Final report: Modularity for CM elliptic curves

Jia Hua Chong

June 15, 2023

0 Introduction

Duering [1] in 1950s proved that the L-function of an elliptic curve E over $\mathbf{Q}$ with complex multiplication coincides with $L(s,\lambda)$ for some grossencharacter λ on the imaginary number field $K = \mathrm{End}_{\mathbf{Q}}(E)$. Later Shimura [6] in 1971 proved the modularity $L(s,\lambda)$ by applying the converse theorem of Weil to show that f_λ is a normalized eigenform, hence proved the modularity of E. He also showed that the abelian variety A_λ decomposed into n-fold product of an elliptic curve whose endomorphism algebra is K.

Theorem I. *Let K be an imaginary quadratic field with $\Delta_K = D,\ \nu \geq 1,\ \lambda \in \Lambda_{\mathfrak{m}}^{\nu}$ a grossencharacter modulo $\mathfrak{m} \subset \mathscr{O}_K$ on K. Set*

$$f_\lambda(z) = \sum_{\xi \subset \mathscr{O}_K,\ (\mathfrak{m},\xi)=1} \lambda(\xi) e^{2\pi i N(\xi) z}.$$

Then

(A) *f_λ is a normalized eigenform in $S_{\nu+1}(D \cdot N(\mathfrak{m}), \varepsilon)$, where $\varepsilon(a) = \left(\frac{D}{a}\right)\frac{\lambda((a))}{a^\nu}$.*

(B) *$A_\lambda := A_{f_\lambda}$ is isogenous to a product of an elliptic curve whose endomorphism algebra is isomorphic K.*

Theorem II. *If E is an elliptic curve over $\mathbf{Q}$ with complex multiplication, then E is isogenous to A_λ, λ is a grossencharacter such that $L(s,E) = L(s,\lambda)$.*

1 Preliminaries

Definition 1.1. An abelian varieties A of dimension n over k has *complex multiplication* (cm) if there exists a ring homomorphism $\iota : K \hookrightarrow \mathrm{End}_{\mathbf{Q}}(A) := \mathrm{End}(A) \otimes \mathbf{Q}$ for some imaginary quadratic field $K = \mathbf{Q}(\sqrt{-D})$ of degree $2n$. Denoted by (A,ι,K) or (A,ι) or A when there is no embiguity.

If $E/\mathbf{C}$ is an elliptic curve, it has cm if and only if $\mathrm{End}(A) \neq \mathbf{Z}$ and in that case, $\iota : K \simeq \mathrm{End}_{\mathbf{Q}}(E)$ is an imaginary quadratic field (c.f. Hartshorne). Indeed, if $E \simeq \mathbf{C}/\Lambda_\tau$ whose endomorphism is larger than $\mathbf{Z}$, then τ is an algebraic number of degree 2 and $\mathbf{Q} \subsetneq \mathrm{End}_Q(A) \subset \mathbf{Q}(\tau)$.

Key Lemma. *Let (A, ι, K) be an abelian variety with cm over $\mathbf{C}$ of dimension n. Suppose that the representation of K on tangent space of X at the origin is equivalent to n copies of the identity injection of K into $\mathbf{C}$. Then A is isogenous to a product of n copies of an elliptic curve E such that $\mathrm{End}_{\mathbf{Q}}(E) \simeq K$.*

Proof. Suppose $X = \mathbf{C}^n/\Lambda$. Let $d\iota : K \to \mathrm{End}_{\mathbf{Q}}(T_eX)$ be the representation of $|iota : K \to \mathrm{End}_{\mathbf{Q}}(X)$ on the tangent space, then by assumption there is a K-equivariant isomorphism

$$T_eX \xrightarrow{\sim} \mathbf{C}^n,$$

let $p : \Lambda_{\mathbf{Q}} \to K^n$ be the restriction, and let $p' : T_eX = \Lambda \otimes_{\mathbf{Q}} \mathbf{R} \xrightarrow{\sim} K^n \otimes_{\mathbf{Q}} \mathbf{R} \simeq \mathbf{C}^n$ the $\mathbf{R}$-linear extension. Since p' is both K-linear and $\mathbf{R}$-linear, hence $\mathbf{C} = K \otimes \mathbf{R}$-linear. Take any rank 2 $\mathscr{O}_K$-submodule $\mathfrak{a} \subset K$, (in fact one can take any nontrivial $\mathscr{O}_K$-submodule) then we obtain an isogeny (over $\mathbf{C}$)

$$(\mathbf{C}/\mathfrak{a})^n \to \mathbf{C}^n/\Lambda.$$

Clearly, $\mathscr{O}_K \subset \mathrm{End}(\mathbf{C}/\mathfrak{a}) \subset K$, so $\mathrm{End}_{\mathbf{Q}}(\mathbf{C}/\mathfrak{a}) = K$. □

Some general facts from class field theory will be assumed without proof:

Definition-Fact. *Let $K/\mathbf{Q}$ be a number field of degree n.*

1. *The ring of integers $\mathscr{O}_K := K \cap \overline{\mathbf{Z}}$ is a dedekind domain, i.e. every nonzero proper ideal uniquely factors into primes, i.e. it is noetherian and the localization at each maximal ideals is PID.*

2. *If $\mathfrak{a}$ is a nonzero integral ideal, $N(\mathfrak{a}) := |\mathscr{O}_K/\mathfrak{a}|$. N is multiplicative, hence defined a norm on $I(1)$.*

3. *Let $\mathfrak{m}$ be an integral ideal, denoted by $I(\mathfrak{m})$ the set of all nonzero fractional ideals coprime to $\mathfrak{m}$, $P(\mathfrak{m})$ the set of ideals (a) with $a \in K$, $a \equiv 1 \ mod^{\times}\mathfrak{m}$, i.e. $a = b/c$ with $b, c \in \mathscr{O}_K$, $(b, \mathfrak{m}) = (c, \mathfrak{m}) = 1$ and $b \equiv c \ mod\ \mathfrak{m}$. $I(\mathfrak{m})$ is a group under ideals multiplication, $P(\mathfrak{m})$ is a subgroup and $I(\mathfrak{m})/P(\mathfrak{m})$ is a finite group. Put $I = I(1)$, $P = P(1)$.*

4. *The different ideal $\mathfrak{d}$ is defined to be $\{a \in K : \mathrm{tr}(ay) \in \mathbf{Z}\ \forall y \in \mathscr{O}\}$ where $\mathrm{tr} := \mathrm{tr}_{\mathbf{Q}}^{K}$, it defines a nondegenerate bilinear form on $K/\mathbf{Q}$. Note that $\mathrm{tr}(\mathscr{O}, \mathscr{O}) \subset \mathscr{O} \cap \mathbf{Q} \subset \mathbf{Z}$, so $\mathscr{O} \subset \mathfrak{d}$, thus $\mathfrak{d}^{-1}$ is integral.*

If K is a quadratic field with discriminant D, then

1. $\mathscr{O}_K = \mathbf{Z}[(D + \sqrt{D})/2]$,

2. *for all rational primes p,* $p\mathscr{O}_K = \begin{cases} \mathfrak{p}\mathfrak{q} & \text{if } (D/p) = 1, \\ \mathfrak{p} & \text{if } (D/p) = -1, \\ \mathfrak{p}^2 & \text{if } (D/p) = 0. \end{cases}$,

3. *for nonzero $a \in K = \mathbf{Q}(\sqrt{D})$, $N((a)) = |a|^2$, where $|\cdot|$ takes absolute value on $\mathbf{C}$.*

Definition 1.2 (Grossencharacter)**.** Let K be an imaginary quadratic field, $\mathfrak{m} \subset \mathscr{O}_K$ be an integral ideal, a grossencharacter modulo $\mathfrak{m}$ is a character $\lambda : I(\mathfrak{m}) \to \mathbf{C}^*$ and for some $\nu \in \mathbf{N}_0$, $\lambda((a)) = a^{\nu}$, let $\Lambda_{\mathfrak{m}}^{\nu}$ denote the set of those. The conductor of $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$ is the minimal divisor $\mathfrak{c}|\mathfrak{m}$ such that λ is the restriction of some $\mu \in \Lambda_{\mathfrak{n}}^{\nu}$. $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$ is called primitive if $\mathfrak{n} = \mathfrak{m}$.

By setting $\lambda(\mathfrak{q}) = 0$ for $(\mathfrak{q}, \mathfrak{m}) \neq 1$, λ can be lifted to $\Lambda_{(1)}^{\nu}$, hence $\Lambda_{\mathfrak{n}}^{\nu} \to \Lambda_{\mathfrak{m}}^{\nu}$ for $\mathfrak{n}|\mathfrak{m}$. Note that if $\Lambda_{\mathfrak{m}}^{\nu} \neq \emptyset$, then it has length $[I(\mathfrak{m}) : P(\mathfrak{m})]$. To see this, take $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$, then $\dfrac{1}{\lambda}\Lambda_{\mathfrak{m}}^{\nu}$ consists of all characters $I(\mathfrak{m})/P(\mathfrak{m}) \to \mathbf{C}^*$, there will be $|I(\mathfrak{m}) : P(\mathfrak{m})|$ of such.

Grossencharacters play a vital role in the studies of cm elliptic curves.

2 L-function of a grossencharacter

Definition 2.1. For $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$, set $L(s,\lambda) = \sum_{\xi} \lambda(\xi) N(\xi)^{-s}$, $f_\lambda(z) = \sum_{\xi} \lambda(\xi) q^{N(\xi)}$, $q = e^{2\pi i z}$ where each sum is taken over all integral ideals ξ in $I(\mathfrak{m})$.

Note that $L(s,\lambda)$ is holomorphic for $\mathrm{Re}(s) > \nu/2+1$. Let $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$, then $\lambda_f : (\mathscr{O}/\mathfrak{m})^* \times \to \mathbf{C}^*$, $a \mapsto \lambda((a))/a^{\nu}$ defines a character, called the finite part. Since $(\mathscr{O}/\mathfrak{m})^*$ is a fintie abelian group, we have gauss sum in hand to obtain the functional equation of a L-function associated to a character on it. However λ cannot be recovered from its finite part, because an ideal of a number field is not principal in general. To make it a character on a finite abelian group while keeping the information, we have to enlarge the space ”to make the ideals principal,” that is, to associate each ideal a number that is determined up to a unit in $\mathscr{O}^*$.

This section will end up with a proof of the following theorem using the converse theorem of Weil.

Theorem 2.1 (Hecke). *Let $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$ be a primitive grossencharacter, put*

$$\Lambda(s,\lambda) = (\sqrt{D \cdot N(\mathfrak{m})}/2\pi)^{s-\nu/2}\Gamma(s)L(s,\lambda).$$

Then Λ satisfies the functional equation

$$\Lambda(\nu+1-s,\lambda) = T(\lambda)\Lambda(s,\overline{\lambda})$$

where

$$T(\lambda) = i^{-\nu} g(\lambda)/N(\mathfrak{m})^{1/2}.$$

Thoughout this section, $K/\mathbf{Q}$ denotes a number field of degree n.

Definition 2.2 (Gauss sum). Let χ be a character of $(\mathscr{O}/\mathfrak{m})^*$ and $y \in \mathfrak{m}^{-1}\mathfrak{d}^{-1}$. We define the Gauss sum of χ to be

$$g(\chi,y) = \sum_{x \in (\mathscr{O}/\mathfrak{m})^*} \chi(x) e^{2\pi i\, \mathrm{tr}(xy)}.$$

Fact 1. *Let $\chi : (\mathscr{O}/\mathfrak{m})^* \to \mathbf{C}^*$ be a primitive character, $y \in \mathfrak{m}^{-1}\mathfrak{d}^{-1}$, $a \in \mathscr{O}$, then*

$$g(\chi,ay) = \begin{cases} \overline{\chi}(a) g(\chi,y), & \textit{if } (a,\mathfrak{m}) = 1, \\ 0, & \textit{else.} \end{cases}$$

Definition 2.3. Let $K/\mathbf{Q}$ be a number field of degree n, $X = \mathrm{Hom}(K,\mathbf{C})$.

1. $\tau \in \mathrm{Hom}(K,\mathbf{C})$ is real if $\tau(K) \subset \mathbf{R}$, and is complex otherwise.
2. $K_{\mathbf{C}} := \prod_{\tau \in X} \mathbf{C} \simeq \mathbf{C}^n$, let $\langle\ ,\ \rangle$ be the canonical inner product. For $z = (z_\tau)_\tau \in K_{\mathbf{C}}$, set $\overline{z} \in K_{\mathbf{C}}$ such that $(\overline{z})_\tau = \overline{z}_{\overline{\tau}}$. The involution z^* is defined to be $(z^*)_\tau = \overline{z}_\tau$.
3. Define the *Minkowski space* $K_{\mathbf{R}}$ to be $\{z \in K_{\mathbf{C}} : \overline{z} = z\}$. There is a natural inclusion $K \hookrightarrow K_{\mathbf{R}} \subset K_{\mathbf{C}}$ defined by $z \mapsto (\tau(z))_\tau$.
4. Define $(K_{\mathbf{R}})_+^*$ by $\{x \in K_{\mathbf{R}} : x = x^*,\ x_\tau > 0\ \forall \tau\}$ and the absolute value $|\ | : (K_{\mathbf{R}})^* \to (K_{\mathbf{R}})_+^*$ by $x \mapsto (|x_\tau|)_\tau$.

5. The trace map $\mathrm{tr}: K_{\mathbf{C}} \to \mathbf{C}$ is defined to be $z \mapsto \sum_{\tau} z_\tau$, while the norm map $N: K_{\mathbf{C}}^* \to \mathbf{C}^*$ is defined to be $z \mapsto \prod_{\tau} z_\tau$. When restricted to K, the trace and norm map are the usual ones.

6. $K_{\mathbf{C}}$ equipped with the canonical hermitian product $\langle (x_\tau), (y_\tau) \rangle = \sum_{\tau} x_\tau \bar{y}_\tau$, which restricted to an inner product on $K_{\mathbf{R}}$.

7. An ideal $\mathfrak{a} \subset K$ can be regarded as a lattice on the euclidean space $(K_{\mathbf{R}}, \langle\ ,\ \rangle)$, the dual lattice is denoted by $\mathfrak{a}'$. One can show that $(\mathfrak{a}')^* = (\mathfrak{a}\mathfrak{d})^{-1}$ and the volume $\mathrm{vol}(\mathfrak{a}) = N(\mathfrak{a})\sqrt{D}$.

If K is an imaginary quadratic field, then $X = \{\mathrm{id},\ \rho\}$, $K_{\mathbf{C}} = \mathbf{C}^2$, $K_{\mathbf{R}} = \{(z, \bar{z} : z \in \mathbf{C})\}$, the inclusion is $K \hookrightarrow K_{\mathbf{R}},\ z \mapsto (z, \bar{z})$.

Proposition 2.1. *There is a subgroup $\hat{K}^* \subset K_C^*$ containing K^* and a group homomorphism $(\ ): \hat{K}^* \to I$ such that there is a commutative exact diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathscr{O}^* & \longrightarrow & K^* & \xrightarrow{(\ )} & P & \longrightarrow & 1 \\ & & \big\downarrow{\scriptstyle id} & & \big\downarrow & & \big\downarrow & & \\ 1 & \longrightarrow & \mathscr{O}* & \longrightarrow & \hat{K}^* & \xrightarrow{(\ )} & I & \longrightarrow & 1 \end{array}$$

and

$$N((a)) = |N(a)|.$$

Proof. See [4], p. 485 □

Consequently, there is an exact sequence $1 \to K^* \to \hat{K}^* \xrightarrow{(\ )} I/P \to 1$.

The elements of $\hat{K}^*$ are called the ideal numbers. Let $\hat{\mathscr{O}}$ denote the set $\{a \in \hat{K}^* : (a) \subset \mathscr{O}_K\}$, an element in $\hat{\mathscr{O}}$ called an ideal integer. For $a, b \in \hat{K}^*$, write $a \sim b$ if $ab^{-1} \in K^*$, i.e. $(a)/(b) \in P$. For $a, b, m \in \hat{K}^*$, write

$$a \equiv b(m)$$

if $a \sim b$ and $\frac{a-b}{m} \in \hat{\mathscr{O}} \cup \{0\}$, if $\mathfrak{m} = (m)$ is an ideal, write $a \equiv b(\mathfrak{m})$. For an integral ideal $\mathfrak{m}$, denote by $\hat{\mathscr{O}}^{(\mathfrak{m})}$ the set of all ideal integers coprime to $\mathfrak{m}$, that is, $a \in \hat{\mathscr{O}}^*$ such that $((a) + \mathfrak{m}) = 1_{I/P}$.

Lemma 2.1. *For every $a \in \hat{\mathscr{O}}^{(\mathfrak{m})}$ one has*

$$a \bmod \mathfrak{m} = a + a(a^{-1})\mathfrak{m}.$$

We now consider the set

$$(\hat{\mathscr{O}}/\mathfrak{m})^* = \hat{\mathscr{O}}^{(\mathfrak{m})} / \equiv_{\mathfrak{m}}.$$

Proposition 2.2. *$(\hat{\mathscr{O}}/\mathfrak{m})^*$ is an abelian group, and we have a canonical exact sequence*

$$1 \to (\mathscr{O}/\mathfrak{m})^* \to (\hat{\mathscr{O}}/\mathfrak{m})^* \to I/P \to 1.$$

Sketch of proof. For $\overline{a}, \overline{b} \in (\hat{\mathscr{O}}/\mathfrak{m})^*$, $\overline{a} \cdot \overline{b} := \overline{ab}$ is well-defined. Since $(a) + \mathfrak{m} = \mathscr{O}$, $\exists \mu \in \mathfrak{m}$, $\alpha \in (a)$ such that $\alpha + \mu = 1$, then $x := \alpha/a \in \hat{\mathscr{O}}$ and $\overline{xa} = 1$. The surjectivity of $(\ ): (\hat{\mathscr{O}}/\mathfrak{m})^* \to I/P$ follows from the fact that every class contains an integral ideal that is coprime to $\mathfrak{m}$. the exactness of the other parts are trivial. □

We now study the character $\chi : (\hat{\mathscr{O}}/\mathfrak{m})^* \to \mathbf{C}^*$ and put $\chi(a) = 0$ for $a \in \mathscr{O}$ such that $(a, \mathfrak{m}) \neq 1$. For a grossencharacter $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$, we define a $\hat{\lambda}_f : (\hat{\mathscr{O}}/\mathfrak{m})^* \to \mathbf{C}^*$ by $a \mapsto \lambda((a))/N(a^{\nu})$. In the application, χ will come from a grossencharacter, but the following treatments of the theory are independent of the origin of χ. Fix $m, d \in \hat{K}^*$ such that $\mathfrak{m} = (m)$, $\mathfrak{d} = (d)$. For a class $\in J/P$, define $\mathfrak{a}' = \mathfrak{m}\mathfrak{d}/\mathfrak{a}$.

Definition-Proposition. *(Gauss sum again) Let $\chi : (\hat{\mathscr{O}}/\mathfrak{m})^* \to \mathbf{C}^*$ be a character, $\mathfrak{a} \in I/P$ be a class. For $a \in \hat{\mathscr{O}} \cap \mathfrak{a} := \{a \in \hat{\mathscr{O}} : (a) \in \mathfrak{a}\}$, we define the Gauss sum to be*

$$\hat{g}(\chi, a) = \sum_{x \in (\hat{\mathscr{O}}/\mathfrak{m})^*,\ (x) \in \mathfrak{a}'} \chi(x) e^{2\pi i \operatorname{tr}(xa/md)},\ \hat{g}(\chi) := \hat{g}(\chi, 1).$$

Then for primitive χ, one has

$$\hat{g}(\chi, a) = \overline{\chi}(a) \hat{g}(\chi)$$

For $x \neq x' \in \hat{\mathscr{O}}^{(\mathfrak{m})}$ such that $x \equiv x'(\mathfrak{m})$, we have $x/x' - 1 \in K^*$, then $((x'a/md)(x/x'-1)) = (x'a/md) = \mathfrak{a}'\mathfrak{a}/\mathfrak{m}\mathfrak{d} = 1$, i.e. $\dfrac{a(x-x')}{md} \in K^*$, and since $\dfrac{x-x'}{m} \in \hat{\mathscr{O}}$, $\dfrac{a(x-x')}{md} \in ((x-x')a/md) \subset \mathfrak{d}^{-1}$, then $\operatorname{tr}((x-x')a/md) \in \mathbf{Z}$, i.e. the sum is well-defined.

Proof. Fix $x \in (\hat{\mathscr{O}}/\mathfrak{m})^*$ such that $(x) = \mathfrak{a}'$, let $y = xa/md$. Since $(y) = 1$, we have $y \in K^*$, so $y \in (y) = (ax)\mathfrak{m}^{-1}\mathfrak{d}^{-1} \subset \mathfrak{m}^{-1}\mathfrak{d}^{-1}$. From the exact sequence $1 \to (\mathscr{O}/\mathfrak{m})^* \to (\hat{\mathscr{O}}/\mathfrak{m})^* \to I/P \to 1$, we see that

$$\{x' \in (\hat{\mathscr{O}}/\mathfrak{m})^* : (x) = \mathfrak{a}'\} = x(\mathscr{O}/\mathfrak{m})^*.$$

Hence

$$\hat{g}(\chi, a) = \chi(x) g(\chi, xa/md),$$

on the otherhand, if $(a, \mathfrak{m}) = 1$,

$$\hat{g}(\chi, 1) = \chi(ax) g(\chi, xa/md),$$

hence

$$\hat{g}(\chi, a) = \overline{\chi}(a) \hat{g}(\chi).$$

Suppose $(a, \mathfrak{m}) = \mathfrak{m}' \neq 1$. Assuming primitivity, then we can find $b \in (\mathscr{O}/\mathfrak{m})^*$ such that

$$\chi(b) \neq 1 \text{ and } b \equiv 1(\mathfrak{m}/\mathfrak{m}').$$

As a consequence, $ab \equiv a(\mathfrak{m})$, so $\hat{g}(\chi, a) = \hat{g}(\chi, ba) = \overline{\chi}(b)\hat{g}(\chi, a)$, hence $\hat{g}(\chi, a) = 0 = \overline{\chi}(a)\hat{g}(\chi)$ still, in this case. □

2.1 Hecke theta function

Now we can define Hecke theta function for a character $\chi : (\hat{\mathscr{O}}/\mathfrak{m})^* \to \mathbf{C}^*$ and prove the functional equation. If $\chi = \hat{\lambda}_f$ for some primitive grossencharacter λ, the Mellin transform is exactly the L-function of λ, hence the functional equation of $L(s, \lambda)$ obtained.

Definition 2.4. Let χ be a character of $(\hat{\mathscr{O}}/\mathfrak{m})^*$, $p \in \prod_{\tau} \mathbf{Z}$ such that $p_\tau \geq 0$. Define the *Hecke theta series*

$$\vartheta^p(\chi, z) = \sum_{a \in \hat{\mathscr{O}} \cup \{0\}} \chi(a) N(a^p) e^{\pi i \langle az/|md|, a\rangle}.$$

For $\mathfrak{a} \in I/P$,

$$\vartheta^p_{\mathfrak{a}}(\chi, z) = \sum_{a \in \hat{\mathscr{O}} \cap \mathfrak{a} \cup \{0\}} \chi(a) N(a^p) e^{\pi i \langle az/|md|, a\rangle}.$$

It is easy to see that $\vartheta^p(\chi,z) = \sum_{\mathfrak{a}\in I/P} \vartheta^p_{\mathfrak{a}}(\chi,z)$. Note that

$$\vartheta^p_{\mathfrak{a}}(\chi,z) = \sum_{b\in\mathfrak{a}\cap\hat{\mathscr{O}}^{(\mathfrak{m})}} \cdots$$

and if $\mathfrak{a} = (a)$, from the exact sequence

$$1 \to (\mathscr{O}/\mathfrak{m})^* \to (\hat{\mathscr{O}}/\mathfrak{m})^* \to I/P \to 1,$$

$$\mathfrak{a}\cap\hat{\mathscr{O}}^{(\mathfrak{m})} = \cup_{a\in(\mathscr{O}/\mathfrak{m})^*}\{a(x+\mathfrak{a}^{-1}\mathfrak{m})\},$$

this gives

$$\vartheta^p_{\mathfrak{a}}(\chi,z) = \chi(a)N(a^p)\sum_{x\in(\mathscr{O}/\mathfrak{m})^*}\chi(x)\sum_{g\in\Gamma}N((x+g)^p)e^{\pi i\langle (x+g)z|a^2/md|,x+g\rangle}, \tag{1}$$

where $\Gamma = \mathfrak{a}^{-1}\mathfrak{m}\subset K_{\mathbf{R}}$ regarded as a lattice. Thus

$$\sum_{g\in\Gamma}N((x+g)^p)e^{\pi i\langle (x+g)z|a^2/md|,x+g\rangle}$$

is the Poisson summation of the Schwartz function $f_p(x) = N(x^p)e^{-\pi\langle x,x\rangle}$ shifted by a, followed by scalar multiplication. A standard calculation shows that the Fourier transform of f_p is

$$\hat{f}_p(y) = i^{-\operatorname{tr}(p)}f_p(y).$$

Let $\vartheta^p_\Gamma(a,b,z) = \sum_{g\in\Gamma}N((a+g)^p)e^{\pi\langle (a+g)z,a+g\rangle+2\pi i\langle b,g\rangle}$. In order to obtain the functional equation, we need

Lemma 2.2 (Theta transformation formula)**.** *For $a,b\in K_{\mathbf{R}}$,*

$$\vartheta_\Gamma(a,b,-1/z) = i^{-\operatorname{tr}(p)}e^{-2\pi i\langle a,b\rangle}\operatorname{vol}(\Gamma)^{-1}N((z/i)^{p+1/2})\vartheta^p_{\Gamma'}(-b,a,z).$$

Proof. Since functions on both sides are holomorphic, therefore it suffices to check the identity for $z = i/t^2$ with $t\in K_{\mathbf{R}}$, $t\geq 0$, i.e. to show that

$$\vartheta_\Gamma(a,b,it^2) = i^{-\operatorname{tr}(p)}e^{-2\pi i\langle a,b\rangle}\operatorname{vol}(\Gamma)^{-1}N(t^{-2p-1})\vartheta^p_{\Gamma'}(-b,a,i/t^2).$$

Note that $\vartheta_\Gamma(a,b,it^2) = N(t^{-p})\sum_{g\in\Gamma}f_p((a+g)t)e^{2\pi i\langle b,g\rangle}$, by Poisson summation formula,

$$\begin{aligned}
\vartheta_\Gamma(a,b,it^2) &= N(t^{-p})\operatorname{vol}(\Gamma)^{-1}\sum_{g\in\Gamma'}\widehat{z\mapsto f_p((a+z)t)}(g-b)\\
&= N(t^{-p-1})\operatorname{vol}(\Gamma)^{-1}\sum_{g\in\Gamma'}\widehat{f}((g-b)/t)e^{2\pi i\langle a,g\rangle}\\
&= N(t^{-p-1})\operatorname{vol}(\Gamma)^{-1}\sum_{g\in\Gamma'}i^{-\operatorname{tr}(p)}f_p((g-b)/t)e^{2\pi i\langle a,g\rangle}\\
&= i^{-\operatorname{tr}(p)}e^{-2\pi i\langle a,b\rangle}\operatorname{vol}(\Gamma)^{-1}N(t^{-2p-1})\vartheta^p_{\Gamma'}(-b,a,i/t^2).
\end{aligned}$$

□

Corollary 2.1. *For a primitive character* χ *of* $(\hat{\mathscr{O}}/\mathfrak{m})^*$, *one has the transformation formula*

$$\vartheta^p_{\mathfrak{a}}(\chi,-1/z) = W(\chi,\overline{p})N((z/i)^{p+1/2})\vartheta_{\mathfrak{a}'}$$

with constant factor

$$W(\chi,\overline{p}) = i^{-\operatorname{tr}(p)}N((md/|md|)^{\overline{p}})^{-1}g(\chi)/\sqrt{N(\mathfrak{m})}.$$

Hence the Hecke theta series has functional equation

$$\vartheta^p(\chi,-1/z) = W(\chi,\overline{p})N((z/i)^{p+1/2})\vartheta^{\overline{p}}(\overline{\chi},z)$$

Proof. Let $\Gamma = \mathfrak{m}/\mathfrak{a}$, recall from *Equation* 1 that

$$\vartheta^p_{\mathfrak{a}}(\chi,z) = \chi(a)N(a^p)\sum_{x\in(\mathscr{O}/\mathfrak{m})^*}\chi(x)\vartheta^p_{\Gamma}(x,0,z|a^2/md|),$$

and $\operatorname{vol}(\mathfrak{a}) = N(\mathfrak{m}/\mathfrak{a})\sqrt{D} = N(|m/a|)N(|d|)^{1/2}$, then by the transformation formula,

$$\vartheta^p_{\Gamma}(x,0,-1/|md/a^2|z) = A(z)\vartheta^p_{\Gamma'}(0,x,z|md/a^2|)$$

with the factor

$$A(z) = i^{-\operatorname{tr}(p)}\sqrt{N(\mathfrak{m})}^{-1}N(|md/a^2|^p)N((z/i)^{p+1/2}).$$

Since $\mathfrak{a}(\mathfrak{m}\mathfrak{d})^{-1}\subset K^*$,

$$md/a\cdot(\mathfrak{m}/\mathfrak{a})* = md/a\cdot\mathfrak{a}(\mathfrak{m}\mathfrak{d})^{-1} = \mathfrak{a}'\cap\hat{\mathscr{O}}\cup\{0\},$$

$$\begin{aligned}
\vartheta^p_{\Gamma'}(0,x,z|md/a^2|) &= \sum_{g\in\Gamma'}N(g^p)e^{2\pi i\langle x,g\rangle}e^{\pi i\langle gz|md/a^2|,g\rangle}\\
&= N((a/md)^{\overline{p}})\sum_{g\in\mathfrak{a}'\cap\hat{\mathscr{O}}\cup\{0\}}N(g^{\overline{p}})e^{2\pi i\langle x,g^*/(md/a)^*\rangle}e^{\pi i\langle g^*z|md/a^2|/(md/a^*),g^*/(md/a)^*\rangle}\\
&= N((a/md)^{\overline{p}})\sum_{y\in\mathfrak{a}'\cap\hat{\mathscr{O}}\cup\{0\}}N(y^{\overline{p}})e^{2\pi i\operatorname{tr}(axy/md)}e^{\pi i\operatorname{tr}(yz/|md|,y)}
\end{aligned}$$

Now

$$\begin{aligned}
\vartheta_{\mathfrak{a}}(\chi,-1/z) &= N(a^p)\sum_{x\in(\mathscr{O}/\mathfrak{m})^*}\chi(ax)\vartheta^p_{\Gamma}(x,0,-1/|md/a^2|z)\\
&= A(z)N(a^p)N((a/md)^{\overline{p}})\sum_{y\in\mathfrak{a}'\cap\hat{\mathscr{O}}\cup\{0\}}\left(\sum_{x\in(\mathscr{O}/\mathfrak{m})^*}\chi(xa)e^{2\pi i\operatorname{tr}(axy/md)}\right)N(y^{\overline{p}})e^{\pi i\langle yz/|md,y\rangle}\\
&= A(z)N(a^p)N((a/md)^{\overline{p}})\sum_{y\in\mathfrak{a}'\cap\hat{\mathscr{O}}\cup\{0\}}g(\chi,y)N(y^{\overline{p}})e^{\pi i\langle yz/|md,y\rangle}\\
&= A(z)N(a^p)N((a/md)^{\overline{p}})\sum_{y\in\mathfrak{a}'\cap\hat{\mathscr{O}}\cup\{0\}}g(\chi)\overline{\chi}(y)N(y^{\overline{p}})e^{\pi i\langle yz/|md,y\rangle}\\
&= W(\chi,\overline{p})N((z/i))\vartheta^{\overline{p}}_{\mathfrak{a}'}(\overline{\chi},z).
\end{aligned}$$

□

For a character $\psi : \mathbf{Z}/p^* \to \mathbf{C}^*$, $\widetilde{\psi} := \psi \circ N : \mathscr{O}/p\mathscr{O}^* \to \mathbf{C}^*$ defines a primitive character. If $(p,\mathfrak{m}) = 1$, then $\lambda_f \widetilde{\psi}_\chi : \mathscr{O}/p\mathfrak{m}\mathscr{O}^* \to \mathbf{C}^*$ defines a primitive character. If $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$ is a grossencharacter, denote by $\hat{\lambda}_f : (\hat{\mathscr{O}}/\mathfrak{m})^* \to \mathbf{C}^*$ the finite part. For a function $f = \sum_n a_n q^n$, let

$$\Lambda_M(s,f) = (2\pi/\sqrt{M})^{-s}\Gamma(s)L(s,f),$$

if $\chi : \mathbf{Z}/r^* \to \mathbf{C}^*$ is a character, let

$$\Lambda_M(s,f,\psi) = (2\pi/r\sqrt{M})^{-s}\Gamma(s)L(s,f,\psi)$$

where

$$L(s,f,\psi) = \sum_n a_n \psi(n) n^{-s},$$

as defined in the statement of the converse theorem of Weil.

2.2 Functional equation and modularity

Proposition 2.3. *Suppose $K = \mathbf{Q}(\sqrt{-D})$, let $M = N(\mathfrak{m})D$, r be a prime such that $(r,M) = 1$, $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$ be a primitive grossencharacter, $\psi : \mathbf{Z}/r^* \to \mathbf{C}^*$ a character. Then*

$$\Lambda_M(\nu+1-s, f_{\overline{\lambda}};, \overline{\psi}) = T(\psi)\Lambda_M(s, f_\lambda, \psi)$$

where

$$T(\psi) = Ci^{-\nu}\lambda_f(p)\psi(M)\frac{g(\psi)}{g(\overline{\psi})}\frac{g(\hat{\lambda}_f)}{\sqrt{N(\mathfrak{m})}}$$

for some contant C depends only on $\mathfrak{m}$

Proof. In this case $K_{\mathbf{C}} = \mathbf{C}\times\mathbf{C}$, $K_{\mathbf{R}} = \{(z,\bar{z}), z \in \mathbf{C}\}$. Set $p = (\nu,0), \chi = \hat{\lambda}_f\hat{\psi} : (\hat{\mathscr{O}}/\mathfrak{m})^* \to \mathbf{C}^*$. Let $g(\chi,y) = \vartheta_{\mathfrak{a}}^p(\chi, i(y,y)) = \sum_{a \in \mathfrak{a}\cap\hat{\mathscr{O}}\cup\{0\}} \chi(a)N(a^p)e^{-\pi t\langle a/|md|,a\rangle}$. Then

$$\mathscr{M}(g)((s/2,s/2)) = 2^{1-s}\Gamma(s)\pi^{-s}(DN(\mathfrak{m}))^{-s/2}\frac{1}{|\mathscr{O}^*|}\sum_{\xi\subset\mathscr{O}_K}\lambda(\xi)N(\xi)^{-s} = \frac{2}{|\mathscr{O}^*|}\Lambda_M(s,f_\lambda,\psi)$$

The functional equation of $\vartheta_{\mathfrak{a}}^p(\chi,z)$ gives

$$g(\chi,1/y) = W(\chi,\overline{p})y^{\nu+1}g(\overline{\chi},y),$$

by the technique used to find the functional equation of a Mellin transform,

$$\Lambda_M(\nu+1-s, f_{\overline{\lambda}}, \overline{\psi}) = W(\chi,\overline{p})\Lambda_M(s,f_\lambda,\psi).$$

Let $C = N((md/|md|)^{\overline{p}})^{-1}$, then $W(\chi,\overline{p}) = Ci^{-\nu}\dfrac{g(\hat{\lambda}_f\hat{\psi})}{\sqrt{N(p\mathfrak{m})}}$. Since for $(p,M) = 1$, $g(\hat{\lambda}_f\hat{\psi}) = \lambda_f(p)\psi(N(\mathfrak{m}))g(\hat{\psi})g(\hat{\lambda}_g)$ and $g(\hat{\psi}) = p\left(\dfrac{-D}{p}\right)\psi(D)g(\psi)^2$,

$$W(\chi,\overline{p}) = \lambda_f(p)\left(\frac{-D}{p}\right)\psi(M)\frac{g(\psi)}{g(\overline{\psi})}\cdot Ci^{-\nu}\frac{g(\hat{\lambda}_f)}{\sqrt{N(\mathfrak{m})}}.$$

□

Corollary 2.2 (Hecke). *If $\nu > 0$, $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$ is a primitive character, then $f_\lambda \in S_{\nu+1}(M,\varepsilon)$. where $\varepsilon(a) = \lambda_f(a)\left(\frac{-D}{a}\right)$.*

Proof. Let $g(z) = i^{-2\nu-1}\frac{g(\hat{\lambda}_f)}{\sqrt{N(\mathfrak{m})}}\sum_{\xi\subset\mathscr{O}}\overline{\lambda}(\xi)e^{2\pi iN(\xi)z}$, then by the previous proposition,

$$\Lambda_M(s,f,\psi) = i^{\nu+1}C_\psi\Lambda_M(\nu+1-s,g,\overline{\psi})$$

where $C_\psi = \varepsilon(p)\psi(M)\frac{g(\psi)}{g(\overline{\psi})}$. Let $f_\lambda = \sum_n a_nq^n$, $g = \sum_n b_nq^n$. Clearly $a_n = O(n^{nu+1})$ and $b_n = O(n^{\nu+1})$ and $\Lambda_M(s,f)$, $\Lambda_M(s,g)$, $\Lambda_M(s,f,\psi)$, $\Lambda_M(s,g,\overline{\psi})$ satisfy conditions in the converse theorem of Weil for all p coprime to M and the character $\psi : \mathbf{Z}/p^* \to \mathbf{C}^*$, hence $f_\lambda \in M_{\nu+1}(M,\varepsilon)$. Furthermore, $L(s,f)$ converges for $\mathrm{Re}(s) > \nu/2+1 = \nu+1-(\nu/2)$, then for $\nu > 0$, $f_\lambda \in S_{\nu+1}(M,\varepsilon)$ by the converse theorem of Weil. □

Proof of theorem I(A).i

If $\mathfrak{p}|\mathfrak{c}^{-1}\mathfrak{m}$, put $\mathfrak{n} = \mathfrak{p}^{-1}\mathfrak{m}$, let $\mu \in \Lambda_{\mathfrak{n}}^{\nu}$ so the restriction to $\Lambda_{\mathfrak{m}}^{\nu}$ is λ. Then

$$f_\mu(N(\mathfrak{p})z) = \sum_{(\xi,\nu)=1}\mu(\xi)q^{N(\mathfrak{p}\xi)}$$

, hence

$$f_\mu(z) - \mu(p)f_\mu(N(\mathfrak{p})z) = \sum_{(\xi,\mathfrak{n})=1} - \sum_{(\xi,\mathfrak{m})=\mathfrak{p}}\mu(\xi)q^{N(\xi)} = f_\lambda(z).$$

By induction on $N(\mathfrak{c}^{-1}\mu)$, it suffices to prove the theorem for the case $\mathfrak{m} = \mathfrak{c}$, i.e. $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$ is primitive. But this reduced to the theorem of Hecke (Corollary 2.2).

Lemma 2.3 (Euler product). *The L-function $L(s,\lambda)$ has an euler product:*

$$L(s,\lambda) = \prod_p(1-a_pp^{-s}+\varepsilon(p)p^{\nu-2s})^{-1},$$

where $\varepsilon(p) = (D/p)\lambda((p))/p^\nu$.

Proof. Observe that $L(s,\lambda) = \prod_{0\neq\mathfrak{p}\in\mathrm{Spec}\,\mathscr{O}_K}(1-\lambda(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}$. For a rational prime p,

$$\text{if } (D/p) = 1,\ p\mathscr{O}_K = \mathfrak{p}_1\mathfrak{p}_2,\ N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p,\ a_p = \lambda(\mathfrak{p}_1)+\lambda(p_2), \tag{2}$$

$$\text{if } (D/p) = -1,\ p\mathscr{O}_K = \mathfrak{p},\ N(\mathfrak{p}) = p^2,\ a_p = 0,\ \lambda(\mathfrak{p}) = \lambda((p)), \tag{3}$$

$$\text{if } (D/p) = 0,\ p\mathscr{O}_K = \mathfrak{p}^2,\ N(\mathfrak{p}) = p,\ a_p = \lambda(\mathfrak{p}). \tag{4}$$

$$\begin{aligned}
L(s,\lambda) &= \prod_{(D/p)=1}\prod_{\mathfrak{p}|p}(1-\lambda(\mathfrak{p})p^{-s})^{-1}\prod_{(D/p)=-1}(1-\lambda((p))p^{-2s})^{-1}\prod_{(D/p)=0}(1-\lambda(\mathfrak{p})p^{-2s})^{-1}\\
&= \prod_{(D/p)=1}(1-(\lambda(\mathfrak{p}_1)+\lambda(\mathfrak{p}_2))p^{-s}+\lambda(\mathfrak{p}_1\mathfrak{p}_2)p^{-2s})^{-1}\prod_{(D/p)=-1}(1-\lambda((p))p^{-2s})^{-1}\\
&\prod_{(D/p)=0}(1-a_pp^{-2s})^{-1}\\
&= \prod_p(1-a_pp^{-s}+(D/p)\lambda((p))p^{-2s})^{-1}\\
&= \prod_p(1-a_pp^{-s}+\varepsilon(p)p^{\nu-2s})^{-1}
\end{aligned}$$

□

Corollary 2.3 (theorem I(A).ii)**.** *f_λ is a normalized eigenform.*

Proof. By theorem I(A).1, $f \in S_{\nu+1}(M,\varepsilon)$, together with the euler product in the previous lemma, we conclude that f is a normalized eigenform. (Cf. [2]]). □

3 Decomposition of A_λ

Lemma 3.1. *Let $f(z) = \sum_{n\in\mathbf{N}} a_n q^n$ be an element of $S_k(N,\chi)$, r a positive integer, M a common multiple of Nr and r^2, and let*

$$g(z) = \sum_{(n,r)=1} a_n q^n.$$

Then $g \in S_k(M,\chi')$, where χ' is the restriction of χ to $(\mathbf{Z}/M\mathbf{Z})^\times$.

Proof. Since $\det(\zeta_r^{un})_{0\le i\le r-1,\ 0\le j\le r-1} = \prod_{0\le i<j<r-1} (\zeta_r^j - \zeta_r^i) \neq 0$, we can solve $x_0,\dots,x_{r-1} \in \mathbf{Q}(\zeta_r)$ such that

$$\sum_{u=0}^{r-1} x_u \zeta_r^{un} = \begin{cases} 1 & \text{if } (n,r)=1 \\ 0. & \text{else} \end{cases}.$$

Set $x_m = x_u$ if $m \equiv u(r)\ \forall m \in \mathbf{Z}$. It can be seen that x_u is invariant under $\mathrm{Gal}(\mathbf{Q}(\zeta_r)/\mathbf{Q})$, hence $x_i \in \mathbf{Q}$ and $g(z) = \sum_{u=0}^{r-1} x_i f[\eta_u]_k$ where $\eta_u = \begin{pmatrix} r & u \\ 0 & r \end{pmatrix}$. Note that

$$\begin{pmatrix} r & u \\ 0 & r \end{pmatrix} \gamma \begin{pmatrix} r & d_\gamma^2 u \\ 0 & r \end{pmatrix}^{-1} \in M_2(\mathbf{Z})\ \forall \gamma \in \Gamma_0(M),$$

$$\begin{pmatrix} r & u \\ 0 & r \end{pmatrix} \gamma \begin{pmatrix} r & d_\gamma^2 u \\ 0 & r \end{pmatrix}^{-1} \equiv \begin{pmatrix} a_\gamma & * \\ 0 & d_\gamma \end{pmatrix} (N),$$

so $f[\eta_u][\gamma] = f[\eta_{d^2u}]$ and since $(d,r)=1$,

$$\sum_{u=0}^{r-1} x_u f[\eta_u][\gamma] = \sum_{u=0}^{r-1} x_u f[\eta_{d^2u}] = \sum_{u=0}^{r-1} x_{d^{-2}u} f[\eta_u] = \sum_{u=0}^{r-1} x_u f[\eta_u],$$

i.e. $g \in S_k(\Gamma_1(M))$. If $(d,M)=1$, put $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(M)$, then $(d,r)=1$ and $f[\eta_u][\gamma] = \chi(d) f[\eta_{d^2u}]$, $g[\gamma] = \chi(d) g$. □

Let us recall that for a normalized eigenform of weight 2, $f = \sum_{n\in\mathbf{N}} a_n q^n \in S_k(N,\chi)$, the associated abelian variety A_f has dimension (i) $[K_f : \mathbf{Q}]$, (ii) $K_f \hookrightarrow \mathrm{End}_{\mathbf{Q}}(A_f)$, $a_n \mapsto T_n\ \forall n$ (Hecke opoerators) and (iii) it is defined over $\mathbf{Q}$. (See [shim1], [diam]).

Let $V_{\mathfrak{m}}^\nu = \langle f_\lambda : \lambda \in \Lambda_\mu^\nu \rangle_{\mathbf{C}}$, $\dim V_\mu^\nu = [I(\mathfrak{m}) : P(\mathfrak{m})]$. Fix a set of representatives S for $I(\mathfrak{m})$ modulo $P(\mathfrak{m})$, define for each $\mathfrak{a} \in S$,

$$g_{\mathfrak{a}}(z) = \sum_{(\alpha)\in P(\mathfrak{m}),\ \alpha\in\mathfrak{a}} \alpha^\nu q^{N(\alpha)/N(\mathfrak{a})}.$$

Note that

$$f_\lambda(z) = \sum_{\mathfrak{a}\in S} \lambda(\mathfrak{a})^{-1} g_{\mathfrak{a}},$$

so $\{g_{\mathfrak{a}} : \mathfrak{a} \in S\}$ forms a basis of $V_{\mathfrak{m}}^{\nu}$. Note that for an automorphism $\sigma : \mathbf{C} \to \mathbf{C}$, $K^{\sigma} = K$ since K is a quadratic field and so $\mathfrak{m}^{\sigma} = \mathfrak{m}$ or $\mathfrak{m}^{\sigma} = \mathfrak{m}^{\rho} := \{\bar{x} : x \in \mathfrak{m}\}$ for $\mathfrak{m} \subset \mathscr{O}_K$. For $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$, define $\lambda_{\sigma} \in \Lambda_{\mathfrak{m}^{\sigma}}^{\nu}$ by $\lambda_{\sigma}(\xi) = \lambda(\xi^{\sigma})^{\sigma}$. Then $f_{\lambda}^{\sigma} = f_{\lambda_{\sigma}}$. Lastly before the proceeding to the proof, we recall a theorem from the theory of abelian varieties:

Poincaré's complete reducibility theorem. *Any abelian variety over k is isogenous over k to a product of simple abelian varieties over k. The isogeny type of the factors are uniquely determined.*

Proof of theorem I(B)

Case 1. $\mathfrak{m}$ is divisible by $2\sqrt{-D}$ and $\mathfrak{m} = \mathfrak{m}^{\rho}$. Put $\Gamma = \Gamma_1(M)$, $\delta = \begin{pmatrix} 1 & 1/D \\ 0 & 1 \end{pmatrix}$, suppose $\Gamma\delta\Gamma = \sqcup_{i=1}^{\kappa} \Gamma\delta\gamma_i$, $\gamma_i \in \Gamma$. Then

$$\mathscr{G}_{\mathfrak{a}}[\Gamma\delta\Gamma]_2 = \sum_i g_{\mathfrak{a}}[\delta\gamma_i]_2.$$

Note that if $\alpha, \beta \in W_{\mathfrak{m}} \cap \mathfrak{a}$,

$$N(\alpha)/N(\mathfrak{a}) \equiv N(\beta)/N(\mathfrak{a}) \mod D,$$

to see this, choose $r \in \mathscr{O}$ such that $r\mathfrak{a} \subset \mathscr{O}$, may suppose $\mathfrak{a} \subset \mathscr{O}$, then $N(\alpha)$, $N(\beta) \in \mathbf{Z}$ and since $\alpha \equiv \beta(\sqrt{-D})$, D divides $N(\alpha) - N(\beta)$. On the other hand, since $N(\mathfrak{a})$ divides $N(\alpha) - N(\beta)$ and is coprime to D, we conclude the equation. Therefore

$$g_{\mathfrak{a}}[\Gamma\delta\Gamma]_2 = \kappa\zeta_D^{N(\alpha)/N(\mathfrak{a})} g_{\mathfrak{a}},$$

with $\alpha \in \mathfrak{a}$ fixed. Let A' be the abelian subvariety of $\mathscr{J}(C_M)$ generated by A_{λ} $\forall\lambda \in \Lambda_{\mathfrak{m}}^1$, i.e. the isogenous image in $\mathscr{J}(C_M)$. The tangent space of A' is spanned by $f_{\lambda}^{\sigma} - f_{\lambda^{\sigma}}$ $\forall\lambda \in \Lambda_{\mathfrak{m}}^1$ $\sigma : \mathbf{C} \to \mathbf{C}$, but since $\mathfrak{m} = \mathfrak{m}^{\rho}$, the tangent space is exactly $V_{\mathfrak{m}}^1$. Then $[\Gamma\delta\Gamma]$ acts on A'. Let ω denote the corresponding endomorphism, then the representation of ω on the tangent space diagonally with eigenvalues $\kappa\zeta - D^{N(\alpha)/N(\mathfrak{a})}$. Let $\chi(r) = (-D/r)$ be the Kronecker symbol, recall that

$$\sqrt{-D} = g(\chi) = \sum_{a \in \mathbf{Z}/\mathbf{D}^*} \chi(a)\zeta_D^a.$$

One sees that $N(\alpha)/N(\mathfrak{a})$ is prime to D and $\chi(N(\alpha)/N(\mathfrak{a})) = 1$. Define an embedding

$$\iota : \mathbf{Q}(\zeta_D) \to \mathrm{End}_{\mathbf{Q}}(A')$$

by

$$\zeta_D \mapsto \kappa^{-1}\omega.$$

$\iota(\sqrt{-D})$ is the idendity map since $\iota(\sqrt{-D})$ has components of the form

$$\sum_{a \in \mathbf{Z}/\mathbf{D}^*} \chi(a)\iota\zeta_D^a = \sum_{a \in \mathbf{Z}/\mathbf{D}^*} \chi(a)\zeta_D^{aN(\alpha)/N(\mathfrak{a})} = \sum_{a \in \mathbf{Z}/\mathbf{D}^*} \chi(a)\chi(N(\alpha)/N(\mathfrak{a}))^{-1}\zeta_D^a = \sqrt{-D},$$

i.e. $\iota : K = \mathbf{Q}(\sqrt{-D}) \to \mathrm{End}_{\mathbf{Q}}(A)$ is equivalent to the identity injection of K into $\mathbf{C}$, by Definition 1, A' is isogenous to a product of an elliptic curve whose endomorphism algebra is K, so does its subvariety A_{λ} by Poincaré's complete reducibility theorem.

Case 2. λ is primitive.

Put $\mathfrak{m}' := 2\mathfrak{m}\mathfrak{m}^\rho(\sqrt{-D})$, $M' = N(\mathfrak{m}')D$, $\eta_u = \begin{pmatrix} M & u \\ & M \end{pmatrix}$ for $u \in \mathbf{Z}$. Then $M' = M^2$ and $\mathfrak{m}' = \mathfrak{m}'^\rho$. Define $x_u \in \mathbf{Q}$ as in the proof of Lemma 3.1 so that

$$\sum_{u=0}^{M-1} x_u \zeta_M^{un} = \begin{cases} 1 & \text{if } (n,M) = 1 \\ 0 & \text{else.} \end{cases}$$

Take $t \in \mathbf{Q}$ so that $tx_u \in \mathbf{Z}$ $\forall u$ and put

$$\xi = \sum_{u=0}^{M-1} tx_u [\eta_u]_2.$$

Then by the proof in Lemma 3.1, if

$$f = \sum_n a_n q^n \in S_2(M,\varepsilon),$$

we have

$$f|\xi = t \sum_{(n,M)=1} a_n q^n \in S_2(M',\varepsilon).$$

Especially $f_\lambda|\xi = tf_\mu$ where $\mu \in \Lambda^1_{\mathfrak{m}'}$ is the restriction of λ to $I(\mathfrak{m}')$. In fact, if $\mathfrak{a}$, $\mathfrak{b}$ are integral ideals,

$$(\mathfrak{a}, \mathfrak{b}\mathfrak{b}^\rho) = 1 \text{ iff } (N(\mathfrak{a}), N(\mathfrak{b})) = 1.$$

Let V_λ be the subspace of $V^1_{\mathfrak{m}} + V^1_{\mathfrak{m}'}$ spanned by f_{λ^σ}, $\sigma : \mathbf{C} \to \mathbf{C}$, then we see that ξ maps V_λ into $V^1_{\mathfrak{m}'}$, it is injective by primitivity of λ. Let A'' be abelian subvariety of $\mathscr{J}(C_{M'})$ generated by A_μ, $\mu \in \Lambda^1_{\mathfrak{m}'}$, the tangent space is $V^1_{\mathfrak{m}'}$ since $(\mathfrak{m}')^\rho = \mathfrak{m}'$. Hence ξ induces a morphism

$$\xi^* : \mathscr{J}(M') \to \mathscr{J}(M)$$

and restricts to a surjection

$$A'' \twoheadrightarrow A_\lambda$$

where by case 1, A'' is isogenous to product of an abelian variety E whose endomorphism algebra is K, then there is a surjective morphism $\varphi : E^k \twoheadrightarrow A_\lambda$, and hence A_λ is isogenous to a product of E. Here we made use of Poincaré's complete reducibility theorem again.

Case 3. General case.

Let $\mathfrak{c}$ be the conductor of λ. We prove by induction on $N(\mathfrak{c}^{-1}\mathfrak{m})$, based on the primitive case, which was proved in case 2. Suppose $\mathfrak{p}|\mathfrak{c}^{-1}\mathfrak{m}$, put

$$\mathfrak{n} = \mathfrak{p}^{-1}\mathfrak{m},\ q = N(\mathfrak{p}),\ N = q^{-1}M,\ \beta = \begin{pmatrix} q & \\ & 1 \end{pmatrix}.$$

Since $\beta\Gamma_1(M)\beta^{-1} \subset \Gamma_1(N)$, $[\beta]_2$ defines a morphism

$$\psi : \mathscr{J}(C_M) \to \mathscr{J}(C_N).$$

Let

$$\varphi : \mathscr{J}(C_M) \to \mathscr{J}(C_N)$$

be the morphism induced by natural projection $C_M \to C_N$. Take $\mu \in \Lambda^1_{\mathfrak{n}}$ whose restriction to $I(\mathfrak{m})$ is λ, then since $f_{\lambda^\sigma} = f_{\mu^\sigma} - sf_{\mu^\sigma}[\beta]_2$, then

$$(\text{res}, [\beta]_2) : V^1_{\mathfrak{n}} \times V^1_{\mathfrak{n}} \twoheadrightarrow V^1_{\mathfrak{m}}$$

is a surjection, so

$$(\psi,\varphi)\mathscr{J}(C_M)\to\mathscr{J}(C_N)\times\mathscr{J}(C_N)$$

induces a finite morphism

$$A_\lambda\to A_\mu\times A_\mu.$$

By induction hypothesis A_μ is isogenous to product of an elliptic curve whose endomorphism algbera is K, , hence also A_λ, by Poincaré's complete reducibility theorem.

4 Modularity of E/Q with complex multiplication

Here we let E be an elliptic curve over $\mathbf{Q}$ with complex multiplication. Deuring in 1950s proved that $L(s,E)$ comes from a grossencharacter $\lambda\in\Lambda^1_{\mathfrak{m}}$:

Theorem 4.1 (Deuring)**.** *Let E be an elliptic curve over $\mathbf{Q}$ with $K\simeq\mathrm{End}_{\mathbf{Q}}(E)$, then*

$$L(s,E)=L(s,\lambda_E)$$

for some $\lambda_E\in\Lambda^1_{\mathfrak{m}}$.

Let $\lambda=\lambda_E\in\Lambda^1_\nu$, by theorem I(A), $\lambda\in S_2(M,\varepsilon)$ and is a normalized eigenform. Since E is defined over $\mathbf{Q}$, we see that $a_n\in\mathbf{Q}$, so A_λ has dimension 1, is defined over $\mathbf{Q}$.

By previous results, if $f_\lambda=\sum_n a_nq^n$,

$$L(s,\lambda)=\prod_p(1-a_pp^{-s}+\varepsilon(p)p^{1-2s}).$$

Since E is defined over $\mathbf{Q}$, $a_n\in\mathbf{Q}$ and ε is the trivial character, so $f_\lambda\in S_2(\Gamma_0(M))$ and both A_λ and A'_λ are elliptic curves over $\mathbf{Q}$ where A'_λ is the abelian subvariety of $\mathscr{J}(X_0(M)_{\mathbf{Q}})$. Clearly A_λ and A'_λ are isogenous over $\mathbf{Q}$.

Theorem 4.2. *The elliptic curve A'_λ is isogenous to E over* $\mathbf{Q}$

Proof. The cotangent space of A'_λ generated solely by f_λ, so the Hecke operators T_n acts on A'_λ as multiplication by $a_n(f)$. By Eichler-Shimura relation, for all but finitely many rational prime p (exactly those primes inducing good reduction), $T_p=\sigma_p^*+(\sigma_p)_*=1+p-\sharp(A'_\lambda[p])$ modulo p, hence $a_p(f)=1+p-\sharp(A'_\lambda[p])$, i.e. the euler factor at p of $L(s,A'_\lambda)$ and that of $L(s,\lambda)$ coincides. By theorem I(B) $\mathrm{End}_{\mathbf{Q}}(A)=K$, and by the theorem of Deuring, there exists a grossencharacter μ of K such that $L(s,\mu)=L(s,A_\lambda)$. Thus $L(s,\lambda)$ coincides with $L(s,\mu)$ up to finitely many euler factors. Let $\mathfrak{m}$ be the common multiple of conductors of λ and μ, then $\lambda/\mu:I(\mathfrak{m})/P(\mathfrak{m})\to\mathbf{C}^*$ is well-defined. Since $\lambda/\mu\neq1$ only for finitely many primes, and there are infinitely many in each classes of $I(\mathfrak{m})/P(\mathfrak{m})$ with has finite order, so $\lambda=\mu$. Thus E and A_λ determine the same grossencharacter, hence isogenous over $\mathbf{Q}$. □

References

[1] Max Deuring. “Die Zetafunktion einer algebraischen Kurve vom Gerschlecht Eins, I, II, III, IV”. In: *Nachr. Akad. Wiss. Göttingen* (1953,1955,1956,1957).

[2] Jerry Shurman Fred Diamond. *A First Course in Modular Forms*. Springer.

[3] Toshitsune Miyake. *Modular Forms*. Springer.

[4] Jürgen Neukirch. *Algebraic Number Theory*. Springer.

[5] Goro Shimura. *Introduction to Arithmetic Theory of Automorphic Functions*. Princeton University Press.

[6] Goro Shimura. “On elliptic curves with complex multiplication as factors of Jacobians of modular function field”. In: *Nagoya Mathematical Jounal* 43 (1971), pp. 199–208.

[7] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer.