DIFFERENT VERSIONS OF THE MODULARITY THEOREM

by

İlkiz Bildik

B.S., Mathematics, Boğaziçi University, 2014

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Mathematics
Boğaziçi University

2017

ACKNOWLEDGEMENTS

First I would like to express my exceptional gratitude to my thesis advisor Assoc. Prof. Ekin Özman, for her guidance and encouragement during my graduate education. She has been a great advisor for my thesis with her infinite energy, support and critical comments during this tough period. I would also like to thank Assoc. Prof. Ayhan Günaydın and Assist. Prof. Ayberk Zeytin for taking part in my jury.

I want to thank my great friends Fulya Taştan and Kübra Kaytancı for their endless support and encouragement, especially for the times we spent in the library. I could not have done this without their support. I would also thank Seza Eraydın and Ayşen Şansal for their help during my hard times. I would like to thank my best friend, Fatih. He was always there cheering me up and stood by me through all the time.

I would like to thank my family, Nurseven and Erkan for supporting me spiritually writing my thesis and my life in general.

I thankfully acknowledge TÜBİTAK for providing me with the scholarship during my studies.

ABSTRACT

DIFFERENT VERSIONS OF THE MODULARITY THEOREM

One of the most interesting results in number theory is the proof of the Modularity Theorem. The Modularity Theorem has many different versions. The geometric version states that there is a surjective morphism between elliptic curves and modular curves over the field of rational numbers. The arithmetic version states that there is a relation between elliptic curves over the field of rational numbers and modular forms. In this thesis, we will give an outline of a proof of the fact that the geometric version of the Modularity Theorem implies the arithmetic version.

ÖZET

MODÜLERLİK TEOREMİNİN FARKLI VERSİYONLARI

Sayılar teorisindeki en ilgi çekici sonuçlardan biri Modülerlik Teoreminin ispatıdır. Modülerlik Teoreminin pek çok farklı versiyonu vardır. Bu versiyonlardan biri olan geometrik versiyon, rasyonel sayılar üzerine tanımlı eliptik eğrilerle modüler eğriler arasında örten bir morfizma olduğunu söyler. Aritmetik versiyon ise rasyonel sayılar üzerine tanımlı eliptik eğrilerle modüler formlar arasında bir ilişki olduğunu söyler. Bu tezde Modülerlik Teoreminin geometrik versiyonunun aritmetik versiyonunu gerektirdiği gerçeğinin ispatı ana hatlarıyla verilmektedir.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS

$a_p(E)$	Modified solution count of E modulo p
A'_f	Abelain variety associated to f and $\Gamma_0(N)$
$\hat{\mathbb{C}}$	$\mathbb{C} \cup \{\infty\}$
$\mathbb{C}(X)$	Function field of X over $\mathbb{C}$
D	Fundamental domain
$\langle d \rangle$	Diamond Hecke operator for $d \in \mathbb{Z}^+$
$Div^0(C)$	Degree-0 divisor group of C
$Div(C)$	Divisor group of C
$Div^l(C)$	Principal divisors of C
$div(f)$	Divisor of f
E	Elliptic curve
E[N]	N-torsion subgroup of E
$\mathbb{F}_p$	Field of p elements
$\overline{\mathbb{F}}_p$	Algebraic closure of $\mathbb{F}_p$
$\mathcal{H}$	Upper half plane
$H_1(X, \mathbb{Z})$	First integral homology group of X
G_k	Eisenstein series of weight k
j	Invariant of a Weierstrass equation
$Jac(X)$	Jacobian of X
$J_0(X)$	Jacobian of $X_0(N)$
$\mathbf{k}(C)$	Function field of C
$\mathbf{k}[C]$	Coordinate ring of C
$M_k(\Gamma)$	The space of all modular forms of weight k with respect to Γ
$M_k(SL_2(\mathbb{Z}))$	The space of all modular forms of weight k
$[N]$	Multiply-by-N isogeny
N_E	Algebraic conductor of E
$S_0(N)$	Moduli space for $\Gamma_0(N)$
$S_0(N)_{alg}$	Algebraic moduli space for $\Gamma_0(N)$

$S_0(N)_{alg,\mathbb{C}}$	Complex algebraic moduli space for $\Gamma_0(N)$
$S_1(N)$	Moduli space for $\Gamma_1(N)$
$SL_2(\mathbb{Z})$	Modular group
$S_k(\Gamma)$	The space of all cusp forms of weight k with respect to Γ
$S_k(\Gamma_0(N))^{new}$	Newform at level N
$S_k(\Gamma_0(N))^{old}$	Oldform at level N
$S_k(SL_2(\mathbb{Z}))$	The space of all cusp forms of weight k
T_p	Hecke operator
$\mathbb{P}^n(\mathbf{k})$	n-dimensional projective space over $\mathbf{k}$
$Pic^0(X)$	Picard group of X
$X_0(N)$	Compact modular curve for $\Gamma_0(N)$
$X_1(N)$	Compact modular curve for $\Gamma_1(N)$
$X_0(N)_{alg}$	Modular curve as algebraic curve for $\Gamma_0(N)$
$X_1(N)_{alg}$	Modular curve as algebraic curve for $\Gamma_1(N)$
$X_0(N)_{alg}^{planar}$	Planar model of the modular curve for $\Gamma_0(N)$
$X_1(N)_{alg}^{planar}$	Planar model of the modular curve for $\Gamma_1(N)$
$X(N)$	Compact modular curve for $\Gamma(N)$
Δ	Discriminant of Weierstrass equation
$\Gamma_0(N)$	Congruence subgroup of level N
$\Gamma(N)$	Principal congruence subgroup of level N
Λ	Lattice in $\mathbb{C}$
Λ_f	Lattice associated to f
ν_P	Valuation at P
$\Omega^1_{hol}(X)^\wedge$	Holomorphic differentials of degree 1 on a modular curve
$\wp$	Weierstrass $\wp$-function
σ_p	Frobenius map
σ_p^{-1}	Inverse of σ_p
σ_p^*	Reverse induced map by σ_p
$\sigma_{p,*}$	Forward induced map by σ_p

1. INTRODUCTION

In this work, we will explain different versions of the Modularity Theorem and the implication from the geometric version of the Modularity Theorem to the arithmetic version. Then we will briefly explain what happens if the elliptic curve in the theorem is defined over a number field instead of the field of rational numbers.

The Modularity Theorem is used to prove Fermat's Last Theorem which says that there are no integer solutions of $x^n+y^n = z^n$ for any $n \geq 3$ such that $xyz \neq 0$. Fermat's Last Theorem is proved by Wiles and Taylor in 1995. The Modularity Theorem has many different versions. Some of them are more analytic and related with Riemann surfaces. Some of them are more algebraic whose statements contain elliptic curves, L-Functions, Galois representations, etc.

In the first part, we will describe modular forms and modular curves which are main objects of the geometric version of the Modularity Theorem. In the second part, we will define elliptic curves both as complex curves and algebraic curves and study some special properties of them. After that point, we describe abelian varieties associated to an eigenform and Hecke operators. Before stating the versions of the Modularity Theorem, we will prove Igusa's Theorem and Eichler-Shimura relation for a congruence subgroup $\Gamma_0(N)$. After all definitions and constructions, we will state the Modularity Theorem and we will show that the geometric version implies the arithmetic version. In the final part, we will state the Modularity Theorem over real quadratic fields and we will give some definitions to understand the statement in this case.

2. PRELIMINARIES

2.1. Modular Group and Modular Forms

Let $\mathcal{H}$ be the upper half plane such that $\mathcal{H} = \{\tau \in \mathbb{C} | \mathrm{Im}(\tau) > 0\}$. The modular group is the set of 2×2 matrices over $\mathbb{Z}$ whose determinants are 1,

$$SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

Remark 2.1. *The modular group is generated by two elements which are*

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Also we can see that an element of $SL_2(\mathbb{Z})$ is an automorphism of Riemann sphere $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ such that for any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ and $\tau \in \hat{\mathbb{C}}$,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} (\tau) = \frac{a\tau + b}{c\tau + d}.$$

If $c \neq 0$, then ∞ is mapped to a/c and $-d/c$ is mapped to ∞. If $c = 0$, then ∞ is mapped to ∞.

When we consider an element γ of $SL_2(\mathbb{Z})$, for $\tau \in \mathcal{H}$, we can easily observe that

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2} \qquad \text{where } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

This implies that $\gamma(\tau) \in \mathcal{H}$. So the image of any element of $\mathcal{H}$ under action of elements of $SL_2(\mathbb{Z})$ is again in $\mathcal{H}$. Also note that for any $\tau \in \mathcal{H}$,

(i) $I(\tau) = \tau$ where I is the 2 by 2 identity matrix in $SL_2(\mathbb{Z})$,

(ii) $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$ for all $\gamma, \gamma' \in SL_2(\mathbb{Z})$.

So we can say that $SL_2(\mathbb{Z})$ acts on $\mathcal{H}$.

Definition 2.2. *Let $k \in \mathbb{Z}$. A meromorphic function $f : \mathcal{H} \to \mathbb{C}$ is a weakly modular form of weight k if*

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau) \qquad \text{for } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \text{ and } \tau \in \mathcal{H}.$$

Definition 2.3. *Let $k \in \mathbb{Z}$. A function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight k if*

(i) f is holomorphic on $\mathcal{H}$,

(ii) f is weakly modular of weight k,

(iii) f is holomorphic at ∞.

The set of modular forms of weight k is denoted by $M_k(SL_2(\mathbb{Z}))$.

In the definition of modular forms of weight k, we say that f is holomorphic at ∞. Now, we will explain this. Let f be a weakly modular form of weight k. We know that one of the generators of $SL_2(\mathbb{Z})$ is $\gamma =: \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ which corresponds to translation:

$$\gamma : \tau \mapsto \tau + 1.$$

Note that $f(\tau + 1) = f(\gamma(\tau)) = (0\tau + 1)^k f(\tau) = f(\tau)$. So f is a $\mathbb{Z}$-periodic function. Let $D = \{q \in \mathbb{C} : |q| < 1\}$ be the unit open disk and $D' = D \setminus \{0\}$ be the punctured unit disk. Define the map $exp : \tau \mapsto e^{2\pi i\tau}$ which is from $\mathcal{H}$ to D'. Then there exists a corresponding function $g : D' \to \mathbb{C}$ to f such that $g \circ exp = f$. It means that $g(e^{2\pi i\tau}) = f(log(e^{2\pi i\tau})/(2\pi i))$. Note that g is well-defined even if the logarithm is determined up to $2\pi i\mathbb{Z}$. If f is holomorphic on $\mathcal{H}$, then g is also holomorphic on D' since the function exp is holomorphic on $\mathcal{H}$. So g has a Laurent expansion such as

$g(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ where $q = e^{2\pi i\tau} \in D'$. Note that if $Im(\tau) \to \infty$, then $q \to 0$. Thus f is holomorphic at ∞ if g can be extended holomorphically to $q = 0$. It means that all Laurent coefficients of g is zero for $n < 0$. Thus the Fourier expansion of f becomes $f(\tau) = \sum_{n=0}^{\infty} a_n(f) q^n$.

Below, we will give the Eisenstein series of weight k for $k > 2$ as a nontrivial example of a modular form of weight k.

Example 2.4. *Let $k > 2$ be an even integer. For any $\tau \in \mathcal{H}$, define Eisenstein series of weight k as follows*

$$G_k(\tau) = \sum_{(c,d)\neq(0,0),(c,d)\in\mathbb{Z}^2} \frac{1}{c\tau + d^k}.$$

Definition 2.5. *Let f be a modular form of weight k. Assume that Fourier expansion of f has leading coefficient $a_0 = 0$, that is*

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n, \qquad q = e^{2\pi i\tau}.$$

Then f is called a cusp form of weight k. The set of cusp forms is denoted by $S_k(SL_2(\mathbb{Z}))$.

As an example of cusp forms, we will define the discriminant function.

Example 2.6. *Let $g_2(\tau) = 60G_4(\tau)$ and $g_3(\tau) = 140G_6(\tau)$. For any $\tau \in \mathcal{H}$, define the discriminant function as*

$$\Delta : \mathcal{H} \to \mathbb{C}, \qquad \Delta(\tau) = (g_2(\tau))^3 - 27(g_3(\tau))^2.$$

Note that $\Delta \in S_{12}(SL_2(\mathbb{Z}))$ since Δ is weakly modular of weight 12 and holomorphic on $\mathcal{H}$. Also in the Fourier expansion of Δ, $a_0 = 0$ and $a_1 = (2\pi)^{12}$. For more details, see Section 1.1 in [1].

Definition 2.7. *Let $g_2(\tau) = 60G_4(\tau)$ and $g_3(\tau) = 140G_6(\tau)$. For any $\tau \in \mathcal{H}$, we will define j function as follows*

$$j : \mathcal{H} \to \mathbb{C}, \qquad j(\tau) = 1728\frac{(g_2(\tau))^3}{\Delta(\tau)}.$$

Note that j is holomorphic on $\mathcal{H}$. Since $(g_2)^3$ and Δ have the same weight which is 12, j is $SL_2(\mathbb{Z})$-invariant.

2.2. Congruence Subgroups

Definition 2.8. *Let $N \in \mathbb{Z}$. The principal congruence subgroup of level N is*

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (\text{mod N}) \right\}.$$

Note that $\Gamma(1) = SL_2(\mathbb{Z})$.

Definition 2.9. *Let Γ be a subgroup of $SL_2(\mathbb{Z})$. If $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$, then we call Γ a congruence subgroup of level N.*

Now, we define some important congruence subgroups which are

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} (\text{mod N}) \right\}$$

where $*$ means any element of $\mathbb{Z}$ and

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})\} : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} (\text{mod N}) \right\}.$$

Note that $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z})$. Also these subsets are normal subgroups of each other.

Definition 2.10. *For any congruence subgroup Γ which acts on the upper half plane $\mathcal{H}$, we can define a modular curve as the quotient space $\Gamma \setminus \mathcal{H}$ of orbits under Γ*

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

When we can compactify $Y(\Gamma)$, we get

$$X(\Gamma) = \Gamma \setminus \mathcal{H}^*$$

as a compact modular curve where $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. For simplicity, we denote $X(\Gamma(N)) = X(N)$, $X(\Gamma_1(N)) = X_1(N)$, and $X(\Gamma_0(N)) = X_0(N)$.

Remark 2.11. *The points in $\Gamma \setminus \mathbb{Q} \cup \{\infty\}$ are called cusps of $X(\Gamma)$ which are Γ-equivalent to ∞. To compactify $Y(\Gamma)$, we add cusps to $Y(\Gamma)$.*

For proof of Remark 2.11 and details about compactified modular curve, see Section 2.4 in [1].

In what follows, we will consider the compact modular curve $X(\Gamma)$ and we call it a modular curve.

Remark 2.12. *The modular curve $X(\Gamma)$ is Hausdorff, connected, and compact. Also we can think a modular curve as a compact Riemann surface.*

For proof and details of Remark 2.12, see Chapter 2 in [1].

2.3. Modular Forms with respect to Γ

Definition 2.13. *Let $k \in \mathbb{Z}$ and $f : \mathcal{H} \to \mathbb{C}$ be a meromorphic function. Define the weight k operator $[\gamma]_k$ on f as follows*

$$(f[\gamma]_k)(\tau) = (c\tau + d)^{-k} f(\gamma(\tau)) \qquad \text{for } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \text{ and } \tau \in \mathcal{H}.$$

Definition 2.14. *Let $k \in \mathbb{Z}$ and $f : \mathcal{H} \to \mathbb{C}$ be a function. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. Then f is called weight-k invariant under Γ if*

$$f[\gamma]_k = f \qquad \text{for all } \gamma \in \Gamma. \tag{2.1}$$

Also if the function f is meromorphic and satisfies (2.1), then f is called a weakly modular form of weight k with respect to Γ.

Definition 2.15. *Let $k \in \mathbb{Z}$ and Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. A function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight k with respect to Γ if*

(i) f is holomorphic on $\mathcal{H}$,
(ii) f is weakly modular of weight k with respect to Γ,
(iii) $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$.

Then the set of modular forms of weight k with respect to Γ is denoted by $M_k(\Gamma)$.

In the definition of modular forms of weight k with respect to Γ, we say that $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$. Now, we will explain this in the same way as modular forms. Let f be a weakly modular form of weight k with respect to Γ. Since any congruence subgroup Γ contains $\Gamma(N)$ for some $N \in \mathbb{Z}^+$, Γ contains a translation matrix in the form

$$\gamma_N =: \begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix} \qquad \text{for some } N \in \mathbb{Z}^+.$$

Let h be the minimal number such that $\gamma_h \in \Gamma$ and $h|N$. Note that $f(\gamma_h(\tau)) = f(\tau + h) = f(\tau)$. So f is a $h\mathbb{Z}$-periodic function. Define the map $exp : \tau/h \mapsto e^{\frac{2\pi i\tau}{h}}$ which is from $\mathcal{H}$ to D'. Then there exists a corresponding function $g : D' \to \mathbb{C}$ to f such that $g \circ exp = f$. As before, if f is a holomorphic on $\mathcal{H}$, then g is also holomorphic on D'. So g has a Laurent expansion such as $g(q_h) = \sum_{n\in\mathbb{Z}} a_n q_h^n$ where $q_h = e^{\frac{2\pi i\tau}{h}} \in D'$. Thus f is holomorphic at ∞ if g can be extended holomorphically to $q = 0$. Therefore the Fourier expansion of f becomes $f(\tau) = \sum_{n=0}^{\infty} a_n(f) q_h^n$.

Definition 2.16. *Let $k \in \mathbb{Z}$ and Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. Let f be a modular form of weight k with respect to Γ. If for all $\alpha \in SL_2(\mathbb{Z})$, $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$, f is called a cusp form of weight k with respect to Γ. Then the set of cusp forms of weight k with respect to Γ is denoted by $S_k(\Gamma)$.*

2.4. Modular Curves as Algebraic Curves

Let $\mathbf{k}$ be any field of characteristic 0 and $\overline{\mathbf{k}}$ be a fixed algebraic closure of $\mathbf{k}$. Let I be the ideal generated by finitely many polynomials in $\overline{\mathbf{k}}[x_1, ..., x_n]$. Then C is the zero set of all polynomials in the ideal I.

Definition 2.17. *Let $\overline{\boldsymbol{k}}(C)$ be the function field of C over $\overline{\boldsymbol{k}}$. If $\overline{\boldsymbol{k}}(C)$ is a finite extension of $\overline{\boldsymbol{k}}(t)$ with transcendental element t over $\overline{\boldsymbol{k}}$, then C is an affine algebraic curve over $\boldsymbol{k}$.*

Let $\bar{\nu}$ be the reduction of any nonzero vector $\nu \in \mathbb{Z}^2$ modulo N. Define

$$f_0^{\bar{\nu}}(\tau) = \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau\left(\frac{c_\nu\tau + d_\nu}{N}\right) \quad \text{for } \nu = (c_\nu, d_\nu)$$

where $\wp_\tau$ is the Weierstrass $\wp$-function. In the next section, we will define explicitly the Weierstrass $\wp$-function. Note that $f_0^{\bar{\nu}}$ is weigth 0 invariant under $\Gamma(N)$ and $f_0^{\pm\bar{\nu}} \in \mathbb{C}(X(N))$. For simplicity, we define

$$f_0^{\bar{d}}(\tau) = f_0^{\overline{(0,d)}}(\tau), \quad d \not\equiv 0 \pmod{\text{N}} \qquad \textit{and} \qquad f_0(\tau) = \sum_{d=1}^{N-1} f_0^{\bar{d}}(\tau). \tag{2.2}$$

Note that $f_0^{\bar{d}}$ and f_0 are weight 0 invariant under $\Gamma_1(N)$ and $\Gamma_0(N)$, respectively and $f_0^{\bar{d}} \in \mathbb{C}(X_1(N))$ and $f_0 \in \mathbb{C}(X_0(N))$. For convenience, we introduce some notation:

$$f_{1,0} = f_0^{\pm\overline{(1,0)}}, \qquad f_{0,1} = f_1 = f_0^{\pm\overline{(0,1)}}, \qquad j_N(\tau) = j(N\tau).$$

Remark 2.18. *The function field of $X_0(N)$, $X_1(N)$, and $X(N)$ are respectively as follows:*

- $\mathbb{C}(X_0(N)) = \mathbb{C}(j, f_0) = \mathbb{C}(j, j_N)$,
- $\mathbb{C}(X_1(N)) = \mathbb{C}(j, \{f_0^{\pm\bar{d}} | \pm\bar{d} \in (\mathbb{Z}/N\mathbb{Z} - 0)/\pm\}) = \mathbb{C}(j, f_1)$,
- $\mathbb{C}(X(N)) = \mathbb{C}(j, \{f_0^{\pm\bar{\nu}} | \pm\bar{\nu} \in ((\mathbb{Z}/N\mathbb{Z})^2 - (0,0))/\pm\}) = \mathbb{C}(j, f_{1,0}, f_{0,1})$.

For proof and details of Remark 2.18, see Section 7.5 in [1].

Definition 2.19. *The planar models of $X_0(N)$ and $X_1(N)$ are*

- $X_1(N)_{alg}^{planar} = \{(j,x) \in \overline{\mathbb{Q}}^2 | \psi_1(j,x) = 0\}$ *where ψ_1 is the polynomial over $\mathbb{Q}[j,x]$ that we get when we clear the denominator of $p_1 \in \mathbb{Q}(j)[x]$ which is the minimal polynomial of f_1 over $\mathbb{Q}(j)$,*
- $X_0(N)_{alg}^{planar} = \{(j,x) \in \overline{\mathbb{Q}}^2 | \psi_0(j,x) = 0\}$ *where ψ_0 is the polynomial over $\mathbb{Q}[j,x]$ that we get when we clear the denominator of $p_0 \in \mathbb{Q}(j)[x]$ which is the minimal polynomial of f_0 over $\mathbb{Q}(j)$.*

3. ELLIPTIC CURVES AND ABELIAN VARIETIES

3.1. Elliptic Curves as Complex Tori

Definition 3.1. *Let $\omega_1, \omega_2 \in \mathbb{C}$. A lattice in $\mathbb{C}$ is a set $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ where $\{\omega_1, \omega_2\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$. A complex torus is the quotient of $\mathbb{C}$ by the lattice as*

$$\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}.$$

Let $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ be the compactification of $\mathbb{C}$. For any lattice Λ, a meromorphic function $f : \mathbb{C}/\Lambda \to \hat{\mathbb{C}}$ gives us a Λ-periodic meromorphic function $f : \mathbb{C} \to \hat{\mathbb{C}}$. One of examples of these functions is the Weierstrass $\wp$-function which is defined as

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \omega \in \Lambda} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \quad \text{for } z \in \mathbb{C} \text{ and } z \notin \Lambda$$

with the derivative of $\wp$

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}.$$

Theorem 3.2. *Let $\wp$ be the Weierstrass function corresponding to the lattice Λ.*

(i) The functions $\wp$ and $\wp'$ satisfy the following differential equation

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.

(ii) Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ *and* $\omega_3 = \omega_1 + \omega_2$. *Then the above cubic equation* $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ *becomes*

$$y^2 = 4(x_1 - e_1)(x_2 - e_2)(x_2 - e_2), \qquad e_i = \wp(\omega_i/2), i = 1, 2, 3.$$

Right side of the equation has three distinct roots. Therefore the equation is nonsingular.

For proof of Theorem 3.2, see Proposition 1.4.1 in [1].

For any field $\mathbf{k}$ with characteristic 0, the solution set of the nonsingular polynomial equation $y^2 = 4x^3 + ax + b$ where $a, b \in \mathbf{k}$ is called an elliptic curve.

Theorem 3.3. *For a given elliptic curve with* $y^2 = 4x^3 - a_2x - a_3$, $a_2^3 - 27a_3^2 \neq 0$, *there exists a lattice such that* $a_2 = g_2(\Lambda)$ *and* $a_3 = g_3(\Lambda)$.

For proof of Theorem 3.3, see Proposition 1.4.3 in [1].

By Theorem 3.2 and Theorem 3.3, for any lattice Λ, the Weierstrass $\wp$-function and its derivative give us a one-to-one correspondence between complex torus $\mathbb{C}/\Lambda$ and elliptic curve E with $y^2 = 4x^3 - g_2(\Lambda) - g_3(\Lambda)$.

Remark 3.4. *After Theorem 3.2 and Theorem 3.3, we will refer the complex torus as the complex elliptic curve. Also we will refer the algebraic elliptic curve as* E_τ *which is the solution set of the polynomial equation* $y^2 = 4x^3 - g_2(\tau) - g_3(\tau)$ *where* $\tau = \omega_2/\omega_1$ *with* $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$.

3.2. Moduli Spaces

Definition 3.5. *An enhanced complex analytic elliptic curve for* $\Gamma_0(N)$ *is an ordered pair* (E, C) *where* E *is a complex elliptic curve and* C *is a cyclic subgroup of* E *of order* N. *Two such pairs* (E, C) *and* (E', C') *are equivalent, denoted by* $(E, C) \sim (E', C')$,

if there exists an isomorphism $E\tilde{\to}E'$ *over* $\mathbb{C}$ *such that it takes* C *to* C'*. The set of equivalence classes is the complex analytic moduli space for* $\Gamma_0(N)$ *and denoted by*

$$\begin{aligned} S_0(N) &= \{\textit{enhanced complex analytic elliptic curves for } \Gamma_0(N)\}/\sim \\ &= \{[\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle] : \tau \in \mathcal{H}\}. \end{aligned}$$

Definition 3.6. *An enhanced complex algebraic elliptic curve for* $\Gamma_0(N)$ *is an ordered pair* (E, C) *where* E *is an algebraic elliptic curve over* $\mathbb{C}$ *and* C *a is cyclic subgroup of* E *of order* N*. Two such pairs* (E, C) *and* (E', C') *are equivalent, denoted by* $(E, C) \sim (E', C')$*, if there exists an isomorphism* $E\tilde{\to}E'$ *over* $\mathbb{C}$ *such that it takes* C *to* C'*. The set of equivalence classes is the complex algebraic moduli space for* $\Gamma_0(N)$ *and denoted by*

$$\begin{aligned} S_0(N)_{alg,\mathbb{C}} &= \{\textit{enhanced complex algebraic elliptic curves for } \Gamma_0(N)\}/\sim \\ &= \{[E_\tau, \langle(\wp_\tau(1/N), \wp'_\tau(1/N))\rangle] : \tau \in \mathcal{H}\}. \end{aligned}$$

Remark 3.7. *There is a bijective correspondence between* $S_0(N)$ *and* $S_0(N)_{alg,\mathbb{C}}$ *such that*

$$[\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle] \mapsto [E_\tau, \langle(\wp_\tau(1/N), \wp'_\tau(1/N))\rangle].$$

For proof and details of Remark 3.7, see Section 7.9 in [1].

Definition 3.8. *An enhanced algebraic elliptic curve for* $\Gamma_0(N)$ *is an ordered pair* (E, C) *where* E *is an algebraic elliptic curve over* $\overline{\mathbb{Q}}$ *and* C *is a cyclic subgroup of* E *of order* N*. Two such pairs* (E, C) *and* (E', C') *are equivalent, denoted by* $(E, C) \sim (E', C')$*, if there exists an isomorphism* $E\tilde{\to}E'$ *over* $\overline{\mathbb{Q}}$ *such that it takes* C *to* C'*. The set of equivalence classes is the algebraic moduli space for* $\Gamma_0(N)$ *and denoted by*

$$\begin{aligned} S_0(N)_{alg} &= \{\textit{enhanced complex algebraic elliptic curves for } \Gamma_0(N)\}/\sim \\ &= \{[E_\tau, \langle(\wp_\tau(1/N), \wp'_\tau(1/N))\rangle] : \tau \in \mathcal{H}\}. \end{aligned}$$

Remark 3.9. *The element [E,C] of $S_0(N)_{alg,\mathbb{C}}$ becomes the element of $S_0(N)_{alg}$ if and only if $j(E) \in \overline{\mathbb{Q}}$.*

For proof of Remark 3.9, see Section 7.9 [1].

3.3. Elliptic Curves as Algebraic Curves

Definition 3.10. *Let $\boldsymbol{k}$ be an arbitrary field. A Weierstrass equation $E(x, y)$ over $\boldsymbol{k}$ is a cubic equation of the form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in \boldsymbol{k}$.

For simplicity, we can define the relations:

$$\begin{aligned} b_8 &= a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

The discriminant of the equation is

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

When the discriminant Δ of a Weierstrass equation is nonzero, the equation is called nonsingular. If $\Delta \neq 0$, we can define the j-invariant as $j = c_4^3/\Delta$.

Remark 3.11. *If $char(\boldsymbol{k}) \neq 2$, then we can simplify the Weierstrass equation by replacing y by $y - (a_1x + a_3)/2$ and we get*

$$E(x, y) : y^2 = x^3 + (b_2x^2 + 2b_4x + b_6)/4$$

where $b_2, b_4, b_6 \in \boldsymbol{k}$ *and* $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$.

Remark 3.12. *If* $char(\boldsymbol{k})$ *is not equal to 2 or 3, then we can simplify the Weierstrass equation by replacing* x *by* $(x - 3b_2)/36$ *and* y *by* $y/216$ *and we get*

$$E(x, y) : y^2 = x^3 - 27c_4x - 54c_6$$

where $c_2, c_6 \in \boldsymbol{k}$.

The general admissible change of variables over an arbitray field $\mathbf{k}$ is

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t, \qquad u, r, s, t \in \mathbf{k}, u \neq 0.$$

These changes transform Weierstrass equations to Weierstrass equations while changing the discriminant Δ to Δ/u^{12} and preserving the j-invariant. The admissible change of variables is special case of an isomorphism between algebraic curves.

Definition 3.13. *Let* $\bar{\boldsymbol{k}}$ *be an algebraic closure of the field* $\boldsymbol{k}$. *Let* $E(x, y)$ *be a Weierstrass equation over* $\boldsymbol{k}$. *The set*

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

is called an elliptic curve over $\boldsymbol{k}$ *if the equation* $E(x, y)$ *is nonsingular.*

Now, we will consider the relation between the cubic equation $y^2 = 4x^3 - g_2x - g_3$ mentioned in Theorem 3.3 and a Weierstrass equation. When we apply the admissible change of variables $(x, y) = (u^2x', u^3y')$ to the cubic equation where $u = (g_3/g_2)^{1/2}$, we get the cubic equation

$$y^2 = 4x^3 - \frac{g_2^3}{g_3^2}x - \frac{g_2^3}{g_3^2}. \tag{3.1}$$

By the definition of Δ in (2.7), we have $g_3^2 = (g_2^3 - \Delta)/27$. Then $g_2^3/g_3^2 = 27g_2^3(g_2^3 - \Delta) = 27j/(j - 1728)$ where $j = j(\tau)$. Thus the cubic equation (3.1) becomes

$$y^2 = 4x^3 - \frac{27j}{j - 1728}x - \frac{1}{j - 1728}. \tag{3.2}$$

After that when we replace y with $2y$ and apply the suitable admissible change of variables, we get

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{27j}{j - 1728}$$

which corresponds to a Weierstrass equation for any field of arbitrary characteristic. For more details about this correspondence, see Section 8.1 in [1].

Remark 3.14. *Let E be an elliptic curve over $\boldsymbol{k}$ given by a Weierstrass equation. Then we can think the points of E over $\bar{\boldsymbol{k}}$ with the point ∞ as an abelian group by the composition law $\oplus$ where the point ∞ is the identity element 0_E of group operation.*

Definition 3.15 (Composition Law)**.** *Let $P, O \in E$. Let L be a line passing through P and Q.(If $P = Q$, then L is the tangent line to E at P.) Let R be another intersection point E and L, which is different from P and Q. Let L' be the line passing through R and the point ∞. The third intersection point E and L' is $P \oplus Q$.*

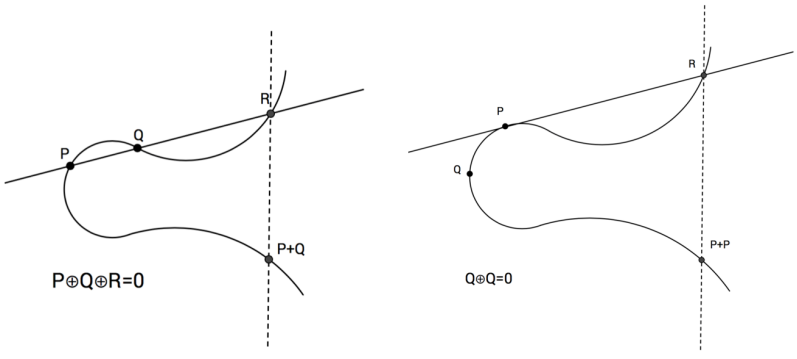


Figure 3.1. Composition Law

Definition 3.16. *For any integer N, we can define a subgroup E[N] of an abelian group E as follows*

$$E[N] = \{P \in E : [N]P = 0_E\}$$

where $[N]$ is the multiplication-by-N isogeny. In the next section, we will define the multiplication-by-N isogeny. The subgroup E[N] is called N-torsion points of E.

Definition 3.17. *Let C be a nonsingular algebraic curve over $\boldsymbol{k}$. The divisor group of C is a free abelian group such that*

$$Div(C) = \left\{ \sum_{P \in C} n_P(P) : n_P \in \mathbb{Z}, n_P = 0 \text{ for all but finitely many } P \in C \right\}.$$

The degree-0 divisor group $Div^0(C)$ is a subgroup of Div(C) defined as

$$Div^0(C) = \left\{ \sum_{P \in C} n_P(P) \in Div(C) : \sum_{P \in C} n_P = 0 \right\}.$$

To define a divisor of $F \in \bar{\mathbf{k}}(C)$, we will define the valuation which is similar to the p-adic valuation. In Definition 3.36, we will define explicitly the p-adic valuation.

Definition 3.18. *Let $\bar{\boldsymbol{k}}[C]$ be the coordinate ring of C over $\bar{\boldsymbol{k}}$. The valuation ν_P at $P \in C$ is defined as*

$$\nu_P : \bar{\boldsymbol{k}}[C] \to \mathbb{N} \cup \{+\infty\}, \qquad \nu_P(f) = \begin{cases} +\infty & \text{if } f = 0 \\ e & \text{if } f = t^e u \end{cases} \tag{3.3}$$

where t is a generator of the maximal ideal of $\bar{\boldsymbol{k}}[C]_P$.
Then we can extend the valuation to the function field $\bar{\boldsymbol{k}}(C)$ of C over $\bar{\boldsymbol{k}}$ such that

$$\nu_P : \bar{\boldsymbol{k}}(C) \to \mathbb{Z} \cup \{+\infty\}, \qquad \nu_P(F) = \nu_P(f) - \nu_P(g)$$

where $F = f/g \in \bar{\boldsymbol{k}}(C)$.

Definition 3.19. *Let* F *be a nonzero element of function field* $\bar{\boldsymbol{k}}(C)$ *of* C*. The divisor of* F *is*

$$div(F) = \sum_{P \in C} \nu_P(F)(P).$$

A divisor of the form div(F) is called principal and the set of principal divisors is denoted by $Div^{\ell}(C)$.

Since F is a rational function on C, F is meromorphic. It implies that the sum of $\nu_P(F)$ for all $p \in C$ is zero. So principal divisors are in $Div^0(C)$. By the properties of the valuation, we can define the homomorphism as follows

$$div : \bar{\mathbf{k}}(C)^* \to Div^0(C), \qquad F \mapsto div(F).$$

Thus $Div^{\ell}(C)$ is a subgroup of $Div^0(C)$.

Definition 3.20. *The Picard group of* C *is the divisor class group as*

$$Pic^0(C) = Div^0(C)/Div^{\ell}(C).$$

3.4. Isogenies

Definition 3.21. *Let* E *and* E' *be elliptic curves. Define the isogeny* ϕ *from* E *to* E' *as a morphism such that*

$$\phi : E \to E', \qquad \phi(O_E) = O_{E'}$$

where O_E *and* $O_{E'}$ *are identity elements of* E *and* E' *as abelian groups, respectively. We call that* E *and* E' *isogenous if there exists a non-constant isogeny* ϕ *from* E *to* E'.

Remark 3.22. *Any isogeny $\phi : E \to E'$ satisfies either $\phi(E) = \{O\}$ or $\phi(E) = E'$. If it satisfies $\phi(E) \neq \{O\}$, it has a finite kernel.*

Example 3.23. *Let E be an elliptic curve and C be a cyclic subgroup of order p. Then E/C is also abelian group. Define a morphism over abelian groups as*

$$\phi : E \to E/C.$$

Note that the morphism ϕ maps the identity element O_E of E to the identity element $O_E + C$ of E/C. Thus we can say that ϕ is a quotient isogeny.

Definition 3.24. *For any $n \in \mathbb{Z}$, we can define the multiplication-by-n isogeny of an elliptic curve E as*

$$[n] : E \to E, \qquad [n]P = \underbrace{P + P + ... + P}_{n \text{ times}}.$$

Theorem 3.25. *Let $\phi : E \to E'$ be a nonconstant isogeny of degree m. Then there exists a unique isogeny*

$$\psi : E' \to E$$

satisfying $\phi \circ \psi = \psi \circ \phi = [m]$.

For proof of Theorem 3.25, see Theorem 6.1 in [2].

Definition 3.26. *Let $\phi : E \to E'$ be a nonconstant isogeny. An isogeny*

$$\psi : E' \to E$$

is called a dual isogeny of ϕ if the equality $\psi \circ \phi = [deg(\phi)] = [deg(\psi)]$ holds.

Now, we will define the Frobenius map and give some properties to explain the Eichler-Shimura relation.

Definition 3.27. *The Frobenius map on* $\mathbb{P}^n(\overline{\mathbb{F}}_p)$ *is*

$$\sigma_p : \mathbb{P}^n(\overline{\mathbb{F}}_p) \to \mathbb{P}^n(\overline{\mathbb{F}}_p)$$

such that $\sigma_p([x_0 : x_1 : ... : x_n]) = [x_0^p : x_1^p : ... : x_n^p]$. *The inverse of* σ_p *is*

$$\sigma_p^{-1} : \mathbb{P}^n(\overline{\mathbb{F}}_p) \to \mathbb{P}^n(\overline{\mathbb{F}}_p)$$

such that $\sigma_p^{-1}([x_0 : x_1 : ... : x_n]) = [y_0 : y_1 : ... : y_n]$
where $[x_0 : x_1 : ... : x_n] = [y_0^p : y_1^p : ... : y_n^p]$.
Let $x_i = z_i \in \overline{\mathbb{F}}_p$. *Then there exist* $y_i, v_i \in \overline{\mathbb{F}}_p$ *such that* $y_i^p = x_i$ *and* $v_i^p = z_i$ *where* $\sigma_p^{-1}(x_i) = y_i$ *and* $\sigma_p^{-1}(z_i) = v_i$. *Since* $x_i = z_i$, $y_i^p = x_i = z_i = v_i^p$. *It implies that* $0 = y_i^p - v_i^p = (y_i - v_i)^p$ *in* $\overline{\mathbb{F}}_p$ *whose characteristic is p. Then it gives us* $y_i = v_i$. *Thus* σ_p^{-1} *is well defined.*

Let $\psi(x_0, x_1, ..., x_n) = \sum_i a_i x^i \in \overline{\mathbb{F}}_p[x_0, x_1, ..., x_n]$ where $x^i = x_0^{i_0} x_1^{i_1} ... x_n^{i_n}$. Then ψ^{σ_p} is obtained by applying the Frobenius map on the coefficients of ψ. So we get the polynomial $\psi^{\sigma_p}(x_0, x_1, ..., x_n) = \sum_i a_i^{\sigma_p} x^i$. Consider for any $P = [x_0 : x_1 : ... : x_n] \in \mathbb{P}^n(\overline{\mathbb{F}}_p)$,

$$\begin{aligned} \psi^{\sigma_p}(P^{\sigma_p}) = \psi^{\sigma_p}([x_0^p : x_1^p : ... : x_n^p]) = \sum_i a_i^{\sigma_p} x^{p^i} = \sum_i a_i^p x^{ip} = (\sum_i a_i x^i)^p \\ = \psi([x_0 : x_1 : ... : x_n])^{\sigma_p} = \psi(P)^{\sigma_p} \end{aligned} \tag{3.4}$$

since the characteristic of $\overline{\mathbb{F}}_p$ is p.

Remark 3.28. *Let C be a projective curve defined over* $\overline{\mathbb{F}}_p$ *by polynomials* ψ_i. *Define a projective curve* C^{σ_p} *over* $\overline{\mathbb{F}}_p$ *by polynomials* $\psi_i^{\sigma_p}$. *If* $P \in C$, *then* $\psi_i(P) = 0$ *for all i. Also* $\psi_i(P)^{\sigma_p} = \psi_i^{\sigma_p}(P^{\sigma_p})$ *by* (3.4). *It means that* $P^{\sigma_p} \in C^{\sigma_p}$. *So we can restrict* σ_p *to a morphism from C to* C^{σ_p} *with* $\sigma_p(P) = P^{\sigma_p}$

Definition 3.29. *Let C be a projective curve over $\overline{\mathbb{F}}_p$. The Frobenius map on C is*

$$\sigma_p : C \to C^{\sigma_p}$$

such that $\sigma_p(P) = P^{\sigma_p}$ for any $P \in C$. Also the inverse of σ_p is

$$\sigma_p^{-1} : C^{\sigma_p} \to C$$

such that $\sigma_p^{-1}(P') = P$ where $P' = P^{\sigma_p}$.

Theorem 3.30. *Let C be a nonsingular projective algebraic curve over a field $\boldsymbol{k}$ and $\boldsymbol{k}(C)$ be the function field of C over $\boldsymbol{k}$. The map*

$$C \mapsto \boldsymbol{k}(C)$$

gives us the bijection between the set of isomorphism classes over $\boldsymbol{k}$ of nonsingular projective algebraic curves over $\boldsymbol{k}$ and the set of conjugacy classes over $\boldsymbol{k}$ of function fields over $\boldsymbol{k}$.

In Theorem 3.30, the conjugation means that if there exists an isomorphism between function fields $\mathbf{K}$ and $\mathbf{K}'$ which fixes $\mathbf{k}$ pointwise, then two function fields $\mathbf{K}$ and $\mathbf{K}'$ over $\mathbf{k}$ are conjugate over $\mathbf{k}$.

Theorem 3.31. *Let C and C' be nonsingular projective algebraic curves over a field $\boldsymbol{k}$. Then the map*

$$h \mapsto h^*$$

gives us the bijection between the set of nonconstant morphism over $\boldsymbol{k}$ from C to C' and the set of $\boldsymbol{k}$-injections of $\boldsymbol{k}(C')$ to $\boldsymbol{k}(C)$.

For proofs of Theorem 3.30 and Theorem 3.31, see Section 7.2 in [1].

Let $h : C \to C'$ be a surjective morphism over $\overline{\mathbb{F}}_p$ of nonsingular projective curves over $\overline{\mathbb{F}}_p$. Then by Theorem 3.31, we have a corresponding $\overline{\mathbb{F}}_p$-injection $h^* : \overline{\mathbb{F}}_p(C') \to \overline{\mathbb{F}}_p(C)$. Note that for the field extension $\overline{\mathbb{F}}_p(C)/\overline{\mathbb{F}}_p(C')$, we have an inclusion such that

$$h^*(\overline{\mathbb{F}}_p(C')) \subset \overline{\mathbb{F}}_p(C')_{sep} \subset \overline{\mathbb{F}}_p(C).$$

In this inclusion, $\overline{\mathbb{F}}_p(C')_{sep}/h^*(\overline{\mathbb{F}}_p(C'))$ is the maximal separable subextension of $\overline{\mathbb{F}}_p(C)/h^*(\overline{\mathbb{F}}_p(C'))$. So we can factorize h^* such as

$$\overline{\mathbb{F}}_p(C') \xrightarrow{h^*_{sep}} \overline{\mathbb{F}}_p(C')_{sep} \xrightarrow{h^*_{ins}} \overline{\mathbb{F}}_p(C).$$

Then again by Theorem 3.31, we have a corresponding factorization of h as

$$C \xrightarrow{h_{ins}} C_{sep} \xrightarrow{h_{sep}} C'.$$

where the first map h_{ins} is σ_p^e with $p^e = [\overline{\mathbb{F}}_p(C) : \overline{\mathbb{F}}_p(C')_{sep}]$. Thus the general factorization of isogeny h is $h = h_{sep} \circ \sigma_p^e$. Also this factorization preserves the degrees of maps such as

$$deg(h) = deg(h_{sep})deg(h_{ins})$$

where $deg(h) = [\overline{\mathbb{F}}_p(C) : h^*(\overline{\mathbb{F}}_p(C'))]$, $deg(h_{sep}) = [\overline{\mathbb{F}}_p(C')_{sep} : \overline{\mathbb{F}}_p(C')]$, and $deg(h_{ins}) = [\overline{\mathbb{F}}_p(C) : \overline{\mathbb{F}}_p(C')_{sep}]$.

Theorem 3.32. *Let ϕ be an isogeny of elliptic curves from E to E'. Then*

$$deg(\phi_{sep}) = |ker(\phi)|.$$

For proof of Theorem 3.32, see Section 8.2 in [1].

Definition 3.33. *Let $h : C \to C'$ be a nonconstant morphism of projective algebraic curves. The induced forward map of h over Picard groups of algebraic curves is defined by*

$$h_* : Pic^0(C) \to Pic^0(C'), \qquad \left[\sum_P n_P(P)\right] \mapsto \left[\sum_P n_P(h(P))\right].$$

Definition 3.34. *Let C be a projective curve over $\overline{\mathbb{F}}_p$ and (P) be the divisor of C. Define the forward map of $Pic^0(C)$ induced by the Frobenius map σ_p as*

$$\sigma_{p,*} : (P) \mapsto (\sigma_p(P)).$$

The reverse map of $Pic^0(C)$ induced by σ_p is

$$\sigma_p^* : (P) \mapsto (\sigma_p^{-1}(P)).$$

Theorem 3.35. *Let $h : C \to C'$ be a map over $\mathbb{F}_p$ between projective curves over $\mathbb{F}_p$. Let $\sigma_{p,C}$ and $\sigma_{p,C'}$ be the Frobenius maps of C and C'. Then the induced forward map h_* commutes with the forward induced map of $\sigma_{p,C}$ as*

$$h_* \circ (\sigma_{p,C})_* = (\sigma_{p,C'})_* \circ h_*.$$

Also the induced forward map h_* commutes with the reverse map of $\sigma_{p,C}$ as

$$h_* \circ (\sigma_{p,C})^* = (\sigma_{p,C'})^* \circ h_*.$$

For proof of Theorem 3.35, see page 321 in [1].

3.5. The Reduction of Elliptic Curves

Let E be an elliptic curve given by a Weierstrass equation over $\mathbb{Q}$. If we apply the admissible change of variables over $\mathbb{Q}$ such that $(x, y) = (u^2x', u^3y')$, then we get another Weierstrass equation corresponding to another elliptic curve E' with coefficients $a'_i = a_i/u^i$. With a suitable choice of u, the coefficients of Weierstrass equation of E' can be made integral. We can say that E and E' are equivalent if there is an admissible change of variables over $\mathbb{Q}$ such that we get the coefficients of Weierstrass equation of E' applying the change of variables to the coefficients of Weierstrass equation of E. After that point, we can think that E is an elliptic curve given by a Weierstrass equation over $\mathbb{Z}$. In this case E is called integral.

Definition 3.36. *Let p be a prime and r a rational number. Then $\nu_p(r)$ is the power of p which appears in r. It means that $\nu_p(p^e m/n) = e \in \mathbb{Z}$ with $p \nmid mn$. Then $\nu_p(r)$ is called the p-adic valuation.*

Proposition 3.37. *For all $r, r' \in \mathbb{Q}$,*

(i) $\nu_p(0) = +\infty$,
(ii) $\nu_p(rr') = \nu_p(r) + \nu_p(r')$ *for all* $r, r' \in \mathbb{Q}$,
(iii) $\nu_p(r + r') \geq min\{\nu_p(r), \nu_p(r')\}$ *with equality if* $\nu_p(r) \neq \nu_p(r')$.

For any prime p, let $\nu_p(E)$ be the smallest power of p in the discriminant $\Delta(E)$ of any Weierstrass equation which is equivalent to E. It means that

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

Definition 3.38. *The global minimal discriminant of E is*

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

The global minimal Weierstrass equation of E' is an integral model such that E' is isomorphic over $\mathbb{Q}$ to E and the discriminant $\Delta(E')$ of E' is equal to $\Delta_{min}(E)$.

Remark 3.39. *In general, the global minimal Weierstrass equation of an elliptic curve E exists if E is defined over a field with ideal class number one.*

To define the reduction of elliptic curves modulo p, we define tilde notation as follows

$$\widetilde{\ }: \mathbb{Z} \to \mathbb{F}_p, \qquad \widetilde{n} = n + p\mathbb{Z}. \tag{3.5}$$

This map reduces the global minimal Weierstrass equation of E to a Weierstrass equation of $\widetilde{E}$ over $\mathbb{F}_p$. If $p \nmid \Delta_{min}(E)$, then $\widetilde{E}$ defines an elliptic curve over $\mathbb{F}_p$. Now, consider all cases of the reduction of E modulo p.

Definition 3.40. *Let E be an elliptic curve as defined above. The reduction of E modulo p is*

(i) good (nonsingular) if $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p$,
- *ordinary if $\widetilde{E}[p] \cong \mathbb{Z}/p\mathbb{Z}$,*
- *supersingular if $\widetilde{E}[p] = \{0\}$,*

(ii) bad (singular) if $\widetilde{E}$ is not an elliptic curve in which case it has only one singular point,
- *multiplicative if $\widetilde{E}$ has a node,*
- *additive if $\widetilde{E}$ has a cusp.*

Remark 3.41. *Let E be an elliptic curve over a field $\boldsymbol{k}$ and N be a positive integer. In general, if $char(\boldsymbol{k}) \nmid N$, then $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$.*

Definition 3.42. *The algebraic conductor of E is $N_E = \prod_p p^{f_p}$ where*

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

with $\delta_2 \leq 6$ and $\delta_3 \leq 3$. For more explicit calculation of δ_p, see page 287 in [3].

Definition 3.43. *Let E be an elliptic curve over $\mathbb{Q}$ and p a prime. Let $\widetilde{E}$ be the reduction of E modulo p. Then define*

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

where $\widetilde{E}(\mathbb{F}_p)$ are $\mathbb{F}_p$-points of $\widetilde{E}$.

Theorem 3.44. *Let p be a prime and E be an elliptic curve over $\mathbb{Q}$ such that E has a good reduction at p. Let $\sigma_{p,*}$ and σ_p^* be the forward and reverse maps of $Pic^0(\widetilde{E})$ induced by σ_p. Then we have the equality*

$$[a_p(E)] = \sigma_{p,*} + \sigma_p^*$$

as endomorphisms of $Pic^0(\widetilde{E})$ where the left side is just multiplication by $a_p(E)$.

For proof of Theorem 3.44, see page 325 in [1].

Definition 3.45. *Let $\mathfrak{p}$ be a maximal ideal of $\overline{\mathbb{Z}}$. Then define the localization of $\overline{\mathbb{Z}}$ at $\mathfrak{p}$ as*

$$\overline{\mathbb{Z}}_{(\mathfrak{p})} = \{a/b : a, b \in \overline{\mathbb{Z}}, b \notin \mathfrak{p}\}.$$

Note that $\overline{\mathbb{Z}}_{(\mathfrak{p})}$ is a subring of $\overline{\mathbb{Q}}$ and the unique maximal ideal of $\overline{\mathbb{Z}}_{(\mathfrak{p})}$ is $\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$. So $\overline{\mathbb{Z}}_{(\mathfrak{p})}/\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$ is a field. Then we can define a natural isomorphism of fields as follows

$$\overline{\mathbb{Z}}/\mathfrak{p} \xrightarrow{\sim} \overline{\mathbb{Z}}_{(\mathfrak{p})}/\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}, \qquad \alpha + \mathfrak{p} \mapsto \alpha + \mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}.$$

Also we can think $\overline{\mathbb{Z}}_{(\mathfrak{p})}/\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$ as $\overline{\mathbb{F}}_p$ since we can write a natural surjection map as

$$\widetilde{\ }: \overline{\mathbb{Z}}_{(\mathfrak{p})} \to \overline{\mathbb{F}}_p, \qquad \widetilde{\alpha} = \alpha + \mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})} \tag{3.6}$$

with the kernel $\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$. We know that $\overline{\mathbb{Z}}/\mathfrak{p}$ is an algebraic closure of $\mathbb{Z}/p\mathbb{Z}$. Since $\overline{\mathbb{Z}}/\mathfrak{p}$ is isomorphic to $\overline{\mathbb{Z}}_{(\mathfrak{p})}/\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$, we can think that $\overline{\mathbb{Z}}_{(\mathfrak{p})}/\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$ is an algebraic closure of $\mathbb{Z}/p\mathbb{Z}$. Also $\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})} \cap \mathbb{Z} = p\mathbb{Z}$. Thus the reduction map $\mathbb{Z} \to \mathbb{F}_p$ in (3.5) extends to the reduction map (3.6).

Now, we can define the reduction of elliptic curves over $\overline{\mathbb{Q}}$. Let E be an elliptic curve given by a Weierstrass equation over $\overline{\mathbb{Q}}$. When we apply the admissible change of variables $(x, y) = (u^2x', u^3y')$, we get another Weierstrass equation corresponding to another elliptic curve E' with coefficients $a_i' = a_i/u^i$. With a suitable choice of $u \in \mathbb{Z}^+$, the coefficients of Weierstrass equation of E' are in $\overline{\mathbb{Z}}_{(\mathfrak{p})}$. So we can define that a Weierstrass equation of E is $\mathfrak{p}$-integral which means that the coefficients of a Weierstrass equation of E lie in $\overline{\mathbb{Z}}_{(\mathfrak{p})}$.

Theorem 3.46. *Let E be an elliptic curve with $\mathfrak{p}$-integral Weierstrass equation over $\overline{\mathbb{Q}}$. When we reduce it to a Weierstrass equation over $\overline{\mathbb{F}}_p$ by the map (3.6), we get*

- *$\widetilde{E}$ as an elliptic curve over $\overline{\mathbb{F}}_p$ if and only if $\widetilde{\Delta} \neq 0$ in which case the curve $\widetilde{E}$ is ordinary if $\widetilde{E}[p] \cong \mathbb{Z}/p\mathbb{Z}$ or the curve is supersingular if $\widetilde{E}[p] = \{0\}$,*
- *$\widetilde{E}$ as a singular curve over $\overline{\mathbb{F}}_p$ with a node if and only if $\widetilde{\Delta} = 0$ and $\widetilde{c}_4 \neq 0$ in which case the curve $\widetilde{E}$ without the singular point forms a multiplicative group which is isomorphic to $\overline{\mathbb{F}}_p{}^*$,*
- *$\widetilde{E}$ as a singular curve over $\overline{\mathbb{F}}_p$ with a cusp if and only if $\widetilde{\Delta} = 0$ and $\widetilde{c}_4 = 0$ in which case the curve $\widetilde{E}$ without the singular point forms an additive group which is isomorphic to $\overline{\mathbb{F}}_p$.*

For proof of Theorem 3.46, see Section 8.4 in [1].

Definition 3.47. *A $\mathfrak{p}$-integral Weierstrass equation over $\overline{\mathbb{Q}}$ with good reduction or multiplicative reduction is called $\mathfrak{p}$-minimal.*

Remark 3.48. *Let E be an elliptic curve over $\overline{\mathbb{Q}}$. Then the reduction type of it at $\mathfrak{p}$ is well-defined as the ordinary, super singular, or multiplicative reduction type for any $\mathfrak{p}$-minimal Weierstrass equation for E. Moreover, if the reduction of it is good, then we get a well-defined elliptic curve $\widetilde{E}$ over $\overline{\mathbb{F}}_p$ up to isomorphism over $\overline{\mathbb{F}}_p$.*

Theorem 3.49. *Let E be an elliptic curve over $\overline{\mathbb{Q}}$ and $\mathfrak{p}$ be a maximal ideal of $\overline{\mathbb{Z}}$. E has good reduction at $\mathfrak{p}$ if and only if $j(E) \in \overline{\mathbb{Z}}_{(p)}$.*

For proof of Theorem 3.49, see page 333 in [1].

Theorem 3.50. *Let E be an elliptic curve over $\overline{\mathbb{Q}}$ with good reduction at $\mathfrak{p}$.*

(i) The reduction map between the groups of N-torsion points of E and $\widetilde{E}$

$$E[N] \to \widetilde{E}[N]$$

is surjective for any N.

(ii) Let C be a cyclic subgroup of E of order p. Then the isogenous image E/C as in (3.23) *has also good reduction at $\mathfrak{p}$. Moreover, if E has ordinary reduction at $\mathfrak{p}$, so does E/C. Also if E has supersingular reduction at $\mathfrak{p}$, so does E/C.*

For proof of Theorem 3.50, see page 335 in [1].

Theorem 3.51. *Let C be a projective algebraic curve over $\mathbb{Q}$ with good reduction at p. Then the reduction map on curve C can be extended on degree-0 divisor groups of C and $\widetilde{C}$ such that*

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

In this map, principal divisors map to principal divisors. So by this map, we can induce a surjection map between Picard group of C and $\widetilde{C}$ as

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

Let C' be a projective algebraic curve over $\mathbb{Q}$ with good reduction at p. Assume that C' has positive genus. Let $h : C \to C'$ be a morphism over $\mathbb{Q}$ and $h_* : Pic^0(C) \to Pic^0(C')$ and $\widetilde{h}_* : Pic^0(\widetilde{C}) \to Pic^0(\widetilde{C}')$ be induced forward maps of h and $\widetilde{h}$. Then we have a

commutative diagram as

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

For proof of Theorem 3.51, see page 344 in [1].

Theorem 3.52. *Let $\phi : E \to E'$ be an isogeny over $\overline{\mathbb{Q}}$ of elliptic curves over $\overline{\mathbb{Q}}$. Then there exits a reduction map*

$$\widetilde{\phi} : \widetilde{E} \to \widetilde{E}'$$

with the properties:

(i) $\widetilde{\phi}$ *is an isogeny,*

(ii) If $\psi : E' \to E''$ *is an isogeny, then* $\widetilde{\psi \circ \phi} = \widetilde{\psi} \circ \widetilde{\phi}$,

(iii) $deg(\widetilde{\phi})=deg(\phi)$,

(iv) The below diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow[\psi]{} & E' \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow[\tilde{\psi}]{} & \widetilde{E'}. \end{array}$$

For proof of Theorem 3.52, see page 345 in [1].

3.6. Abelian Varieties and Jacobians

Definition 3.53. *Let X be a compact Riemann surface. The Jacobian of X is the quotient group*

$$Jac(X) = \Omega^1_{hol}(X)^\wedge / H_1(X, \mathbb{Z})$$

where $H_1(X, \mathbb{Z})$ is the first homology group of X which is a free abelian group containing integer sums of integrations of loops on X and $\Omega^1_{hol}(X)^\wedge$ is the dual space of the degree 1 holomorphic differentials on X. For more details, see Section 6.1 [1].

From now on, we denote $Jac(X_0(N))$ as $J_0(N)$.

Definition 3.54. *Let X be a compact Riemann surface. The divisor group of X is free abelian group such that*

$$Div(X) = \left\{ \sum_{x \in X} n_x x : n_x \in \mathbb{Z}, n_x = 0 \text{ for all but finitely many } x \in X \right\}.$$

The degree-0 divisor group $Div^0(X)$ is a subgroup of Div(X) such that

$$Div^0(X) = \left\{ \sum_{x \in X} n_x x \in Div(X) : \sum_{x \in X} n_x = 0 \right\}.$$

Let f be a meromorphic function as $f : X \to \hat{\mathbb{C}}$. Define a divisor of f as $div(f) = \sum_{x \in X} \nu_x(f)x$ where $\nu_x(f)$ is the order of vanishing of f at x. Let $\mathbb{C}(X)$ be the function field of a compact Riemann surface X. Define the principal divisors which is a subgroup of the degree-0 divisor group as

$$Div^\ell(C) = \{div(f) \in Div^0(X) : \text{ for some } f \in \mathbb{C}(X)\}.$$

Definition 3.55. *The Picard group of X is the quotient group of degree-zero divisors modulo principal divisors on X as $Pic^0(X) = Div^0(X)/Div^\ell(X)$.*

Then we can embed X to $Pic^0(X)$ by the map

$$X \to Pic^0(X), \qquad x \mapsto [x - x_0]$$

where x_0 is a base point in X. So we can define the well-defined map from the degree-0 divisor group to the Jacobian of X as

$$Div^0(X) \to Jac(X), \qquad \sum_{x\in X} n_x x \mapsto \sum_{x\in X} n_x \int_{x_0}^{x} \cdot \tag{3.7}$$

Theorem 3.56 (**Abel's Theorem**). *The map given in* (3.7) *can be extended to the below isomorphism as*

$$Pic^0(X) \to Jac(X), \qquad \left[\sum_{x\in X} n_x x\right] \mapsto \sum_{x\in X} n_x \int_{x_0}^{x} \cdot$$

For more details about Theorem 3.56, see pages 197-198 in [3].

3.7. Hecke Operators

Definition 3.57. *Let Γ_1 and Γ_2 be two congruence subgroups of $SL_2(\mathbb{Z})$. For any $\alpha \in GL_2^+(\mathbb{Q})$, define a double coset in $GL_2^+(\mathbb{Q})$ as*

$$\Gamma_1 \alpha \Gamma_2 = \{\gamma_1 \alpha \gamma_2 : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}.$$

Now, we will define Hecke operators. For the first type Hecke operator, we take $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$ and an arbitrary $\alpha \in \Gamma_0(N)$. Consider for any $f \in M_k(\Gamma_1(N))$,

$$f[\Gamma_1 \alpha \Gamma_2]_k = f[\alpha]_k \in M_k(\Gamma_1(N))$$

So $\Gamma_0(N)$ acts on $M_k(\Gamma_1(N))$ by the action of $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ which is determined by d modulo N and denoted by $\langle d \rangle$. Now, we will define $\langle d \rangle$.

Definition 3.58. *A diamond operator $\langle d \rangle$ is defined as*

$$\langle d \rangle : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N)).$$

such that

$$\langle d \rangle f = f[\alpha]_k \text{ for any } \alpha = \begin{bmatrix} a & b \\ c & \delta \end{bmatrix} \in \Gamma_0(N) \text{ where } \delta \equiv d \text{ (mod N)}.$$

To define the second type of Hecke operator, take again $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$ but $\alpha = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$ where p is prime.

Definition 3.59. *The operator T_p is defined as*

$$T_p : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$$

such that

$$T_p f = f[\Gamma_1 \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \Gamma_2]_k$$

where the double coset is

$$\Gamma_1\alpha\Gamma_2 = \Gamma_1(N)\alpha\Gamma_1(N) = \left\{ \gamma \in M_2(Z) : \gamma \equiv \begin{bmatrix} 1 & * \\ 0 & p \end{bmatrix} \pmod{\text{N}},\ det\gamma = p \right\}.$$

In the next chapter, we will consider the reduction of Hecke operator T_p acting on $Div(S_0(N))$. So we will define T_p for moduli spaces of elliptic curves.

Definition 3.60. *The Hecke operator T_p acts on the moduli spaces of elliptic curves as*

$$T_p : Div(S_0(N)) \to Div(S_0(N)), \qquad T_p[E, C_N] = \sum_C [E/C, (C_N \oplus C)/C] \tag{3.8}$$

where the sum is taken over all order p subgroups C of elliptic curve E such that $C \cap C_N = \{O_E\}$.

Definition 3.61. *Let $f, g \in S_k(\Gamma_0(N))$. The Petersson inner product of f and g is*

$$\langle f, g \rangle = \frac{1}{V_{\Gamma_0(N)}} \int_D f(\tau)\overline{g(\tau)}y^{k-2}dxdy$$

where D is the fundamental domain for $\Gamma_0(N)$, $V_{\Gamma_0(N)} = [SL_2(\mathbb{Z}) : \Gamma_0(N)]$, and $\tau = x + iy \in \mathcal{H}$.

For the definition and more details about fundamental domain, see Section 5.8 in [4].

Definition 3.62. *For any divisor d of N, define the map*

$$i_d : (S_k(\Gamma_0(Nd^{-1})))^2 \to S_k(\Gamma_0(N)), \qquad (f, g) \mapsto f + g[\alpha_d]_k$$

where $\alpha_d = \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix}$. *The subspace of oldforms at level N is*

$$S_k(\Gamma_0(N))^{old} = \sum_{p|N, prime} i_p((S_k(\Gamma_0(Np^{-1})))^2).$$

The orthogonal complement of $S_k(\Gamma_0(N))^{old}$ *with respect to the Peterson inner product is the subspace of newforms* $S_k(\Gamma_0(N))^{new}$ *at level N.*

Definition 3.63. *Let* $f \in M_k(\Gamma_0(N))$ *be a nonzero modular form. If f is an eigenvector of the Hecke operator* T_n *for all* $n \in \mathbb{Z}^+$, *then f is called an eigenform. The eigenform* $f = \sum_{n=0}^{\infty} a_n(f)q^n$ *is called a normalized eigenform if* $a_1(f) = 1$. *The element f of* $S_k(\Gamma_0(N))^{new}$ *is called a newform which is a normalized eigenform.*

Definition 3.64. *Let f be a newform in* $S_2(\Gamma_0(M_f))$. *Then the abelian variety associated to f is*

$$A'_f = J_0(M_f)/I_f J_0(M_f)$$

where I_f *is the kernel of the eigenvalue map*

$$\lambda_f : \mathbb{T}_{\mathbb{Z}} \to \mathbb{C}, \qquad Tf = \lambda_f(T)f \text{ for } T \in \mathbb{T}_{\mathbb{Z}}$$

as $I_f = ker(\lambda_f) = \{T \in \mathbb{T}_{\mathbb{Z}} : Tf = 0\}$ *where* $\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[\{T_n, \langle n \rangle : n \in \mathbb{Z}^+\}]$.

Definition 3.65. *Let* $f \in S_2(\Gamma_0(N))$ *be a normalized eigenform and for all* $n \in \mathbb{Z}^+$, $a_n(f)$ *be a Fourier coefficients of f. Then the field* $\boldsymbol{K}_f = \mathbb{Q}(\{a_n(f)\})$ *is called the number field of f.*

Remark 3.66. *Note that* $a_n(f)$ *is an algebraic integer since it satisfies the characteristic polynomial of* T_p. *So* $\boldsymbol{K}_f$ *is a number field.*

For more details about $\mathbf{K}_f$, see Section 6.5 in [1].

Theorem 3.67. *There exists an isogeny between the Jacobian associated to* $\Gamma_0(N)$ *and the sum of abelian varieties such that*

$$J_0(N) \to \bigoplus_{f,n} A'_f \tag{3.9}$$

where the sum is taken over the set of equivalence classes of newforms $f \in S_2(\Gamma_0(M_f))$ *and divisors* n *of* N/M_f.

For proof of Theorem 3.67, see Theorem 6.6.6 in [1].

Note that the isogeny between abelian varieties is a surjective homomorphism between same dimensional abelian varieties. The definition of dual isogeny between abelian varieties is the same as the definition of an isogeny between elliptic curves where the degree is the extension degree of the function fields of abelian varieties. For more details, see [5].

So there exists a dual isogeny of (3.9) as

$$\bigoplus_{f,n} A'_f \to J_0(N). \tag{3.10}$$

Then for any prime $p \nmid N$, we have a commutative diagram

$$\begin{array}{ccc} \bigoplus_{f,n} A'_f & \xrightarrow{\prod_{f,n} a_p(f)} & \bigoplus_{f,n} A'_f \\ \downarrow & & \downarrow \\ J_0(N) & \xrightarrow{T_p} & J_0(N) \end{array} \tag{3.11}$$

where the maps on the left and right side are dual isogenies in (3.10).

4. MODULARITY THEOREM

4.1. Igusa's Theorem

Definition 4.1. *The restriction of moduli space $S_0(N)_{alg}$ over $\overline{\mathbb{Q}}$ is*

$$S_0(N)'_{gd} = \{[E, C] \in S_0(N)_{alg} : E \text{ has good reduction at } \mathfrak{p}, \widetilde{j(E)} \notin \{0, 1728\}\}$$

where $\mathfrak{p}$ is a maximal ideal of $\overline{\mathbb{Q}}$ lying over prime p with $p \nmid N$ and $\widetilde{j(E)} \in \overline{\mathbb{F}}_p$ is a reduction at $\mathfrak{p}$ of $j(E)$. Note that $\widetilde{j(E)} \in \overline{\mathbb{F}}_p$ is well defined since E has a good reduction at $\mathfrak{p}$ and $j(E) \in \overline{\mathbb{Z}}_{(p)}$.
The moduli space over $\overline{\mathbb{F}}_p$ is denoted by $\widetilde{S}_0(N)$ whose elements are equivalence classes $[E, C]$ where E is an elliptic curve over $\overline{\mathbb{F}}_p$ and C is a subgroup of E or order N. To avoid $j(E) = 0, 1728$, we define

$$\widetilde{S}_0(N)' = \{[E, C] \in \widetilde{S}_0(N) : j(E) \notin \{0, 1728\}\}.$$

Now, we can define the reduction map on moduli spaces. Let $[E, C] \in S_0(N)'_{gd}$ be an equivalence class where C is a cyclic subgroup of E of order N and $j = j(E)$. The reduction map between moduli spaces is

$$S_0(N)'_{gd} \to \widetilde{S}_0(N)', \qquad [E_j, C] \mapsto [\widetilde{E}_j, \widetilde{C}].$$

Let $\psi_{0,N} \in \mathbb{F}_p(j)[x]$ be the minimal polynomial of the sum of the x-coordinates of nonzero points of $\widetilde{C}$. Denote $x(\widetilde{C})$ for the sum of the x-coordinates of nonzero points of $\widetilde{C}$. Define the function field as follows

$$K_0(N) = \mathbb{F}_p(j)[x]/\langle \psi_{0,N}(x) \rangle.$$

Theorem 4.2 (**Igusa's Theorem**). *Let N be a positive integer and p be a prime such that $p \nmid N$. Then the modular curve $X_0(N)$ as an algebraic curve has good reduction at p. There is an isomorphism of function fields between $\overline{\mathbb{F}}_p(\widetilde{X}_0(N))$ and $K_0(N)$. Also the below diagram commutes:*

$$\begin{array}{ccc} S_0(N)'_{gd} & \xrightarrow[\varphi_0]{} & X_0(N) \\ \downarrow & & \downarrow \\ \widetilde{S}_0(N)' & \xrightarrow[\widetilde{\varphi}_0]{} & \widetilde{X}_0(N). \end{array} \tag{4.1}$$

The top row is the map from $[E_j, C]$ to $(j, x(C))$ where $x(C)$ is the sum of x-coordinates of the points of C. The bottom row is a map in characteristic p which is similar to φ_0. The vertical maps are reduction maps of moduli spaces and modular curves.

Proof. Note that $\widetilde{X}_0(N)^{planar}_{alg}$ is the set of elements $(j, x) \in \overline{\mathbb{F}}_p{}^2$ such that $\widetilde{\psi}_0(j, x) = 0$ where $\widetilde{\psi}_0$ is the minimal polynomial of reduction of f_0 in (2.2). So the function field of $\widetilde{X}_0(N)^{planar}_{alg}$ is $\mathbb{F}_p(j)[x]/\langle\widetilde{\psi}_0(x)\rangle$. For any given j, we want to show that $\widetilde{\psi}_0(x)$ and $\psi_{0,N}(x)$ are the same polynomial. Note that

$$f_0(\tau) = \sum_{d=1}^{N-1} f_0^{\bar{d}}(\tau) = \sum_{d=1}^{N-1} f_0^{\overline{(0,d)}}(\tau) = \sum_{d=1}^{N-1} \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau\left(\frac{d}{N}\right) = \frac{g_2(\tau)}{g_3(\tau)} \sum_{d=1}^{N-1} \wp_\tau\left(\frac{d}{N}\right). \tag{4.2}$$

When we consider $S_0(N)_{alg}$, the last summation is equal to the sum of x-coordinates of nonzero points of C where C is a cyclic group of $E_{j(\tau)}$ of order N. If we consider $\widetilde{S}_0(N)_{alg}$, the last summation is $x(\widetilde{C})$. So the polynomials $\widetilde{\psi}_0(x)$ and $\psi_{0,N}(x)$ are the same. Thus $\overline{\mathbb{F}}_p(\widetilde{X}_0(N))$ and $K_0(N)$ are isomomorphic. Let $[E_{j(\tau)}, C] \in S_0(N)'_{gd}$, then $\varphi_0([E_{j(\tau)}, C]) = (j(\tau), x(C))$. If we apply the reduction to $(j(\tau), x(C))$, we get $(\widetilde{j}(\tau), \widetilde{x(C)})$. When we first reduce $[E_{j(\tau)}, C]$ to $[\widetilde{E}_{j(\tau)}, \widetilde{C}]$ and then apply $\widetilde{\varphi}_0$, we get

$\widetilde{\varphi}_0([\widetilde{E}_{j(\tau)}, \widetilde{C}]) = (j(\widetilde{E}_{j(\tau)}), x(\widetilde{C}))$. Note that $\widetilde{x(C)}$ and $x(\widetilde{C})$ are the same since we can apply the reduction by pointwise on C. Since the j-invariant is a rational function of coefficients of Weierstrass equation of E, the reduction of j-invariant is the same as j-invariant of the reduced curve $\widetilde{E}$. Hence the above diagram (4.1) commutes. □

Remark 4.3. *After Theorem 4.2, we have a commutative diagram between degree zero divisors and Picard groups as in Theorem 4.2 such as*

$$\begin{array}{ccc} Div^0(S_0(N)'_{gd}) & \longrightarrow & Pic^0(X_0(N)) \\ \downarrow & & \downarrow \\ Div^0(\widetilde{S}_0(N)') & \longrightarrow & Pic^0(\widetilde{X}_0(N)). \end{array}$$

In this diagram, the maps on the left side and on the bottom of the diagram are surjective.

4.2. The Eichler - Shimura Relation

We defined the Hecke operator T_p on $S_0(N)$ in (3.8) as

$$T_p[E, C_N] = \sum_C [E/C, (C_N \oplus C)/C] \tag{4.3}$$

where C is the order p subgroup of E such that $C \cap C_N = \{O\}$ since $p \nmid N$.

Let E be an elliptic curve over $\overline{\mathbb{Q}}$ with ordinary reduction at $\mathfrak{p}$ and C_N be a cyclic subgroup of E with order N.

Let C_0 be the kernel of the reduction map $\sim$: $E[p] \to \widetilde{E}[p]$. Note that C_0 is a subgroup of E of order p since the reduction map is surjective and the reduction is ordinary.

Lemma 4.4.

$$[\widetilde{E/C}, \widetilde{(C_N \oplus C)/C}] = \begin{cases} [\widetilde{E^{\sigma_p}}, \widetilde{C_N^{\sigma_p}}] & if \quad C = C_0 \\ [\widetilde{E^{\sigma_p^{-1}}}, \widetilde{C_N^{\sigma_p^{-1}}}] & if \quad C \neq C_0 \end{cases}$$

for all p order subgroups C of E.

Proof. **Case 1:** Assume that $C = C_0$. Let $E' = E/C$ and $C' = (C_N \oplus C)/C$. Define the quotient isogeny $\phi : E \to E'$ such that $\phi(C_N) = C'$ and the dual isogeny of it $\psi : E' \to E$. Then it gives us a commutative diagram by Theorem 3.52:

$$\begin{array}{ccc} E'[p] & \xrightarrow[\psi]{} & E[p] \\ \downarrow & & \downarrow \\ \widetilde{E'}[p] & \xrightarrow[\tilde{\psi}]{} & \widetilde{E}[p]. \end{array}$$

By Theorem 3.50, E' has ordinary reduction at $\mathfrak{p}$ since E has ordinary reduction at $\mathfrak{p}$. So $|\widetilde{E'}[p]| = p$. Also $\psi(E'[p])$ is a subgroup of E[p] of order p since $|ker\psi| = deg(\psi) = deg(\phi) = p$. Since $\phi(\psi(E'[p])) = [p](E'[p]) = \{0\}$, $E'[p]$ is a subgroup of $C = ker(\phi)$. Since C and $\psi(E'[p])$ are subgroup of E with order p, $\psi(E'[p]) = C = C_0$ which is the kernel of the reduction map on the right vertical arrow. Since the reduction map on the left vertical arrow is surjective, the map on the bottom arrow is zero map. Thus $\widetilde{E'}[p] \subset ker(\tilde{\psi})$. Also we know that $ker(\tilde{\psi}) \subset ker([p]_{\widetilde{E'}}) = \widetilde{E'}[p]$ since $[p]_{\widetilde{E'}} = \tilde{\psi} \circ \tilde{\phi}$. Thus $\widetilde{E'}[p] = ker(\tilde{\psi})$ and $ker(\tilde{\psi})$ is a group of order p.

By Theorem 3.52, the reduction at $\mathfrak{p}$ preserves the degree of isogeny. Therefore $deg([p]_{\widetilde{E'}}) = p^2$, $deg(\tilde{\psi}) = p$, and $deg(\tilde{\phi}) = p$. Since separable degree of a map is the order of kernel of the map and total degree is the product of the separable and inseparable degrees, $deg_{sep}([p]_{\widetilde{E'}}) = |ker([p]_{\widetilde{E'}})| = |\widetilde{E'}[p]| = |ker(\tilde{\psi})| = p$ and so $deg_{ins}([p]_{\widetilde{E'}}) = p$. Also $deg_{sep}(\tilde{\psi}) = |ker(\tilde{\psi})| = p$ and $deg_{ins}(\tilde{\psi}) = 1$. Since we have $[p]_{\widetilde{E'}} = \tilde{\psi} \circ \tilde{\phi}$ and the

separable and inseparable degrees are multiplicative, $deg_{sep}(\tilde{\phi}) = 1$ and $deg_{ins}(\tilde{\phi}) = p$.

By the general factorization of isogeny defined in Section 3.4, we know that $\tilde{\phi} = \tilde{\phi}_{sep} \circ \sigma_p^e$ with $deg(\tilde{\phi}_{sep}) = deg_{sep}(\tilde{\phi}) = 1$ and $deg_{ins}(\tilde{\phi}) = p^e$. Since $deg_{ins}(\tilde{\phi}) = p$, $\tilde{\phi} = \tilde{\phi}_{sep} \circ \sigma_p$. Since $deg(\tilde{\phi}_{sep}) = 1$, $\tilde{\phi}_{sep}$ is an isomorphism from $\widetilde{E}^{\sigma_p}$ onto $\widetilde{E'}$. Under this isomorphism, $\widetilde{C}_N^{\sigma_p}$ goes to $\widetilde{C'}$. Hence on the enhanced elliptic curves we have the equivalence $[\widetilde{E/C}, \widetilde{(C_N \oplus C)/C}] = [\widetilde{E'}, \widetilde{C'}] = [\widetilde{E}^{\sigma_p}, \widetilde{C}_N^{\sigma_p}]$.

Case 2: Assume that $C \neq C_0$. Let $E' = E/C$ and $C'' = (C_N \oplus C)/C = \phi(C_N)$ where ϕ is the quotient isogeny such that $\phi : E \to E'$ and ψ is the dual isogeny of ϕ. Let $C' = ker(\psi)$ and C_0' be the kernel of the reduction map $E'[p] \to \widetilde{E}'[p]$. Note that C_0' is a subgroup of $E'[p]$ of order p since the reduction map is surjective and $|\widetilde{E}'[p]| = p$.

By Theorem 3.52, we have a commutative diagram:

$$\begin{array}{ccc} E[p] & \xrightarrow{\phi} & E'[p] \\ \downarrow & & \downarrow \\ \widetilde{E}[p] & \xrightarrow{\tilde{\phi}} & \widetilde{E'}[p]. \end{array}$$

Since $C_0 \neq C = ker(\phi)$ and C_0 is a subgroup of $E[p]$ of order p, $\phi(C_0)$ is a subgroup of $E'[p]$ of order p. Note that $\psi(\phi(C_0)) = [p](C_0) = \{0\}$ since C_0 is a subgroup of $E[p]$. It implies that $\phi(C_0) \subset ker(\psi) = C'$. Since $|C'| = |ker(\psi)| = |ker(\phi)| = p$ and $|\psi(C_0)| = p$, $\phi(C_0) = C'$. Also $\phi(C_0) \subset C_0'$ since the above diagram commutes. Thus $\phi(C_0) = C' = C_0'$ since C_0' has an order p.

Then we can apply Case 1 to E', C', and ψ instead of E, C, and ϕ. So we get $\tilde{\psi} = i \circ \sigma_p$ where $i : \widetilde{E'}^{\sigma_p} \to \widetilde{E}$ with $i(\widetilde{C''}^{\sigma_p}) = \widetilde{C_N}$. When we apply ${\sigma_p}^{-1}$ to the coefficients of i, we get $i^{{\sigma_p}^{-1}} : \widetilde{E'} \to \widetilde{E}^{{\sigma_p}^{-1}}$ is an isomorphism with $i^{{\sigma_p}^{-1}}(\widetilde{C'}) = \widetilde{C_N}^{{\sigma_p}^{-1}}$ since inverse

of the Frobenius map σ_p is bijective and preserves the homomorphism property. Thus it gives us an equivalence relation such that $[\widetilde{E/C}, \widetilde{(C_N \oplus C)/C}] = [\widetilde{E}^{\sigma_p{}^{-1}}, \widetilde{C_N}^{\sigma_p{}^{-1}}]$.

□

Since E has $(p+1)$ many subgroups C of order p and one of these subgroups is C_0, we can write

$$\sum_C [\widetilde{E/C}, \widetilde{(C_N \oplus C)/C}] = (\sigma_p + p\sigma_p^{-1})[\widetilde{E}, \widetilde{C_N}]. \tag{4.4}$$

Theorem 4.5 (**Eichler-Shimura Relation**). *Let p be a prime with $p \nmid N$. The below diagram commutes:*

$$\begin{array}{ccc} Pic^0(X_0(N)) & \xrightarrow{T_p} & Pic^0(X_0(N)) \\ \downarrow & & \downarrow \\ Pic^0(\widetilde{X}_0(N)) & \xrightarrow[\sigma_{p,*} + \sigma_p^*]{} & Pic^0(\widetilde{X}_0(N)). \end{array}$$

Proof. We get the following commutative diagram by the Equations (4.3) and (4.4)

$$\begin{array}{ccc} S_0(N)'_{gd} & \xrightarrow{T_p} & Div(S_0(N)'_{gd}) \\ \downarrow & & \downarrow \\ \widetilde{S}_0(N)' & \xrightarrow[\sigma_p + p\sigma_p^{-1}]{} & Div(\widetilde{S}_0(N)'). \end{array}$$

When we extend the Hecke operator T_p to divisor groups of $S_0(N)'_{gd}$ and $\widetilde{S}_0(N)'$

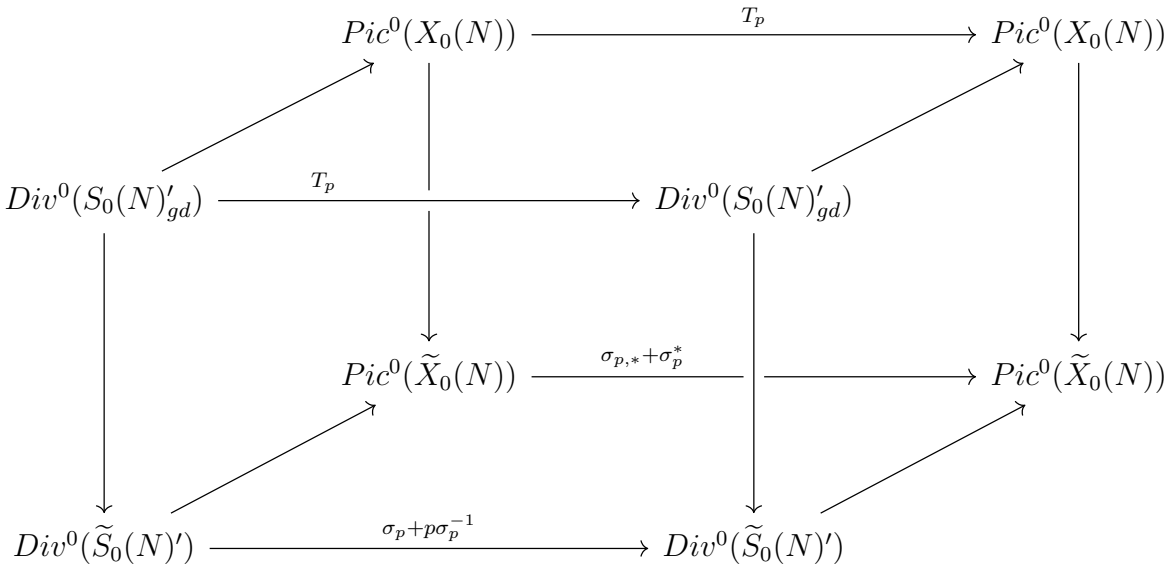
and then restrict to degree-0 divisors, we get the commutative diagram:

$$\begin{array}{ccc} Div^0(S_0(N)'_{gd}) & \xrightarrow{T_p} & Div^0(S_0(N)'_{gd}) \\ \downarrow & & \downarrow \\ Div^0(\widetilde{S}_0(N)') & \xrightarrow{\sigma_p + p\sigma_p^{-1}} & Div^0(\widetilde{S}_0(N)'). \end{array} \tag{4.5}$$

We get the commutative diagram below by Exercise 8.7.2 in [1]:

$$\begin{array}{ccc} Div^0(\widetilde{S}_0(N)') & \xrightarrow{\sigma_p + p\sigma_p^{-1}} & Div^0(\widetilde{S}_0(N)') \\ \downarrow & & \downarrow \\ Pic^0(\widetilde{X}_0(N)) & \xrightarrow{\sigma_{p,*} + \sigma_p^*} & Pic^0(\widetilde{X}_0(N)). \end{array} \tag{4.6}$$

When we construct the following cube-shaped diagram by the above commutative diagrams, all square diagrams except possibly the back diagram commute.



In the above diagram we observe that:

- The bottom square contains maps between moduli spaces and modular curves in characteristic p and it is a commutative diagram, by Diagram (4.6).
- The front square contains reduction map of T_p on the zero divisor groups of moduli space and it is a commutative diagram, by Diagram (4.5).
- The side squares contains the reductions of maps between zero divisors of moduli space and Picard group of modular curve and they are commutative diagrams by Remark 4.3.
- The top square relates T_p between moduli spaces and modular curves in characteristic 0 and it is a commutative diagram. For more details about these diagrams, see Section 7.9 of [1].

We want to show that the back square diagram is also commutative. Consider the maps from the front left corner $Div^0(S_0(N)'_{gd})$ to $Pic^0(\widetilde{X}_0(N))$. First, we will consider the sequence:

$$Div^0(S_0(N)'_{gd}) \longrightarrow Div^0(\widetilde{S}_0(N)') \longrightarrow Pic^0(\widetilde{X}_0(N)) \xrightarrow{\sigma_{p,*}+\sigma_p^*} Pic^0(\widetilde{X}_0(N)). \tag{4.7}$$

By Remark 4.3, we know that the first two maps surject. Since the left side square in the cube-shaped diagram is commutative, we can say that the sequence (4.7) becomes:

$$Div^0(S_0(N)'_{gd}) \longrightarrow Pic^0(X_0(N)) \longrightarrow Pic^0(\widetilde{X}_0(N)) \xrightarrow{\sigma_{p,*}+\sigma_p^*} Pic^0(\widetilde{X}_0(N)). \tag{4.8}$$

Moreover the first two maps in the sequence (4.8) surject. Since the bottom, front, left side, and top square diagrams in the cubed-shaped diagram are commutative, the

sequence (4.8) becomes:

$$Div^0(S_0(N)'_{gd}) \longrightarrow Pic^0(X_0(N)) \xrightarrow{T_p} Pic^0(X_0(N)) \longrightarrow Pic^0(\widetilde{X}_0(N)). \tag{4.9}$$

Let $\widetilde{T}_p$ is the reduction map of T_P on $Pic^0(\widetilde{X}_0(N))$. Then there is a commutative diagram

$$\begin{array}{ccc} Pic^0(X_0(N)) & \xrightarrow[T_p]{} & Pic^0(X_0(N)) \\ \downarrow & & \downarrow \\ Pic^0(\widetilde{X}_0(N)) & \xrightarrow[\widetilde{T}_p]{} & Pic^0(\widetilde{X}_0(N)). \end{array}$$

According to this commutative diagram, the sequence (4.9) becomes

$$Div^0(S_0(N)'_{gd}) \longrightarrow Div^0(\widetilde{S}_0(N)') \longrightarrow Pic^0(\widetilde{X}_0(N)) \xrightarrow{\widetilde{T}_p} Pic^0(\widetilde{X}_0(N)). \tag{4.10}$$

Since (4.7) and (4.10) are equal and the first two maps of these sequences are surjective, $\sigma_{p,*} + \sigma_p^*$ and $\widetilde{T}_p$ are equal. Thus the back square diagram in the cubed-shaped diagram is commutative. □

4.3. Modularity Theorem for $\mathbb{Q}$

In this section, we try to give a proof of the fact that the version X_Q of the Modularity Theorem implies the version a_p of the Modularity Theorem. First, we will state the theorems.

Theorem 4.6 (**Modularity Theorem, Version** X_Q)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then for some N there exists a surjective morphism of curves over $\mathbb{Q}$ from the*

modular curve $X_0(N)_{alg}$ as algebraic curve over $\mathbb{Q}$ to the elliptic curve E,

$$X_0(N)_{alg} \to E.$$

Theorem 4.7 (**Modularity Theorem, Version a_p**)**.** *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Then there exists a newform $f \in S_2(\Gamma_0(N_E))$ such that*

$$a_p(f) = a_p(E) \text{ for all primes } p.$$

Theorem 4.8. *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Let N be a positive integer and*

$$\alpha : X_0(N) \to E \tag{4.11}$$

be a nonzero morphism over $\mathbb{Q}$ of curves over $\mathbb{Q}$. Then there exists a newform $f \in S_2(\Gamma_0(M_f))$ with $M_f|N$ such that

$$a_p(f) = a_p(E) \text{ for all primes } p \nmid N_E N.$$

Proof. In order to use the commutative diagram (3.11) between $\bigoplus_{f,n} A'_f$ and $J_0(N)$, we will work over $\mathbb{C}$. Consider the given map in (4.11)

$$\alpha_{\mathbb{C}} : X_0(N)_{\mathbb{C}} \to E_{\mathbb{C}}$$

between complex algebraic curves. The map over $\mathbb{C}$ surjects since the map over $\mathbb{Q}$ in (4.11) surjects.

Claim. *The diagram*

$$\begin{array}{ccccc} \bigoplus_{f,n} A'_{f,\mathbb{C}} & \xrightarrow{\prod_{f,n}(a_p(f)-a_p(E))} & \bigoplus_{f,n} A'_{f,\mathbb{C}} & & \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi'} & & \\ Pic^0(X_0(N)_{\mathbb{C}}) & \xrightarrow{T_p - a_p(E)} & Pic^0(X_0(N)_{\mathbb{C}}) & \xrightarrow{a_{\mathbb{C},*}} & Pic^0(E_{\mathbb{C}}) \end{array} \tag{4.12}$$

satisfies the properties below for all $p \nmid N_E N$ where $a_{\mathbb{C},*}$ is induced forward map of $\alpha_{\mathbb{C}}$:

(i) if $a_p(f) \neq a_p(E)$, then the map on the top row of diagram surjects,

(ii) the square commutes,

(iii) the composition of the maps on the bottom row of diagram is the zero map.

Proof of the Claim. To prove property (i), assume that $a_p(f) \neq a_p(E)$. Let δ be the difference between $a_p(f)$ and $a_p(E)$. We know that $a_p(E)$ is an integer and $a_p(f)$ is an algebraic integer since it satisfies the characteristic polynomial of T_p. For more details, see Section 6.5 in [1]. Since $\delta \in \overline{\mathbb{Q}}$, δ satisfies a monic polynomial with coefficients in $\mathbb{Z}$. Also $\delta = |a_p(f) - a_p(E)|$ is an algebraic integer. It means that δ satisfies a minimal polynomial with integer coefficients such that for some $e \in \mathbb{Z}^+$

$$\delta^e + a_1\delta^{e-1} + ... + a_{e-1}\delta + a_e = 0, \qquad a_1, ..., a_{e-1}, a_e \in \mathbb{Z} \text{ with } a_e \neq 0.$$

Then we can get $\delta(\delta^{e-1} + a_1\delta^{e-2} + ... + a_{e-1}) = -a_e$. Since the multiplication by $(-a_e)$ map is a nonzero isogeny, it surjects. Then the map δ surjects also. Thus the map $\prod_{f,n}(a_p(f) - a_p(E))$ is also surjective.

We have a commutative diagram (3.11) between $\bigoplus_{f,n} A'_f$ and $J_0(N)$. Also we know that $J_0(N)$ is isomorphic to $Pic^0(X_0(N))$ by Theorem 3.56. Thus the square commutes.

Now, we will prove property (iii). It is enough to show that the map on the bottom row is zero over $\mathbb{Q}$ since we can extend this map over $\mathbb{C}$ as a zero map. Consider the

diagram

$$\begin{array}{ccccc} Pic^0(X_0(N)) & \xrightarrow{T_p - a_p(E)} & Pic^0(X_0(N)) & \xrightarrow{a_*} & Pic^0(E) \\ \downarrow{\scriptstyle \psi} & & \downarrow & & \downarrow{\scriptstyle \psi'} \\ Pic^0(\widetilde{X}_0(N)) & \xrightarrow{\sigma_{p,*} + \sigma_p^* - a_p(E)} & Pic^0(\widetilde{X}_0(N)) & \xrightarrow{\tilde{a}_*} & Pic^0(\widetilde{E}) \\ \downarrow{\scriptstyle 1} & & & & \downarrow{\scriptstyle 1} \\ Pic^0(\widetilde{X}_0(N)) & \xrightarrow{\tilde{a}_*} & Pic^0(\widetilde{E}) & \xrightarrow{\sigma_{p,*} + \sigma_p^* - a_p(E)} & Pic^0(\widetilde{E}). \end{array} \tag{4.13}$$

Note that when we define the composition of maps $T_p - a_p(E)$ and $a_{\mathbb{C},*}$ in (4.12) over $\mathbb{Q}$, we get the composite map which is the same as the composite map on the top row of the diagram (4.13). So we need to show that the top row of the diagram (4.13) is not a surjective map which means that it is a zero map.

By Eichler-Shimura relation, the left top square commutes. Also the right top square commutes by Theorem 3.51. The bottom rectangle commutes since by Theorem 3.35, $\sigma_{p,*}$ and σ_p^* commute with the forward induced map $\tilde{a}_*$ of $\tilde{a}$ and also $\tilde{a}_*$ commutes with the multiplication map by $a_p(E)$. We know that $\sigma_{p,*} + \sigma_p^* - a_p(E)$ is the zero map over $Pic^0(\widetilde{E})$ by Theorem 3.44. So the composite map on the bottom row is zero. Since the bottom rectangle commutes, the composite map on the middle row is also zero. Since the two top squares commute and the map ψ is the reduction map which surjects by Theorem 3.51, the composition of the composite map on the top row and the map ψ' gives us a zero map. But we know that the map ψ' surjects by Theorem 3.51. Thus the composite map on the top row does not surject.

Assume for a contradiction that all newforms $f \in S_2(\Gamma_0(M_f))$ satisfy $a_p(f) \neq a_p(E)$ for some prime $p \nmid N_E N$. Then by (i) in the claim, the map on the top row surjects. Since the map ϕ is a nonzero isogeny as in (3.10), the isogenous image of $\bigoplus_n A'_{f,\mathbb{C}}$ under ϕ lies in $Pic^0(X_0(N)_{\mathbb{C}})$. Then by (ii) in the claim, the diagram commutes. So the isogenous image of $\bigoplus_n A'_{f,\mathbb{C}}$ under ϕ' lies in $Pic^0(X_0(N)_{\mathbb{C}})$ in the middle of bottom row. Also by (iii) in the claim, the isogenous image of $\bigoplus_n A'_{f,\mathbb{C}}$ under

ϕ lies in $ker(a_{\mathbb{C},*})$. Note that two isogenous image of $\bigoplus_n A'_{f,\mathbb{C}}$ are the same since the top row surjects and ϕ and ϕ' is actually the same isogeny. So the map $T_p - a_p(E)$ surjects. Thus by (iii) in the claim, all of $Pic^0(X_0(N)_{\mathbb{C}})$ lies in $ker(a_{\mathbb{C},*})$. But we know that $a_{\mathbb{C},*}$ surjects. Therefore there exists a newform f such that $a_p(f) = a_p(E)$ for all prime $p \nmid N_E N$. □

To show the fact that the version X_Q of the Modularity Theorem implies the version a_p after Theorem 4.8, we need to show that the level of newform f constructed in Theorem 4.8 is N_E and the equality $a_p(f) = a_p(E)$ holds for all prime p. Let σ be an automorphism of $\overline{\mathbb{Q}}$. For all prime p with $p \nmid N$, $a_p(f) = a_p(E)$. Since $a_p(E)$ is an integer, $a_p(f)$ is also integer. Therefore $(a_p(f))^\sigma = a_p(f^\sigma) = a_p(f)$. For more details about this equality, see Section 6.5 in [1]. By Strong Multiplicity One Theorem, $f^\sigma = f$ and so for all prime p, the Fourier coefficients $a_p(f)$ of f are integers. So the number field of f is $\mathbf{K}_f = \mathbb{Q}$. Since $[\mathbf{K}_f : \mathbb{Q}] = 1$, we can think A'_f as an elliptic curve over $\mathbb{Q}$. For more details about this result, see Section 7.7 in [1]. Then we can get a nonzero map $\beta : X_0(N) \to Pic^0(X_0(N)) \to A'_f$ over $\mathbb{Q}$. By Theorem 4.8, there exists a newform $g \in S_2(\Gamma_0(M_g))$ with $M_g | N$ such that $a_p(g) = a_p(A'_f)$ for all primes $p \nmid N_{A'_f} N$. We can write the map β over $\mathbb{C}$ as in the proof of Theorem 4.8, we get $\beta_{\mathbb{C}} : X_0(N)_{\mathbb{C}} \to A'_{f,\mathbb{C}}$. Then the diagram

$$\begin{array}{ccccc} \bigoplus_{g,n} A'_{g,\mathbb{C}} & \xrightarrow{\prod_{g,n}(a_p(g) - a_p(A'_f))} & \bigoplus_{g,n} A'_{g,\mathbb{C}} & & \\ \downarrow & & \downarrow & & \\ Pic^0(X_0(N)_{\mathbb{C}}) & \xrightarrow{T_p - a_p(A'_{f,\mathbb{C}})} & Pic^0(X_0(N)_{\mathbb{C}}) & \xrightarrow{\beta_{\mathbb{C},*}} & Pic^0(A'_{f,\mathbb{C}}) \end{array} \tag{4.14}$$

satisfies the below properties for all $p \nmid N_E N$:

(i) if $a_p(g) \neq a_p(A'_{f,\mathbb{C}})$, then the map on the top row of diagram surjects,

(ii) the square commutes,

(iii) the composition of the maps on the bottom row of diagram is zero map.

By similar reasoning as in the proof of Theorem 4.8, the top row of diagram (4.14) does not surject. So there is a newform in $g \in S_2(\Gamma_0(M_g))$ with $M_g|N$ such as $a_p(g) = a_p(A'_f)$. Note that the sum in $\bigoplus_{g,n} A'_{g,\mathbb{C}}$ is taken over a newform $g \in S_2(\Gamma_0(M_g))$ for all $M_g|N$. Note that the level of f is also divisor of N and so we can consider $g = f$ for the map on the top row of the diagram (4.14), we get the map

$$\psi : A'_{f,\mathbb{C}} \xrightarrow{a_p(f) - a_p(A'_f)} A'_{f,\mathbb{C}}. \tag{4.15}$$

Since $a_p(f)$ and $a_p(A'_f)$ are integers, the map ψ is just a multiplication by $a_p(f) - a_p(A'_f)$ map. Since $a_p(f) = a_p(A'_f) \in \mathbb{Z}$ [6], the map (4.15) does not surject. Thus there exists a newform $f \in S_2(\Gamma_0(M_f))$ with $M_f|N$ such as $a_p(f) = a_p(A'_f)$. Carayol showed in his work [7] that $a_p(f) = a_p(A'_f)$ for all p and the level M_f of f is the conductor N_f of A'_f. Also this work [7] gives us that there exists an isogeny over $\mathbb{Q}$ from A'_f to E with $a_p(A'_f) = a_p(E)$ for all p and the conductor N_E of E is equal to the conductor N_f of A'_f. Hence there exists a newform $f \in S_2(\Gamma_0(N_E))$ such that $a_p(f) = a_p(E)$ for all prime p.

4.4. Modularity Theorem for Real Quadratic Fields

After the Modularity Theorem, the natural question is what happens if the elliptic curve in the Modularity Theorem is defined over a number field instead of $\mathbb{Q}$. There exists a conjecture for elliptic curves over totally real fields. Before we state the conjecture, we define a totally real field.

Definition 4.9. *Let $\boldsymbol{k}$ be a number field. If all embeddings of $\boldsymbol{k}$ in $\mathbb{C}$ are real, $\boldsymbol{k}$ is called totally real field.*

Conjecture 4.10. *Let E be an elliptic curve over totally real field $\boldsymbol{k}$. Then E is modular, i.e there exists a Hilbert eigenform $\mathfrak{f}$ of parallel weight 2 over $\boldsymbol{k}$ such that $L(E, s) = L(\mathfrak{f}, s)$.*

After this conjecture, Le Hung [8] and Freitas-Le Hung-Siksek [9] showed Theorem 4.14 which is a more general case of the Modularity Theorem for elliptic curves over real quadratic number fields. In this thesis, we cannot prove this theorem, but we will try to explain some notions to understand the statement of the theorem.

Let $\mathbf{k}$ be a real quadratic field $\mathbb{Q}(\sqrt{d})$ for any squarefree integer $d > 1$ and $\mathcal{O}_{\mathbf{k}}$ be the ring of integer of $\mathbf{k}$. Now, we will consider $SL_2(\mathbf{k})$ and its action on $\mathcal{H}^2 = \mathcal{H} \times \mathcal{H}$. The action is defined as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \left(\frac{az_1 + b}{cz_1 + d}, \frac{a'z_1 + b'}{c'z_1 + d2} \right)$$

for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{k})$ and $z = (z_1, z_2) \in \mathcal{H}^2$ where x' denotes a Galois conjugate of x for any $x \in \mathbf{k}$.

Definition 4.11. *Let $f : \mathcal{H}^2 \to \mathbb{C}$ be a holomorphic function. If*

$$f(\gamma z) = (cz_1 + d)^{k_1}(c'z_2 + d')^{k_2} f(z) \qquad \text{for all } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma,$$

then f is called a holomorphic Hilbert modular form of weight (k_1, k_2) for Γ. If $k_1 = k_2 = k$, then f is called a Hilbert modular form of parallel weight k.

Definition 4.12. *A holomorphic Hilbert modular form f for Γ is called a cusp form if f vanishes at all points which are Γ-equivalent to ∞. Also these points are called cusps of Γ.*

Definition 4.13. *Let f be a Hilbert modular cusp form. If f is a common eigenvector of Hecke Algebra, then f is called an eigenform.*

In this definition, Hecke algebra is a commutative algebra and self adjoint with respect to the Petersson inner product on the space of all cusp forms. For more detail, see [10].

Theorem 4.14. *Let* $\boldsymbol{k}$ *be a real quadratic number field and E be an elliptic curve over* $\boldsymbol{k}$*. Then E is modular if there exists a Hilbert eigenform* $\mathfrak{f}$ *of parallel weight 2 over* $\boldsymbol{k}$ *such that the Galois representations associated to an elliptic curve E is equivalent to the Galois representations associated to a Hilbert eigenform* $\mathfrak{f}$*.*

Theorem 4.14 explains the notion of modularity in terms of Galois representations. Also there is a version of the Modularity Theorem for elliptic curves over $\mathbb{Q}$ which is stated in terms of the Galois representations. In this thesis, we will not give more details about else versions but interested reader may for more details see Chapter 9 [1].

5. CONCLUSION

In this thesis, we studied the Modularity Theorem for the field of rational numbers $\mathbb{Q}$ and mainly focused on the geometric and the arithmetic versions of the Modularity Theorem. To state the Modularity Theorem, we defined modular forms and modular curves which are main objects of the geometric version of the Modularity Theorem. Then we defined elliptic curves and studied some special properties of them. Also we described abelian varieties associated to an eigenform and Hecke operators to understand Eichler-Shimura relation. Before stating the versions of the Modularity Theorem, we proved Igusa's Theorem and Eichler-Shimura relation for a congruence subgroup $\Gamma_0(N)$. After all definitions and constructions, we stated the versions and showed that the geometric version implies the arithmetic version. After that point, the natural question is "What happens if the elliptic curve in the Modularity Theorem is defined over a number fields instead of the field of rational numbers?". This is an open question for number fields but it is proved by Freitas-Le Hung-Siksek for real quadratic number fields in [9].

REFERENCES

1. Diamond, F. and J. Shurman, *A First Course in Modular Forms*, 2005.

2. Silverman, J. H., *The Arithmetic of Elliptic Curves*, Springer, Springer-Verlag New York, Inc., 1986.

3. Silverman, J. H., *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, Springer-Verlag New York, Inc., 1994.

4. Jones, G. A. and D. Singerman, *Complex Functions, an Algebraic and Geometric Viewpoint*, Cambridge University Press, Cambridge University Press, Cambridge, 1987.

5. Moonen, B., G. van der Geer and B. Edixhoven, *Abelian Varieties*, `https://www.math.ru.nl/%7Ebmoonen/BookAV/Isogs.pdf`, accessed at July 2017.

6. Bruns, G., *The Shimura Construction and The Modularity Theorem*, 2014, `https://www.math.hu-berlin.de/%7Ebrunsgre/notes/2014-shimura.pdf`, accessed at July 2017.

7. Carayol, H., "Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert", pp. 409–468, 1986.

8. Hung, B. V. L., "Modularity of some elliptic curves over totally real fields", *Doctoral dissertation*, 2014, `http://nrs.harvard.edu/urn-3:HUL.InstRepos:12269826`, accessed at July 2017.

9. Freitas, N., B. V. L. Hung and S. Siksek, "Elliptic Curves Over Real Quadratic Fields Are Modular", *Invent. Math.*, 2014,

https://arxiv.org/abs/1310.7088v4, accessed at July 2017.

10. Dembélé, L., *Computing Hilbert Modular Forms Over Real Quadratic Field*, 2006, http://wstein.org/msri06/lassina/MSRI%5FNotes.pdf, accessed at July 2017.

11. Bruinier, J. H., "Hilbert Modular Forms and Their Applications", pp. 105–179, 2008, https://arxiv.org/abs/math/0609763v1, accessed at July 2017.

12. Ribet, K. A. and W. A. Stein, *Lectures on modular forms and Hecke operators*, 2011, http://wstein.org/books/ribet-stein/main.pdf, accessed at July 2017.