Hecke Theta Series and Modularity of CM Elliptic Curves[1]

Stephen Liu December 16, 2024

Contents

1 Introduction **1**

2 Elliptic Curves with Complex Multiplication **2**

3 Hecke Characters **4**

4 Hecke Theta Series **5**

4.1 Holomorphicity 5

4.2 Automorphy properties 6

4.3 Modularity of CM curves 11

5 Examples **12**

5.1 $E_1 : y^2 = x^3 + x.$ 12

5.2 $E_2 : y^2 = x^3 + D$ 12

1 Introduction

Modularity of elliptic curves is a key step towards the proof of Fermat's last theorem. While it was not until 1995 did Wiles and Taylor prove that every semistable elliptic curve is modular and hence Fermat's last theorem was finally proven, it had been well-known that elliptic curves with complex multiplication (CM) are modular. Hecke (1920) constructed the *Größencharaktere*, which we call *Hecke characters* henceforth, and constructed the corresponding L-series and a generalized theta series, which are modular forms. By the theory of

[1]This is a note in supplement of a talk of the same title I gave in a Modular Functions class at Temple University on December 3, 2024.

complex multiplication, to every CM elliptic curve one can attach an algebraic Hecke character. Then Deuring (1953) proved that the L-series of a CM elliptic curve can be identified with that of an algebraic Hecke character. Modularity of CM curves thus follows.

Hecke also showed the convergence, analytic continuation, and functional equations of the L-series. In particular, the functional equations are used to show that the newly defined theta series are modular forms. Recall that the classical theta function is defined to be

$$\theta(z) = \sum_{n=-\infty}^{\infty} q^{n^2}, \quad \text{where } q = e^{2\pi i z}.$$

Then through the function $\omega(t) = \sum_{-\infty}^{\infty} e^{-\pi n^2 t}$ which satisfies $\omega(t) = (1/\sqrt{t})\omega(1/t)$ by Poisson summation, we see that the theta function satisfies the transformation formula

$$\theta(-1/4z) = (2z/i)^{1/2}\theta(z).$$

The Riemann Zeta function $\zeta(s)$ satisfies a functional equation $\Lambda(s) = \Lambda(1-s)$ where $\Lambda(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$. This functional equation is equivalent to the transformation formula for the theta function via Mellin transformation. This is generalized to Lemma 6, which implies that we can obtain certain transformation properties from functional equations of L-series of Hecke characters. Using this result and others from [Miy89], we reproduce the proof that the theta series attached to a primitive Hecke character on an imaginary quadratic number field that induces a trivial nebentypus character is a modular form of weight 2, level $\Gamma_0(N)$ for some positive integer N. These conditions are satisfied by the modular forms attached to CM elliptic curves.

More broadly, Hecke constructed of theta series from quadratic forms over the integers and they are modular forms of various weights and levels. See Section 4.9 in [Miy89].

2 Elliptic Curves with Complex Multiplication

For $E_1/\mathbb{C} \cong \mathbb{C}/\Lambda_1, E_2/\mathbb{C} \cong \mathbb{C}/\Lambda_2$ complex elliptic curves, every *isogeny* from E_1 to E_2 is given by multiplication by a complex number

$$\alpha \in \mathbb{C}^\times : \alpha\Lambda_1 \subseteq \Lambda_2.$$

Hence the endomorphism ring of a complex elliptic curve can be identified as a subring of $\mathbb{C}$ where composition of functions is amount to multiplication of complex numbers. Since a lattice is a $\mathbb{Z}$-submodule of $\mathbb{C}$, any integer determines an endomorphism. On the other hand, it is a fact that $\mathrm{End}(E) = \mathbb{Z}$ for a lot of elliptic curves. And by Theorem VI.5.5 in [Sil09], in fact only two cases occur.

Theorem 1. *Let $E/\mathbb{C}$ be an elliptic curve, and let $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$ be the lattice associated to E, where $\tau \in \mathfrak{H}$. Then one of the following is true:*

(a) $\mathrm{End}(E) = \mathbb{Z}$.

(b) *The field* $K = \mathbb{Q}(\tau)$ *is an imaginary quadratic extension of* $\mathbb{Q}$, *and* $\mathrm{End}(E)$ *is isomorphic to an order* R *in* $K = \mathbb{Q}(\tau)$. *Note an order* R *in* K *is a subgroup of* K *such that* $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$.

In the latter case, we say that E has *complex multiplication by* $K = \mathbb{Q}(\tau)$ or has *complex multiplication by* R. Henceforth we will only consider elliptic curves with endomorphism ring being the ring of integers $\mathcal{O}_K$ of K.

Example 1. (a) $y^2 = x^3 - Ax$ ($A \in \mathbb{Z}_{\neq 0}$) has CM by $\mathbb{Z}[i]$, ring of integers of $\mathbb{Q}(i)$;
(b) $y^2 = x^3 + B$ ($B \in \mathbb{Z}_{\neq 0}$) has CM by $\mathbb{Z}[(1+\sqrt{-3})/2]$, ring of integers of $\mathbb{Q}(\sqrt{-3})$;
(c) $y^2 = x^3 - 35x + 98$ has CM by $\mathbb{Z}[(1+\sqrt{-7})/2]$, ring of integers of $\mathbb{Q}(\sqrt{-7})$.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. For each prime p, if $p \nmid N_E$, define $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)$.

Definition 1. The *L-series of* $E/\mathbb{Q}$ is defined by the Euler product

$$L(E/\mathbb{Q}, s) = \prod_{p \nmid N_E} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \mid N_E} (1 - a_p p^{-s})^{-1}.$$

where the product is over all primes.

Remark 1. The product converges and gives an analytic function for all s satisfying $\mathrm{Re}(s) > 3/2$.

Without Modularity, there is no way of proving analytic continuation and functional equations for $L(E/\mathbb{Q}, s)$. However, as a corollary of the main theorem of complex multiplication, one can construct an algebraic Hecke character (to be defined in Section 3) to E. Furthermore, after defining L-series for Hecke characters, we see that the L-series defined by elliptic curves coincide with the L-series given by Hecke characters ([Sil94] II.10.5(b)). Hecke showed analytic continuation and functional equations for these L-series. As a result, we have analytic continuation and functional equations for $L(E/\mathbb{Q}, s)$.

Theorem 2 (Deuring)**.** *Let* $E/\mathbb{Q}$ *be an elliptic curve with CM by* $\mathcal{O}_K$ *of* K. *Let* $\psi_{E/K} : I_K \to K^\times$ *be the Hecke character attached to* E *over* K. *Then*

$$L(E/\mathbb{Q}, s) = L(s, \psi_{E/K}).$$

Proof. See [Sil94] Sections II.10.4 and II.10.5. □

This implies that their power series expansions have identical coefficients a_n. This is the first step to show the modularity of CM curves.

3 Hecke Characters

Let K be a number field, that is, a finite extension of $\mathbb{Q}$. Consider all embeddings of K into $\mathbb{C}$. We say that an embedding $\tau : K \hookrightarrow \mathbb{C}$ is *real* if $\tau(K) \subseteq \mathbb{R}$, and *imaginary* otherwise. Imaginary embeddings come in complex conjugate pairs, if exist. Let $\tau_1, \dots, \tau_{r1}$ be the real embeddings, and let $\tau_{r_1+1}, \dots, \tau_{r_1+2r_2}$ be the imaginary embeddings such that $\tau_\nu = \overline{\tau_{\nu+r_2}}$ for all $r_1 + 1 \le \nu \le r_1 + r_2$. Also denote $a_\nu = \tau_\nu(a)$ for all $a \in K$.

Recall that a fractional ideal on K is a $\mathcal{O}_K$-submodule $\mathfrak{a}$ of K such that there exists $0 \neq r \in \mathcal{O}_K$ such that $r\mathfrak{a}$ is an (integral) ideal of $\mathcal{O}_K$. Fractional ideals form an abelian group under multiplication. Let P_K be the subgroup of I_K consisting of principal ideals. Note that $\mathcal{O}_K$ is a Dedekind domain, hence all ideals factor into products of prime powers uniquely. It follows that fractional ideals factor into product of (possibly negative) powers of prime ideals. Hence the notion of greatest common divisor and least common multiple makes sense for fractional ideals. For any integral ideal $\mathfrak{m} \subseteq \mathcal{O}_K$ we consider subgroups

$$\begin{aligned} I(\mathfrak{m}) &= \{\mathfrak{a} \in I_K : (\mathfrak{a}, \mathfrak{m}) = 1\}, \\ P(\mathfrak{m}) &= \left\{(a) \in P_K : a \equiv 1 \bmod^\times \mathfrak{m},\ a_\tau > 0 \text{ for all real embeddings } \tau\right\}, \end{aligned}$$

where $\bmod^\times$ indicates the multiplicative congruence, that is, for all primes $\mathfrak{p}|\mathfrak{m}$, the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}(a-1) \ge v_\mathfrak{p}(\mathfrak{m})$. Then $P(\mathfrak{m})$ is a subgroup of $I(\mathfrak{m})$.

Definition 2. A group homomorphism (character) $\xi : I(\mathfrak{m}) \to \mathbb{C}^\times$ is called an *(algebraic) Hecke character* mod $\mathfrak{m}$ if

$$\xi((a)) = \prod_{\nu=1}^{r_1+r_2} (a_\nu/|a_\nu|)^{u_\nu} |a_\nu|^{iv_\nu} \quad \text{for } (a) \in P(\mathfrak{m}), \tag{1}$$

with real numbers u_ν, v_ν such that

(a) $u_\nu \in \begin{cases} \{0,1\} & (\nu < r_1), \\ \mathbb{Z} & (\nu \ge r_1 + 1), \end{cases}$

(b) $\displaystyle\sum_{\nu=1}^{r_1+r_2} v_\nu = 0.$

Given a Hecke character ξ mod $\mathfrak{m}$, the *conductor* of ξ is the greatest common divisor $\mathfrak{m}_\xi$ of all integral ideals $\mathfrak{n}$ such that (1) holds for $(a) \in P(\mathfrak{n}) \cap I(\mathfrak{m})$. And we say that ξ is *primitive* if $\mathfrak{m} = \mathfrak{m}_\xi$.

Remark 2. (a) If $K = \mathbb{Q}$, then all integral ideals are of the form $\mathfrak{m} = M\mathbb{Z}$ for some $M \in \mathbb{Z}$. Condition (1) becomes

$$\xi((a)) = (a/|a|)^u \quad \text{for } a \equiv 1 \bmod^\times M$$

for some $u \in \{0,1\}$. Since $(a) = (-a)$, we must have $u = 0$, and hence ξ factors through $I(M\mathbb{Z})/P(M\mathbb{Z}) \cong (\mathbb{Z}/M\mathbb{Z})^\times$. Thus, ξ is a Dirichlet character mod M.

(b) If $K = \mathbb{Q}(\sqrt{d})$ is imaginary quadratic, then Condition (1) becomes

$$\xi((a)) = (a/|a|)^u \quad \text{for } a \equiv 1 \bmod^{\times} \mathfrak{m} \tag{2}$$

for some $u \in \mathbb{Z}$.

Remark 3. (a) The quotient $\mathrm{CL}(K) := I_K/P_K$ is called the *ideal class group* of K. The class group is a finite group whose order h_K is called the *class number* of K.

(b) The quotient $I(\mathfrak{m})/P(\mathfrak{m})$ is called the *ray class group* of $\mathfrak{m}$.

(c) There is another definition of Hecke characters as certain characters of the idele group $\mathbb{A}_K^{\times}$. Any Hecke character defined in the above way induces such a character on the idele group.

Definition 3. Let ξ be a primitive Hecke character on I_K with conductor $\mathfrak{m}$. Then the *attached L-series* is

$$L(s, \xi) = \prod_{\mathfrak{p}} (1 - \xi(\mathfrak{p}) N_{\mathbb{Q}}^K(\mathfrak{p})^{-1})$$

with $\xi(\mathfrak{p}) = 0$ if $\mathfrak{p} | \mathfrak{m}$.

Converges $\mathrm{Re}(s) \geq 1 + \epsilon$ for all $\epsilon > 0$.

Theorem 3 (Hecke)**.** *$L(s, \xi)$ has an analytic continuation to $\mathbb{C} - \{0, 1\}$, and to the entire complex plane if ξ is nontrivial, and there is a functional equation*

$$\Lambda(1 - s; \xi) = T(\xi) \Lambda(s, \overline{\xi}), \tag{3}$$

where $T(\xi)$ is some function related to the Gauss sum *$W(\xi)$, and $\Lambda(s; \xi)$ is some normalization of $L(s; \xi)$.*

Proof. This was proven by Hecke, and reformulated and reproven in Tate's thesis using Fourier analysis on the adele ring $\mathbb{A}_K$. □

4 Hecke Theta Series

4.1 Holomorphicity

Lemma 4.3.3 in [Miy89]:

Proposition 4. *Let k, N be positive integers. For a sequence $\{a_n\}_{n=0}^{\infty}$ of complex numbers such that $a_n = O(n^{\nu})$ for some $\nu > 0$, put*

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

for $z \in \mathfrak{H}$. Then the right-hand side converges absolutely and uniformly on any compact subset of $\mathfrak{H}$, and

$$f(z) = O(\mathrm{Im}(z)^{-\nu-1}) \quad (\mathrm{Im}(z) \to 0)$$
$$f(z) - a_0 = O(e^{-2\pi \mathrm{Im}(z)}) \quad (\mathrm{Im}(z) \to \infty)$$

And by Theorem 2.1.4 in [Miy89], we have

Proposition 5. *Assume that f is weakly modular of weight k, level $\Gamma \leq \Gamma(1)$, and is holomorphic on $\mathfrak{H}$. If there exists a positive number ν such that*

$$f(z) = O(\mathrm{Im}(z)^{\nu}) \quad (\mathrm{Im}(z) \to 0)$$

uniformly with respect to $\mathrm{Re}(z)$, then $f \in M_k(\Gamma)$. Moreover if we can take $\nu < k$, then $f \in S_k(\Gamma)$.

4.2 Automorphy properties

The main theorem is a special case of Theorem 4.8.2 in [Miy89]. Since the functional equation (3) of a Hecke character ξ relates $L(s, \xi)$ with $L(1-s, \overline{\xi})$, we can transform the functional equation into relation (A_ψ) between $L(s, f_\psi)$ and $L(k-s, g_{\overline{\psi}})$ for some functions f, g constructed in a suitable manner.

Remark 4. The map $f \mapsto f|_k \omega_N = (\sqrt{N}z)^{-k} f(-1/Nz)$ defines an automorphism of $M_k(\Gamma_0(N))$ (and $S_k(\Gamma_0(N))$).

Hence if the functions f, g mentioned above satisfy formula (A) $g(z) = (\sqrt{N}z)^{-k} f(-1/Nz)$, then both functions are modular forms as soon as we can show that one of them is. The following paragraphs are dedicated to explain how we can show that g is a modular form.

Let k, N be positive integers. For two sequences $\{a_n\}_{n=0}^{\infty}$, $\{b_n\}_{n=0}^{\infty}$ of complex numbers such that $a_n = O(n^\nu)$, $b_n = O(n^\nu)$ $(\nu > 0)$, put

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

and

$$g(z) = \sum_{n=0}^{\infty} b_n q^n, \quad q = e^{2\pi i z}$$

for $z \in \mathfrak{H}$.

Also let

$$L(s; f) = \sum_{n=0}^{\infty} a_n n^{-s}$$
$$\Lambda_N(s; f) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) L(s; f).$$

We have Theorem 4.3.6 in [Miy89].

Lemma 6 (Hecke)**.** *With k, N, f, g as defined above, the following conditions are equivalent:*

(A) $g(z) = (\sqrt{N}z)^{-k} f(-1/Nz)$ $(= (f|_k \omega_N))(z)$.

(B) Both $\Lambda_N(s; f)$ and $\Lambda_N(s; g)$ can be analytically continued to the whole s-plane, satisfying

$$\Lambda_N(s; f) = i^k \Lambda_N(k - s; g),$$

and certain modification of Λ is holomorphic on the whole s-plane and bounded on any vertical strip.

Proof. The proof generalizes that of the classical theta function and uses Poisson summation formula and Mellin transformation. □

Let ψ be a primitive Dirichlet character with conductor p a prime number such that $(p, N) = 1$. We consider the twists of $f = \sum_{n=0}^{\infty} a_n q^n$ by

$$f_\psi = \sum_{n=0}^{\infty} \psi(n) a_n q^n$$

and define

$$\begin{aligned} L(s; f, \psi) &= L(s, f_\psi) \\ \Lambda_N(s; f, \psi) = \Lambda_{Nm^2}(s; f_\psi) &= \left(m \frac{\sqrt{N}}{2\pi} \right)^s \Gamma(s) L(s; f, \psi). \end{aligned}$$

Now we have Theorem 4.3.9 in [Miy89].

Lemma 7. *With k, N, f_ψ, g_ψ as defined above, the following conditions are equivalent:*

(A_ψ) $C_\psi g_\psi(z) = (f_\psi|_k \omega_{Nm^2})(z)$.

(B_ψ) Both $\Lambda_N(s; f, \psi)$ and $\Lambda_N(s; g, \overline{\psi})$ can be analytically continued to be a holomorphic function the whole s-plane, bounded on any vertical strip, and satisfies the functional equation

$$\Lambda_N(s; f, \psi) = i^k C_\psi \Lambda_N(k - s; g, \overline{\psi}).$$

Proof. Plug in f_ψ, g_ψ in Lemma 6. □

A fact about twisting by Dirichlet characters: for $a \in \mathbb{R}$, let

$$\alpha(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Proposition 8. *(a) Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a holomorphic function on $\mathfrak{H}$, and ψ a primitive Dirichlet character of conductor m. Then for an integer $k > 0$ we have*

$$f_\psi = W(\overline{\psi})^{-1} \sum_{u=1}^{m} \overline{\psi}(u) f|_k \alpha(u/m).$$

(b) Let $f = \sum_{n=0}^{\infty} a_n q^n \in M_k(N, \chi)$ for some Dirichlet character χ with conductor m_χ, ψ a primitive Dirichlet character of conductor m_ψ, and M the least common multiple of N,m_ψ^2, and $m_\psi m_\chi$. Then $f \in M_k(M, \chi\psi^2)$, and is a cusp form if f is.

Proof. Part (a) follows from the definition of the Gauss sum $W(\overline{\psi})$, which we omitted. Part (b) can be proven using (a). □

A key result that goes into the proof of Theorem 11 is Theorem 4.3.15 in [Miy89], which can be used to show that f and g above are cusp forms simultaneously.

Theorem 9 (Weil, with k even and trivial nebentypus character)**.** *Let k be a positive even integer and N, f, g as defined above. Then $f, g \in S_k(\Gamma_0(N))$, and $g = f|_k \omega_N$, if the following conditions are satisfied:*

(a) $\Lambda_N(s; f)$ and $\Lambda_N(s; g)$ satisfy condition (B) in Lemma 6;

(b) for any primitive Dirichlet character ψ with conductor p an odd prime number such that $(p, N) = 1$, $\Lambda_N(s; f, \psi)$ and $\Lambda_N(s; g, \psi)$ satisfy condition (B_ψ) in Lemma 7 with the constant

$$C_\psi = C_{N,\psi} = \frac{\psi(-N) W(\psi)}{W(\overline{\psi})};$$

(c) (cusp form condition) $L(s; f)$ converges absolutely at $s = k - \delta$ for all $\delta > 0$.

Proof. (Sketch) By propositions 4 and 5, f and g are holomorphic on $\mathfrak{H}$ and at the cusps, by analyzing the behavior $\mathrm{Im}(z) \to 0$, we see that f, g are cusp forms if the satisfy automorphy properties. We need to show that $g|_k\gamma = g$ for all $\gamma = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$. For $c = 0$, $\gamma = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix}$. Then $(g|_k\gamma)(z) = (\pm 1)^k g(z \mp b) = g(z)$, since k is even and q-expansion is invariant under translation by integer values. Now assume $c \neq 0$. Then $(a, cN) = 1 = (d, cN)$. By Dirichlet's theorem on arithmetic progression, there exist odd primes $m, n \nmid N$ and $s, t \in \mathbb{Z}$ such that

$$a + tcN = m,$$
$$d + scN = n.$$

Put $u = -c$, $v = -(b + sm + stuN + nt)$. Then

$$\begin{pmatrix} a & b \\ cN & d \end{pmatrix} = \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} m & -v \\ -uN & n \end{pmatrix} \begin{pmatrix} 1 & -s \\ 0 & 1 \end{pmatrix}.$$

Hence it suffices to show the automorphy properties for matrices of the form

$$\gamma = \begin{pmatrix} m & -v \\ -uN & n \end{pmatrix} \in \Gamma_0(N)$$

for odd primes $m, n \nmid N$. By assumption, for any primitive Dirichlet character ψ with conductor m or n in particular, $\Lambda_N(s; f, \psi)$ and $\Lambda_N(s; g, \psi)$ satisfy condition (B_ψ), hence (A_ψ). Let

$$\gamma' = \begin{pmatrix} n & v \\ uN & m \end{pmatrix} \in \Gamma_0(N).$$

Then by some algebraic manipulation, (A_ψ) and Proposition 8 implies (extending the operator $g|_k$ linearly to the algebra $\mathbb{C}[\Gamma_0(N)]$ for convenience)

$$\begin{aligned} g|_k(1-\gamma')\alpha(-v/m) &= g|_k(1-\gamma)\alpha(v/m) \\ g|_k(1-\gamma'^{-1})\alpha(v/n) &= g|_k(1-\gamma^{-1})\alpha(-v/n) \end{aligned}$$

These mean that each side of the equation is independent of the choice of γ of that particular form. From these we get

$$g|_k(1-\gamma)(1-\gamma^{-1}\alpha(-2v/n)\gamma'\alpha(-2v/n)) = 0. \tag{4}$$

Now let $h = g|_k(1-\gamma) = g - g|_k\gamma$, a holomorphic function on $\mathfrak{H}$. We claim that $h = 0$. Let

$$\beta = \gamma^{-1}\alpha(-2v/n)\gamma'\alpha(-2v/n) = \begin{pmatrix} 1 & -2v/m \\ 2uN/n & 4/mn - 3 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Q}).$$

Then Equation (4) implies

$$h|_k\beta = h. \tag{5}$$

The matrix β has two properties worth mentioning:

(a) The trace $|\mathrm{Tr}\beta| = |4/mn - 2| < 2$, hence β is elliptic as an isometry on $\mathfrak{H}$. Hence β fixes a point $z_0 \in \mathfrak{H}$.

(b) Also, since m, n are odd primes, $|\mathrm{Tr}\beta| \neq 1, 0$. This implies that eigenvalues of β are not roots of unity. Since $\beta \in \mathrm{SL}_2(\mathbb{Q})$, the splitting field of the characteristic polynomial of β is a quadratic field, which can only contain the 1, 2, 3, 4, 6-th roots of unity. One can check that $|\mathrm{Tr}\beta| = 0, 1, 2$ if the eigenvalues are a pair of any of these roots of unity, hence a contradiction.

Put

$$\begin{aligned} \rho &= (z_0 - \overline{z_0})^{-1} \begin{pmatrix} 1 & -z_0 \\ 1 & -\overline{z_0} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}), \\ p(w) &= h|_k\rho^{-1}(w), \end{aligned}$$

for $w \in D$, the open unit disk. Then p is holomorphic on D. Since

$$\rho\beta\rho^{-1} = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$$

for some $\zeta \in \mathbb{C}$, we see by (5) that

$$p(\zeta^2 w) = \zeta^{-k} p(w).$$

Take the Taylor expansion $p(w) = \sum_{n=0}^{\infty} c_n w^n$ around $w = 0$, we get

$$\zeta^{2n} c_n = \zeta^{-k} c_n$$

for all n. Since ζ is not a root of unity, we must have $c_n = 0$ for all n. Therefore $h = 0$, so that $g|_k\gamma = g$. Since $f|_k\omega_N = g$, we also have $f|_k\gamma = f$. □

Recall that a newform $f \in S_k(\Gamma_1(N))^{\text{new}}$ is *primitive* if f is a normalized Hecke eigenform for Hecke operators T_n for all $n \geq 1$. When is f above a primitive form?

Lemma 10. *Let $0 \neq f = \sum_{n=1}^{\infty} a_n q^n \in S_K(\Gamma_0(N))$. Then f is a normalized Hecke eigenform for all Hecke operators T_n with $T_n(f) = a_n \cdot f$ if and only if*

$$L(s; f) = \prod_p (1 - a_p p^{-s} + p^{k-1-2s})^{-1}$$

has an Euler product over all prime numbers. Furthermore, let $(f|_k\omega_N)(z) = c\sum_{n=0}^{\infty} b_n q^n$ with $b_1 = 1$. Then f is a primitive form if and only if $L(s; f)$ has the above Euler product and $L(s; f|_k\omega_N)$ has the following Euler product

$$L(s; f|_k\omega_N) = c\prod_p (1 - b_p p^{-s} + p^{k-1-2s})^{-1}.$$

Hence the main theorem:

Theorem 11. *Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field with discriminant d (hence nonzero, $d \equiv 1 \bmod 4$, and square-free), and ξ a primitive Hecke character with conductor $\mathfrak{n}$ such that*

$$\xi((a)) = a/|a| \qquad \text{for } a \equiv 1 \bmod \mathfrak{n};$$
$$\xi((m)) = \left(\frac{d}{m}\right) \qquad \text{for } m \in \mathbb{Z}.$$

For $z \in \mathfrak{H}$, put

$$\theta_{tw}(z) = \theta_{tw}(\xi; z) = \sum_{\mathfrak{a}} \xi(\mathfrak{a}) N_K(\mathfrak{a})^{1/2} q^{N(\mathfrak{a})}, \ q = e^{2\pi i z},$$

where $\mathfrak{a}$ runs over all integral ideals of K. Then $\theta_{tw}(\xi) \in S_2(\Gamma_0(N))^{\text{new}}$. Here $N = |d|N_K(\mathfrak{n})$. Moreover, $\theta_{tw}(\xi)$ is a primitive form.

Proof. (Sketch) The function θ_{tw} serves as the function f in Theorem 9, and we will define the auxiliary function g below. By construction, we have

$$L(s; f) = L(s - 1/2; \xi).$$

Let ψ is a primitive Dirichlet character of conductor $p \nmid N$ a prime. Then since $(p, |d|) = 1$, $\psi \circ N_K$ is a primitive Hecke character on K with conductor $(p) \subseteq \mathcal{O}_K$. We also have

$$L(s; f_\psi) = L(s - 1/2; \xi(\psi \circ N_K)).$$

Then the functional equation (3) implies

$$\Lambda_N(s; f, \psi) = -C_\psi \Lambda_N(2 - s; g, \overline{\psi}),$$

where

$$C_\psi = \frac{\psi(-N)W(\psi)}{W(\overline{\psi})},$$
$$g(z) = \frac{iW(\xi)}{N_K(\mathfrak{n})^{1/2}} \sum_{\mathfrak{a}} \overline{\xi}(\mathfrak{a}) N_K(\mathfrak{a})^{1/2} q^{N_K(\mathfrak{a})}.$$

And f, g satisfy (B) and (B_ψ). So by Theorem 9 $f, g \in S_2(\Gamma_0(N))$. Since $L(s; f)$ has an Euler product, by Lemma 10 f is primitive. □

The proof above works for all Hecke characters satisfying Condition (2), where the constructed functions are of weight $u+1$, level $N = |d|N(\mathfrak{n})$, and possibly nontrivial nebentypus characters by $\chi(m) = \left(\frac{d}{m}\right) \xi((m))$. In general, the theta series attached to all primitive Hecke characters are primitive forms.

4.3 Modularity of CM curves

Note that if $\xi = \psi_{E,K}$ where $E/\mathbb{Q}$ is an elliptic curve with CM by K, we have

$$L(s, \theta_{tw}(\psi_{E,K})) = L(s - 1/2, \psi_{E,K}) = L(E/\mathbb{Q}, s - 1/2).$$

Thus the p-th Fourier coefficients of $\theta_{tw}(\psi_{E,K})$ does not match up with $a_p(E)$. Namely, $a_p(E) = a_p(\theta_{tw})/p^{1/2}$. To fix this issue, let

$$\theta(z) = \theta(\xi; z) = \sum_{\mathfrak{a}} \xi(\mathfrak{a}) q^{N(\mathfrak{a})}, \ q = e^{2\pi i z}.$$

Then we have

$$L(s, \theta(\psi_{E,K})) = L(s, \psi_{E,K}) = L(E/\mathbb{Q}, s).$$

In fact, θ and θ_{tw} are related by "twisting" by powers of the norm character, hence they are modular forms of the same weight. So $\theta(\psi_{E,K}) \in S_2(\Gamma_0(N'))^{\text{new}}$ is the modular form attached to E.

5 Examples

5.1 $E_1 : y^2 = x^3 + x$.

The curve E_1 has CM by $K = \mathbb{Q}(i)$, for which $\mathcal{O}_K$ is a principal ideal domain. Its p-th Fourier coefficients are

$$a_p = -\sum_{x \pmod p} \left(\frac{x^3+x}{p}\right) = \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4, \\ 2a & \text{if } p = a^2 + 4b^2, a \equiv 1 \pmod 4. \end{cases}$$

And explicitly

$$L(E_1/\mathbb{Q}, s) = L(s, \psi_{1,\mathbb{Q}(i)}) = \sum_{0 \neq \mathfrak{a} \subseteq \mathbb{Z}[i]} \psi_{E_1,\mathbb{Q}(i)}(\mathfrak{a}) N(\mathfrak{a})^{-s},$$

where $\psi_{1,\mathbb{Q}(i)}$ is the character on $\mathbb{Q}(i)$ such that ([Zag08] 105)

$$\psi_{1,\mathbb{Q}(i)}(\mathfrak{a}) = \begin{cases} 0 & \text{if } 2 | N(\mathfrak{a}), \\ \lambda & \text{if } 2 \nmid N(\mathfrak{a}),\ \mathfrak{a} = (\lambda),\ \lambda \in 4\mathbb{Z} + 1 + 2\mathbb{Z}i. \end{cases}$$

The corresponding cusp form is given by ([Zag08] 106)

$$\begin{aligned} \theta(\psi_{1,\mathbb{Q}(i)}, z) &= \sum_{0 \neq \mathfrak{a} \subseteq \mathbb{Z}[i]} \psi_{1,\mathbb{Q}(i)}(\mathfrak{a}) q^{N(\mathfrak{a})} = \sum_{\substack{a \equiv 1 \pmod 4 \\ b \equiv 0 \pmod 2}} a q^{a^2+b^2} \\ &= q + 2q^5 - 3q^9 - 6q^{13} + 2q^{17} - q^{25} + 10q^{29} + 2q^{37} + 10q^{41} + \cdots, \end{aligned}$$

which is a primitive form of weight 2 and level $64 = 2^6$ (LMFDB 64.2.a.a).

5.2 $E_2 : y^2 = x^3 + D$

([Sil94] Example 10.6)

The curve E_2 has CM by $K = \mathbb{Q}(\sqrt{-3})$, for which $\mathcal{O}_K$ is a principal ideal domain. For each prime ideal $\mathfrak{p}$, the corresponding Hecke character value is

$$\psi_{2,\mathbb{Q}(\sqrt{-3})}(\mathfrak{p}) = -\overline{\left(\frac{4D}{\pi}\right)_6} \pi, \quad \text{where } \mathfrak{p} = (\pi) \text{ and } \pi \equiv 2 \pmod 3.$$

Here $(\frac{\cdot}{\pi})_6$ is the sixth power residue symbol. Using $N_{\mathbb{Q}}^K(\pi) = \pi\overline{\pi}$, we have the Euler product

$$L(E/\mathbb{Q}, s) = L(s, \theta(\psi_{2,\mathbb{Q}(\sqrt{-3})})) = \prod_{\substack{\pi \in \mathcal{O}_K \text{ prime} \\ \pi \equiv 2 \pmod 3}} \left(1 + \overline{\left(\frac{4D}{\pi}\right)_6} \pi^{1-s} \overline{\pi}^{-s}\right)^{-1}.$$

And from this Euler product one obtains the coefficients for each integral ideal $\mathfrak{a} \subseteq \mathcal{O}_K$. And one can further obtain the n-th coefficients by summing up all ideals with norm n. For example, if $D = 4$,

$$\theta(\psi_{2,\mathbb{Q}(\sqrt{-3})}, z) = q + 5q^7 - 7q^{13} - q^{19} - 5q^{25} - 4q^{31} - q^{37} + 8q^{43} + \cdots,$$

which is a primitive form of weight 2 and level $108 = 2^2 \cdot 3^3$ (LMFDB 108.2.a.a).

References

[Miy89] Toshitsune Miyake. "Modular Groups and Modular Forms". In: *Modular Forms*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1989, pp. 96–194.

[Sil09] Joseph H. Silverman. "Elliptic Curves over $\mathbb{C}$". In: *The Arithmetic of Elliptic Curves*. New York, NY: Springer New York, 2009, pp. 157–183.

[Sil94] Joseph H. Silverman. "Complex Multiplication". In: *Advanced Topics in the Arithmetic of Elliptic Curves*. New York, NY: Springer New York, 1994, pp. 95–186.

[Zag08] Don Zagier. "Elliptic Modular Forms and Their Applications". In: *The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeid, Norway*. Ed. by Kristian Ranestad. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 1–103.