of X, which can be considered to be a higher-dimensional analogue of $\mathbb{C}/\Lambda$. Note that it is a commutative group.

We can define $\mathrm{Jac}(X)$ more canonically. Let $\Omega^1(X)^\vee$ be the dual of $\Omega^1(X)$ as a complex vector space. For any $\gamma \in H_1(X, \mathbb{Z})$,

$$\omega \mapsto \int_{\gamma} \omega$$

is an element of $\Omega^1(X)^\vee$, and in this way we obtain an injective homomorphism

$$H_1(X, \mathbb{Z}) \hookrightarrow \Omega^1(X)^\vee$$

which identifies $H_1(X, \mathbb{Z})$ with a lattice in $\Omega^1(X)^\vee$. Define

$$\mathrm{Jac}(X) = \Omega^1(X)^\vee / H_1(X, \mathbb{Z}).$$

When we fix a point $P_0 \in X$, any $P \in X$ defines an element F_P of $\mathrm{Jac}(X)$,

$$F_P : \omega \mapsto \int_{P_0}^{P} \omega \ \ mod\ H_1(X, \mathbb{Z})$$

and so we get a map $X \to \mathrm{Jac}(X)$. The choice of a different P_0 gives a map that differs from the first only by a translation.

Now we apply above theory to the Riemann surface $X_0(N)$. We have known that $X_0(N)$ is a Riemann surface with genus 1.

Proposition 7.1. *Let π be the quotient map $\mathbb{H}^* \to \Gamma_0(N) \setminus \mathbb{H}^*$, and for any holomorphic differential ω on $\Gamma_0(N) \setminus \mathbb{H}^*$, set $\pi^*\omega = f dz$. Then $\omega \mapsto f$ is an isomorphism from the space of holomorphic differentials on $\Gamma_0(N) \setminus \mathbb{H}^*$ to $\mathcal{S}_2(\Gamma_0(N))$.*

By the above Proposition we get an isomorphism $\mathcal{S}_\epsilon(\Gamma_0(N)) \cong \Omega^1(X_0(N))$. The Hecke operator $T(n)$ acts on $\mathcal{S}_2(\Gamma_0(N))$, and hence on the vector space $\Omega^1(X_0(N))$ and its dual. Moreover, the Hecke operator acts on $\mathrm{Jac}(X)$.

Proposition 7.2. *There is a canonical action of $T(n)$ on $H_1(X_0(N), \mathbb{Z})$, which is compatible with the map $H_1(X_0(N), \mathbb{Z}) \to \Omega^1(X_0(N))^\vee$. In other words, the action of $T(n)$ on $\Omega^1(X_0(N))^\vee$ stabilizes its sublattice $H_1(X_0(N), \mathbb{Z})$, and therefore induces an action on the quetient* $\mathrm{Jac}(X_0(N))$.

Now let $f = \sum c(n)q^n$ be a normalized newform for $\Gamma_0(N)$ with $c(n) \in \mathbb{Z}$. The map

$$\alpha \mapsto \alpha(f) : \Omega^1(X_0(N))^\vee \to \mathbb{C}$$

identifies $\mathbb{C}$ with the largest quotient of $\Omega^1(X_0(N))^\vee$ on which each $T(n)$ acts as multiplication by $c(n)$. The image of $H_1(X_0(N, \mathbb{Z}))$ is a lattice Λ_f, and we set $E_f = \mathbb{C}/\Lambda_f$ −− it is an elliptic curve over $\mathbb{C}$. Note that have constructed maps

$$X_0(N) \to \mathrm{Jac}(X_0(N)) \to E_f$$

Moreover, the inverse image of the differential on E_f represented by dz is the differential on $X_0(N)$ represented by $f dz$.

Theorem 7.1. *Let $f = \sum c(n)q^n$ be a newform in $\mathcal{S}(\Gamma_0(N))$, normalized to have $c(1) = 1$, and assume that all $c(n) \in \mathbb{Z}$. Then there exists an elliptic curve E_f and a map $\alpha : X_0(N) \to E_f$ with the following properties:*

(a) α factors uniquely through $\mathrm{Jac}(X_0(N))$,

$$X_0(N) \to \mathrm{Jac}(X_0(N)) \to E_f,$$

and the second map realizes E_f as the largest quotient of $\mathrm{Jac}(X_0(N))$ *on which the endomorphism $T(n)$ and $c(n)$ of* $\mathrm{Jac}(X_0(N))$ *agree.*

(b) The inverse image of an invariant differential ω on E_f under $\mathbb{H} \to X_0(N) \to E_f$ is a nonzero rational multiple of $f dz$.

8 The relation between the L-Series of E_f and the L-Series of f

8.1 The Hecke correspondence

Definition 8.1. Let X and X' be projective nonsingular curves over a algebraically closed field k. A correspondence T between X and X' is a pair of finite surjective regular maps, denoted $T : X \vdash X'$

$$X \xleftarrow{\alpha} Y \xrightarrow{\beta} X'$$

A correspondence T can be viewed as a many-valued map $X \to X'$ sending a point $P \in X(k)$ to the set $\{\beta(Q_i)|Q_i \in \alpha^{-1}(P)\}$ As we defined before, Div(X) is the free Abelian group on the points of X, so the element of Div(X) is a finite sum

$$D = \sum n_P[P],\ n_p \in \mathbb{Z},\ P \in X(k)$$

Therefore, a correspondence T then induces a map between $T : \mathrm{Div(X)} \to \mathrm{Div(X')}$

$$[P] \mapsto \sum_i [\beta(Q_i)]$$

This map multiplies the degree of a divisor by $\deg(\alpha)$. It therefore sends the divisors of degree 0 in Div(X) to the divisors of degree 0 in Div(X′) and sends the principal divisors of Div(X) to the principal divisors of Div(X′). Define $J(X) := \mathrm{Div}^0(\mathrm{X})/\mathrm{principaldivisors}$. Then a correspondence T induces a map $T : J(X) \to J(X')$.

Definition 8.2. Let T is a correspondence

$$X \xleftarrow{\alpha} Y \xrightarrow{\beta} X$$

then the transpose T^{tr} of T is the correspondence

$$X \xleftarrow{\beta} Y \xrightarrow{\alpha} X$$

Let T is a correspondence $T : X \vdash X'$

$$X \xleftarrow{\alpha} Y \xrightarrow{\beta} X'$$

For any regular function f on X', we define $T(f)$ to be the regular function on X, $T(f) : P \mapsto \sum f(\beta Q_i)$. So T induces a homomorphism $\Omega^1 \to \Omega^1(X)$. Now we use above theory on the modular curve $Y_0(N)$.

Definition 8.3. Let $p \nmid N$, the Hecke correspondence $T(p) : Y_0(N) \to Y_0(N)$ is defined below

$$Y_0(N) \xleftarrow{\alpha} Y_0(pN) \xrightarrow{\beta} Y_(N)$$

where α is the projection map and β is the map induced by $z \mapsto pz : \mathbb{H} \to \mathbb{H}$

First, we consider the point in $Y_0(N)$. As we discuss before, a point of $Y_0(pN)$ is represented by a pair of (E, S) where E is an elliptic curve and S is a cyclic subgroup of E of order pN. Because $p \nmid N$, any subgroup S of order pN can be decomposes uniquely into subgroups of N and p, $S = S_N \times S_p$. The map α sends the point represented by (E, S) to the point represented by (E, S_N) and β sends (E, S) to the point represented by $(E/S_p, S/S_p)$. Recall that E_p has $p + 1$ cyclic subgroups, the correspondence is $1 : p + 1$.

The unique extension of $T(p)$ to a correspondence $X_0(N) \to X_0(N)$ acts on $\Omega^1(X_0(N)) = \mathcal{S}_2(\Gamma_0(N))$

8.2 The Frobenius map

Let C be a curve defined over the algebraic closure $\mathbb{F}^{al}$ of $\mathbb{F}_p$. If C defined by equations

$$\sum a_{i_0 i_1 \cdots} X_0^{i_0} X_1^{i_1} \cdots = 0$$

then we let $C^{(p)}$ be the curve defined by the equations

$$\sum a^p_{i_0 i_1 \cdots} X_0^{i_0} X_1^{i_1} \cdots = 0$$

and we let the Frobenius map $\varphi : C \to C(p)$ send the point $(b_0 : b_1 : b_2 : \cdots)$ to $(b_0^p : b_1^p : b_2^p : \cdots)$. If C is defined over $\mathbb{F}_p$, then $C = C^{(p)}$ and φ_p is the Frobenius map defined earlier.

Recall a result from the field extension.

Proposition 8.1. *Let K be a field extension of F. If S and I are the separable and purely inseparable closures of F in K, respectively, then S and I are field extension of F with S/F separable, I/F purely inseparable, and $S \cup I = F$. If K/F s algebraic, then K/F is purely inseparable.*

Recall that a nonconstant morphism $\alpha : C \to C'$ of curves defines an inclusion $\alpha^* : k(C') \hookrightarrow k(C)$ of function fields, and that the degree of α is defined to be $[k(C) : \alpha^* k(C')]$. The map α is said to be separable or purely inseparable according as $k(C)$ is a separable or purely inseparable extension of $\alpha^* k(C')$. If the separable degree of $k(C)$ over $\alpha^* k(C')$ is m, then the map $C(k^{al}) \to C'(k^{al})$ is $m : 1$, except over the finite set where it is ramified.

Proposition 8.2. *The Frobenius map $\varphi_p : C \to C^{(p)}$ is purely inseparable of degree p, and any purely inseparable map $\varphi : C \to C'$ of degree p (of complete nonsingular curves) factors as*

$$C \xrightarrow{\varphi_p} C^{(p)} \xrightarrow{\approx} C'$$

8.3 The Eichler-Shimura relation

For almost all primes $p \nmid N$, $X_0(N)$ will reduce to a nonsingular curve $\tilde{X}_0(N)$. In fact, it is known that $X_0(N)$ has a good reduction for all primes $p \nmid N$, but this is hard to prove. It is easy to see that $X_0(N)$ does not have good reduction at primes dividing N.

Theorem 8.1. *For a prime p where $X_0(N)$ has good reduction,*

$$\tilde{T}(p) = \varphi_p + \varphi_p^{tr}$$

Proof. We sketch a proof that they agree as many-valued maps on an open subset of $\tilde{X}_0(N)$. We will state another proof by using the commutative diagram.

As we discuss above, there is a isomorphism between $\psi_0 : \mathrm{S}_0(N) \xrightarrow{\sim} Y_0(N)$, where

$$\mathrm{S}_0(N) = \{\text{enhanced elliptic curves for } \Gamma_0(N)\}/\sim$$

Over $\mathbb{Q}_p^{\mathrm{al}}$ we have the following description of $T(p)$: a point P on $Y_0(N)$ is represented by a homomorphism of elliptic curves $\alpha : E \to E'$ with cyclic kernel of order N; let $S_0, \ldots, S_p$ be the subgroups of order p in E; then $T_p(P) = \{Q_0, \ldots, Q_p\}$ where Q_i is represented by $E/S_i \to E'/\alpha(S_i)$.

Consider a point $\tilde{P}$ on $\tilde{X}_0(N)$ with coordinates in $\mathbb{F}$ - by Hensel's lemma it will lift to a point on $X_0(N)$ with coordinates in $\mathbb{Q}_p^{\mathrm{al}}$. Ignoring a finite number of points of $\tilde{X}_0(N)$, we can suppose $\tilde{P} \in \tilde{Y}_0(N)$ and hence is represented by a map $\tilde{\alpha} : \tilde{E} \to \tilde{E}'$ where $\alpha : E \to E'$ has cyclic kernel of order N. By ignoring a further finite number of points, we may suppose that $\tilde{E}$ has p points of order dividing p.

Let $\alpha : E \to E'$ be a lifting of $\tilde{\alpha}$ to $\mathbb{Q}_p^{\mathrm{al}}$. The reduction map $E_p(\mathbb{Q}_p^{\mathrm{al}}) \to \tilde{E}_p(\mathbb{F}_p^{\mathrm{al}})$ has a kernel of order p. Renumber the subgroups of order p in E so that S_0 is the kernel of this map. Then each $S_i, i \neq 0$, maps to subgroup of order p in $\tilde{E}$.

Then map $\tilde{T}(p) : \tilde{E} \to \tilde{E}$ has factorizations

$$\tilde{E} \xrightarrow{\varphi} \tilde{E}/S_i \xrightarrow{\psi} \tilde{E},\ i = 0, 1, \ldots, p.$$

When $i = 0$, φ is a purely inseparable map of degree p (it is the reduction of the map $E \to E/S_0$ - it therefore has degree p and has zero kernel), and so ψ must be separable of degree p (we are assuming $\tilde{E}$ has p points of order dividing p). By Proposition 8.2 shows that there is an isomorphism $\tilde{E}^{(p)} \to \tilde{E}/S_0$. Similarily $\tilde{E}'^{(p)} \approx \tilde{E}'/S_0$. Therefore Q_0 is represented by $\tilde{E}^{(p)} \to \tilde{E}'^{(p)}$, which also represents $\varphi_p(P)$.

When $i \neq 0$, φ is separable (its kernel is the reduction of S_i), and so ψ is purely inseparable. Therefore $\tilde{E} \approx \tilde{E}_i^{(p)}$, and similarly $\tilde{E}' \approx \tilde{E}_i'^{(p)}$, where $\tilde{E}_i = \tilde{E}/S_i$ and $\tilde{E}_i' = \tilde{E}'/S_i$ It follows that $\{Q_1, \ldots, Q_p\} = \varphi^{-1}(P) = \varphi^{\mathrm{tr}}(P)$.

□

8.4 The zeta function of an elliptic curve

For an Elliptic curve $E = \mathbb{C}/\Lambda$ over $\mathbb{C}$, the degree of a nonzero endomorphism of E is the determinant of α acting on Λ. More generally, for an elliptic curve E over an algebraically closed field $\mathbf{k}$, and l be a prime not equal to the characteristic of $\mathbf{k}$,

$$\deg(\alpha) = \det(\alpha | T_l E)$$

where $T_l E$ is the Tate module $T_l E = \lim_{\leftarrow} E(\mathbf{k})_{l^n}$ of E.

Proposition 8.3. *Let E be an elliptic curve over $\mathbb{F}_p$. Then the trace of the Frobenius endomorphism φ_p on $T_l E$ has the following formula*

$$\mathrm{Tr}(\varphi_p | T_l E) = a_p := p + 1 - N_p.$$

Corollary 8.2. *Let E be an elliptic curve over $\mathbb{F}_p$. Then*

$$\mathrm{Tr}(\varphi_p^{tr} | T_l E) = \mathrm{Tr}(\varphi_p | T_l E).$$

8.5 The action of the Hecke operators on $H_1(E, \mathbb{Z})$

Corollary 8.3. *For any $p \nmid N$,* $\mathrm{Tr}(T(p) | H_1(X_0(N), \mathbb{Z})) = \mathrm{Tr}(T(p) | \Omega^1(X_0(N))) + \overline{\mathrm{Tr}(T(p) | \Omega^1(X_0(N)))}$

Proof. The proof of above Proposition and Corollary is straightforward calculation on [4], which we will skip. □

Theorem 8.4. *Consider an $f = \sum c(n) q^n$ and a map $X_0(N) \to E$, as in Theorem 7.1. For all $p \nmid N$,*

$$c(p) = a_p := p + 1 - N_p$$

Proof. We assume initially that $X_0(N)$ has genus 1. Then $X_0(N) \longrightarrow E$ is an isogeny, and we can take $E = X_0(N)$. Let p be a prime not dividing N. Then E has good reduction at p, and for any $l \neq p$, the reduction map $T_l E \longrightarrow T_l \widetilde{E}$ is an isomorphism. The Eichler-Shimura Relation states that

$$\widetilde{T}(p) = \varphi_p + \varphi_p^{\mathrm{tr}}$$

We take trace on $T_l \widetilde{E}$. According to the Proposition 8.3, Corollary 8.2 and Corollary 8.3, we get the following result

$$c(p) = a_p := p + 1 - N_p$$

□

9 Another Proof of Eichler-Shimura Relation

We will proof the Eichler-Shimura Relation by using the commutative diagram, this proof is mainly come from [2].

9.1 Further discussion for Hecke operator

As we discuss above, there is a natural map between moduli space and modular curve,

$$\psi_1 : \mathrm{S}_1(N) \longrightarrow X_1(N), \qquad [\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] \mapsto \Gamma_1(N)\tau,$$

to divisor groups. To make ψ_1 algebraic, consider the following commutative diagram

$$\begin{array}{ccc} \mathrm{S}_1(N) & \longrightarrow & \mathrm{S}_1(1) \\ {\scriptstyle\psi_1}\downarrow & & \downarrow \\ X_1(N) & \longrightarrow & X_1(N) \end{array}$$

given by

$$\begin{array}{ccc} [\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] & \longrightarrow & [\mathbb{C}/\Lambda_\tau] \\ \downarrow & & \downarrow \\ \Gamma_1(N)\tau & \longrightarrow & \mathrm{SL}_2(\mathbb{Z})\tau \end{array}$$

As we discuss in Hecke operator, we have the following commutative diagram

$$\begin{array}{ccc} \mathrm{Div}(\mathrm{S}_1(N)) & \xrightarrow{T_p} & \mathrm{Div}(\mathrm{S}_1(N)) \\ {\scriptstyle\psi_1}\downarrow & & \downarrow{\scriptstyle\psi_1} \\ \mathrm{Div}(\mathrm{X}_1(\mathrm{N})) & \xrightarrow{T_p} & \mathrm{Div}(X_1(N)) \end{array}$$

The map $\psi_1 : \mathrm{S}_1(N) \longrightarrow Y_1(N)$ from the discussion on moduli space and modular curve. Now we restrict the vertical maps to degree-zero divisors and then the bottom row passes to Picard groups, giving a commutative diagram

$$\begin{array}{ccc} \mathrm{Div}^0(\mathrm{S}_1(N)) & \xrightarrow{T_p} & \mathrm{Div}^0(\mathrm{S}_1(N)) \\ {\scriptstyle\psi_1}\downarrow & & \downarrow{\scriptstyle\psi_1} \\ \mathrm{Pic}^0(X_1(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N)) \end{array} \tag{2}$$

9.2 Proof of Eichler-Shimura Relation

Let N be a positive integer and let $p \nmid N$ be prime. We will first give a description of the Hecke operator T_p at the level of Picard groups of reduced modular curves,

$$\widetilde{T_p} : \mathrm{Pic}^0(\widetilde{X}_1(N)) \longrightarrow \mathrm{Pic}^0(\widetilde{X}_1(N)).$$

By Theorem 5.5 the Hecke operator $\langle d\rangle$ on $X_1(N)$ reduces modulo p and passes to Picard groups to give a commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{\langle d\rangle_*} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\widetilde{\langle d\rangle}_*} & \mathrm{Pic}^0(\widetilde{X}_1(N)) \end{array} \tag{3}$$

We want a similar diagram for the Hecke operator T_p on $\mathrm{Pic}^0(X_1(N))$,

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\widetilde{T_p}} & \mathrm{Pic}^0(\widetilde{X}_1(N)) \end{array} \tag{4}$$

However, since the top row here is not the pushforward of a morphism from $X_1(N)$ to $X_1(N)$, Theorem 5.5 doesn't give this diagram as it gives Equation 3. The way to compute the reduction $\widetilde{T_p}$ on $\mathrm{Pic}^0(\widetilde{X}_1(N))$ is to compute it first in the moduli space environment. We will establish a moduli sapce diagram analogous to Equation 4 and then use Igusa's Theorem to translate it to modular curves. Recall the moduli space interpretation of the Hecke operator T_p on the divisor group of $\mathrm{S}_1(N)$,

$$T_p[E, Q] = \sum_C [E/C, Q + C]. \tag{5}$$

The sum is taken over all order p subgroups $C \subset E$ such that $C \cap \langle Q \rangle = \{0\}$, in this case all order p subgroups since $p \nmid N$.

Let E be an elliptic curve over $\overline{\mathbb{Q}}$ with ordinary reduction at $\mathfrak{p}$ and let $Q \in E$ be a point of order N. Let C_0 be the kernel of the reduction map $E[p] \longrightarrow \widetilde{E}[p]$, an order p subgroup of E since the ma surjects and the reduction is ordinary.

Lemma 9.1. *For any order p subgroup C of E,*

$$[\widetilde{E/C}, \widetilde{Q + C}] = \begin{cases} [\widetilde{E}^{\varphi_p}, \widetilde{Q}^{\varphi_p}] & \text{if } C = C_0 \\ [\widetilde{E}^{\varphi_p^{-1}}, [p]\widetilde{Q}^{\varphi_p^{-1}}] & \text{if } C \neq C_0 \end{cases}$$

There are $p+1$ order p subgroups C of E, one of which is C_0. Define the moduli space diamond operator in characteristic p to be

$$\widetilde{\langle d \rangle} : \widetilde{\mathrm{S}}_1(N) \longrightarrow \widetilde{\mathrm{S}}_1(N), \qquad [E, Q] \mapsto [E, [d]Q], \quad (d, N) = 1.$$

Then summing the formula of above Lemma over all order p subgroups $C \subset E$ gives for a curve E with ordinary reduction at $\mathfrak{p}$,

$$\sum_C [\widetilde{E/C}, \widetilde{Q + C}] = (\varphi_p + p\widetilde{\langle p \rangle}\varphi_p^{-1})[\widetilde{E}, \widetilde{Q}]. \tag{6}$$

The above Lemma extends to supersingular curves. If E is an elliptic curve over $\overline{\mathbb{Q}}$ with supersingular reduction at $\mathfrak{p}$ and $Q \in E$ is a point of order N, then for any order p subgroup C of E

$$[\widetilde{E/C}, \widetilde{Q + C}] = [\widetilde{E}^{\varphi_p}, \widetilde{Q}^{\varphi_p}] = [\widetilde{E}^{\varphi_p^{-1}}, [p]\widetilde{Q}^{\varphi_p^{-1}}].$$

Summing this over the $p + 1$ such subgroups C of E, using the first expression for $[\widetilde{E/C}, \widetilde{Q + C}]$ once and the second expression p times, shows that formula 6 applies to curves with supersingular reduction at $\mathfrak{p}$ as well. Therefore it applies to all curves with good reduction at $\mathfrak{p}$.

If an elliptic curve $\widetilde{E}$ over $\overline{\mathbb{F}}_p$ has invariant $j \notin \{0, 1728\}$ then the same holds for $\widetilde{E}^{\varphi_p}$ and $\widetilde{E}^{\varphi_p^{-1}}$. Formulas 5 and 6 combine with this observation to give a commutative diagram, where as before the primes mean to avoid some points, only finitely many in characteristic p,

$$\begin{array}{ccc} \mathrm{S}_1(N)'_{\mathrm{gd}} & \xrightarrow{T_p} & \mathrm{Div}(\mathrm{S}_1(N)'_{\mathrm{gd}}) \\ \downarrow & & \downarrow \\ \widetilde{\mathrm{S}}_1(N)' & \xrightarrow{\varphi_p + p\widetilde{\langle p \rangle}\varphi_p^{-1}} & \mathrm{Div}(\widetilde{\mathrm{S}}_1(N)') \end{array}$$

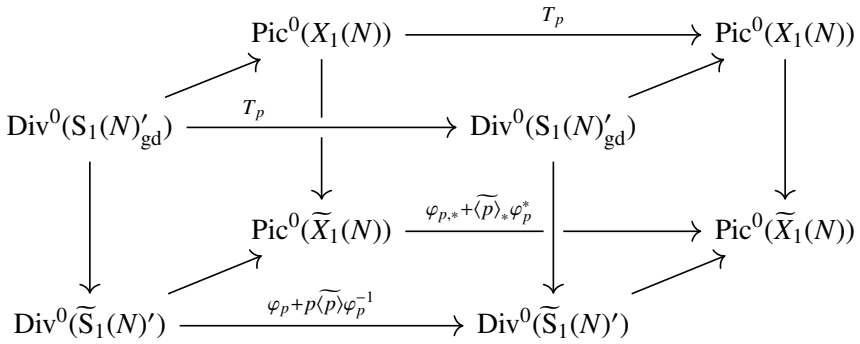
That is, T_p on $\mathrm{S}_1(N)'_{\mathrm{gd}}$ reduces at $\mathfrak{p}$ to $\varphi_p + p\widetilde{\langle p\rangle}\varphi_p^{-1}$. This extends to divisor groups and then restricts to degree-0 divisors,

$$\begin{array}{ccc} \mathrm{Div}^0(\mathrm{S}_1(N)'_{\mathrm{gd}}) & \xrightarrow{T_p} & \mathrm{Div}(\mathrm{S}_1(N)'_{\mathrm{gd}}) \\ \downarrow & & \downarrow \\ \mathrm{Div}^0(\widetilde{\mathrm{S}}_1(N)') & \xrightarrow{\varphi_p + p\widetilde{\langle p\rangle}\varphi_p^{-1}} & \mathrm{Div}(\widetilde{\mathrm{S}}_1(N)') \end{array} \tag{7}$$

We also have a commutative diagram

$$\begin{array}{ccc} \mathrm{Div}^0(\widetilde{\mathrm{S}}_1(N)') & \xrightarrow{\varphi_p + p\widetilde{\langle p\rangle}\varphi_p^{-1}} & \mathrm{Div}(\widetilde{\mathrm{S}}_1(N)') \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\varphi_{p,*} + \widetilde{\langle p\rangle}_*\varphi_p^*} & \mathrm{Pic}^0(\widetilde{X}_1(N)) \end{array} \tag{8}$$

A cube-shaped diagram now exist as follows, where all squares except possibly the back one commute.



To establish this, note that

(1) The top square, a diagram in characteristic 0 relating T_p on the moduli space and on the modular curve, is a restriction of commutative diagram 2

(2) The side squares, relating reduction at p to the map from the moduli space to the modular curve, are commutative diagram from 1 Igusa's Theorem.

(3) The front square, relating T_p on the moduli space to reduction at p, is commutative diagram 7 resulting from Lemma 9.1.

(4) The bottom square, relating maps in characteristic p on the moduli space and on the modular curve, is commutative diagram 8.

Therefore, the back square is commute. Moreover, the cube commute. We get the following result

Theorem 9.1 (Eichler-Shimura Relation)**.** *Let $p \nmid N$. The following diagram commutes:*

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\varphi_{p,*} + \widetilde{\langle p\rangle}_*\varphi_p^*} & \mathrm{Pic}^0(\widetilde{X}_1(N)) \end{array}$$

In particular since $\widetilde{\langle p \rangle}$ acts trivially on $\widetilde{X}_0(N)$, the following diagram commutes as well:

$$\begin{array}{ccc} \mathrm{Pic}^0(X_0(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_0(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_0(N)) & \xrightarrow{\varphi_{p,*}+\varphi_p^*} & \mathrm{Pic}^0(\widetilde{X}_0(N)) \end{array}$$

We main use the book [4] and [2] and [1]

Bibliography

[1] A. O. L. Atkin and J. Lehner. *Hecke operators on* $\Gamma_0(m)$. Math. Ann, 1970.

[2] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Vol. 228. Series Title Graduate Texts in Mathematics. Springer New York, NY, 2005.

[3] Anthony W. Knapp. *Elliptic Curves*. Princeton University Press, 1992.

[4] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.