# Explicit Construction of Hecke Character Associated to Certain CM Elliptic Curves

SPUR Final Paper, Summer 2021

Yuyuan Luo
Mentor: Gefei Dang
Project suggested by Prof. Wei Zhang

August 4, 2021

**Abstract**

Deuring proved that each CM elliptic curve has a corresponding Hecke character with the same $L$-function, hence showing that the $L$-functions of CM elliptic curves have analytic continuation in $\mathbb{C}$. In this paper, we explicitly construct the Hecke character for a particular elliptic curve whose endomorphism ring is an order of $\mathbb{Q}(\sqrt{-7})$, with views towards generalizing this result to classes of CM elliptic curves.

## Contents

# 1 Introduction

Certain classes of elliptic curves were first studied by Diophantus in the third century, but elliptic curves as a whole were not studied systematically until the nineteenth century, when Jacobi and Weierstrass connected the geometric ideas of Newton and algebraic formulas of Bachet and Fermat with elliptic integrals and elliptic functions. In 1901, Poincaré unified and generalized these ideas to the theory of algebraic curves [BM02]. Elliptic curves are defined as curves $E$ over a perfect field $K$ of genus one having a specified base point; each elliptic curve can be represented by as the set of solutions to a *Weierstrass equation*, a cubic of the form

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

where $a_1, ..., a_6 \in K$, together with a point at infinity. Further, if $\text{char}(K) \neq 2, 3$, then $E$ takes the form $y^2 = x^3 + Ax + B$ with the appropriate change of variables. An elliptic curve is said to have *complex multiplication* if its endomorphism ring is larger than $\mathbb{Z}$.

The prototype for $L$-functions is the Riemann zeta function, and the first appearance of the $L$-function was with Dirichlet in 1837, who defined it as a series based on the Dirichlet character and used it to show that there are infinitely many primes in any primitive arithmetic progression. Then, in 1877, Dedekind generalized this notion of an $L$-function to number fields; Hecke later named the Dedekind zeta-function after him [LMF21a].

Then, in the early 20th century Hecke looked for a generalization for the Dirichlet $L$-function and the Dedekind zeta function. He introduced the notion of a Hecke character, which is the character of ideals of a number field, and established a number of important properties, including the following theorem.

**Theorem 1.1.** *(Hecke) Let $\chi$ be an algebraic Hecke character and $L_\chi(s)$ the corresponding $L-$function. If $\chi(A)$ is not equal to 1 for some ideal $A$, then $L_\chi(s)$ can be analytically continued to a function defined on $\mathbb{C}$.*

In 1955 Hasse introduced the Hasse-Weil zeta function, which is the zeta function associated with a curve. The $L$-function of an elliptic curve $E$ over $K$ is a function based on the number of points on $E$ in the reductions modulo a prime $p$, and we can express the Hasse-Weil zeta function in terms of the Riemann zeta function and the $L$-function of the curve. With this, one might wonder whether the $L$ function of elliptic curves can be analytically continued. The following theorem relates $L$-functions of elliptic curves with

complex multiplication to Hecke $L$-functions, and hence demonstrating that the $L$-functions of CM elliptic curves can be analytic continuted to a function on $\mathbb{C}$.

**Theorem 1.2.** *(Deuring) Let $E$ be an elliptic curve defined over $\mathbb{Q}$ having complex multiplication when it is considered as a curve over $\mathbb{C}$. Then there exists an algebraic Hecke character $\chi$ on a number field $K$ such that:*

$$L_E(s) = L_\chi(s).$$

This theorem gives us the existence of such a Hecke character, but the explicit construction of it is nontrivial. Our work is concerned with exactly this – to find an associated algebraic Hecke character to a particular elliptic curve.

In 2015, [Tam14] does the construction for curves of the form $y^2 = x^3 + D$ and $y^2 = x^3 - Dx$. We attempt a similar construction in our work.

In this paper, we begin by considering the curve

$$E : y^2 = x^3 - 35x + 98$$

to find its associated algebraic Hecke character $\chi$. Note that $E$ has complex multiplication and its endomorphism ring is an order of $\mathbb{Q}(\sqrt{-7})$ [LMF21b]. We will do this in three steps:

1. compute $N_p$, the number of points on $E$ in the reduction modulo $p$, in order to write down its $L$-function $L_E$
2. define $\chi$ and show that it is an algebraic Hecke character
3. prove that its $L$-function coincides with $L_E$

We provide necessary definitions in [§ 2], and we accomplish step 1 in [§ 3] and steps 2 and 3 in [§ 4]. Finally, in [§ 5], we provide some possible generalizations and future directions.

## 2 Preliminaries

In this section, we provide the necessary definitions for our work. We begin by defining the $L$-function of an ellptic curve defined over $\mathbb{Q}$.

**Definition 2.1.** *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with discriminant $\Delta$. The $L$-function of $E$ is*

$$L_E(s) = \prod_{p|\Delta}(1 - a_p p^{-s})^{-1} \cdot \prod_{p\nmid\Delta}(1 - a_p p^{-s} + p^{1-2s})^{-1},$$

*where if $p$ is a prime of good reduction, $a_p = p + 1 - N_p$; if $E$ has bad split multiplicative, bad non-split multiplicative, or bad additive reduction at $p$, $a_p$ is 1,-1,0 respectively. $N_p$ is the number of points on $E$ in the reduction modulo $p$.*

Now, we provide our definition of an algebraic Hecke character from [Tam14].

**Definition 2.2.** *Let $K$ be a $CM$ field which is also a Galois extension of $\mathbb{Q}$. Let $\mathcal{O}$ be the ring of integers of $K$ and $M$ a fixed ideal of $\mathcal{O}$. An algebraic Hecke character modulo $M$ is a function $\chi : \{I : I \subseteq \mathcal{O} \text{ ideal}\} \to \mathbb{C}$ that satisfies the following properties:*

1. $\chi(\mathcal{O}) = 1$
2. $\chi(A) \neq 0$ *if and only if* $(A, M) = (1)$
3. $\chi(AB) = \chi(A)\chi(B)$
4. *There is an element $\theta = \sum_\sigma n_\sigma \sigma \in \mathbb{Z}[G]$ such that if $\alpha \in \mathcal{O}, \alpha \equiv 1 \mod M$, then $\chi((\alpha)) = \alpha^\theta$*
5. *There is an integer $m > 0$, called the weight of $\chi$, such that $n_\sigma + n_{j\sigma} = m \forall \sigma \in G$.*

Finally, we define the $L$-function of a Hecke character.

**Definition 2.3.** *Let $\chi$ be an algebraic Hecke character on a $CM$ field $K$ with ring of algebraic integers $\mathcal{O}$. The Hecke $L$-function associated to $\chi$ is*

$$L_\chi(s) = \sum_A \chi(A)N(A)^{-s} = \prod_P (1 - \chi(P)N(P)^{-s})^{-1}$$

*where the sum is over all nonzero ideals of $\mathcal{O}$, the product over all maximal ideals of $\mathcal{O}$.*

## 3 Counting points modulo p

In this section, we will count the number of points on the reduction of $E$ modulo primes $p$, in order to find the $L$-function for $E$. We will do this in two cases: when $p$ is a non-square

modulo 7, and when it is a square modulo 7. We will make use of the following fact: If $K = \mathbb{Q}(\sqrt{d})$ for $d$ squarefree and $p$ is an odd prime, then

- $p$ is ramified if $p|d$,
- $p$ splits if $\left(\frac{d}{p}\right) = 1$,
- $p$ is inert if $\left(\frac{d}{p}\right) = -1$

where $\left(\frac{d}{p}\right)$ is the Legendre symbol.

### 3.1 Non-squares modulo 7

The following theorem tells us that in this case, the reduced curve is supersingular.

**Theorem 3.1.** *[Lan87] Let $A$ be an elliptic curve over a number field, with $End(A) \approx \mathfrak{b}$, where $\mathfrak{b}$ is an order in an imaginary quadratic field $k$. Let $\mathfrak{B}$ be a place of ${}^a\mathbb{Q}$ (algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$) over a prime number $p$, where $A$ has non-degenerate reduction $\tilde{A}$. The curve is supersingular if and only if $p$ has only one prime of $k$ above it ($p$ ramifies or remains prime in $k$).*

Hence, in this case, $E$ is supersingular over $p$. When $p = 3$, we can check that $N_p = 4$. The following result tells us that $N_p = p+1$ for all odd primes that are non-square modulo 7.

**Theorem 3.2.** *[Sil09] Suppose that $p \geq 5$ is prime. Then, $E$ is supersingular if and only if $N_p = p + 1$.*

### 3.2 Squares modulo 7

We will use the following theorem from [Sta96].

**Theorem 3.3.** *(Stark) Suppose $D$ is the discriminant of a complex quadratic field $k$ and that $(D, 6) = 1$. Suppose that*

$$\pi = \frac{u + v\sqrt{D}}{2}$$

*and that $(\pi)$ is a ideal in $k$ of norm $p$ (with $p$ prime) where $(p, 6D) = 1$. Let $\mathfrak{B}$ be a prime ideal of $H$ (the Hilbert class field of $k$) above $(\pi)$. Let also $a$ be any nonzero number of $H^+$ (the real subfield of $H$) whose numerator and denominator are relatively prime to*

$\mathfrak{B}$. *Further, let* $\gamma_2 = \gamma_2(\theta)$ *and* $\gamma_3 = \gamma_3(\theta)$ *with* $\theta = \frac{-3+\sqrt{D}}{2}$ *and* $\gamma_2(z)$ *and* $\gamma_3(z)$ *are the classical modular functions. Then the curve*

$$E_a : y^2 = 4x^3 - a^2 D\frac{\gamma_2}{12}x + a^3 D\frac{\gamma_3\sqrt{D}}{216}$$

*with coefficients in* $H^+$ *reduces mod* $\mathfrak{B}$ *to a curve* $\bar{E}_a$ *defined over* $\mathbb{F}_p$ *with*

$$p + 1 - \begin{cases} \left(\frac{a}{\mathfrak{B}}\right)\left(\frac{2u}{|D|}\right)u & \text{if } D \equiv 1 \mod 8 \\ \left(\frac{-a}{\mathfrak{B}}\right)\left(\frac{2u}{|D|}\right)u & \text{if } D \equiv 5 \mod 8 \end{cases}$$

*points.*

The author of [Sta96] provided several examples of this; in particular, when $D = -7$, the curve $y^2 = 4x^3 - 5 \cdot 7a^2x/4 - 7^2a^3/8$ has $p + 1 - \left(\frac{a}{u}\right)\left(\frac{u}{7}\right)u$ when reduced mod $p$. From this theorem, for $a = -4$ and $D = -7$, the curve

$$E' : y^2 = 4x^3 - 140x + 392$$

has $p + 1 - \left(\frac{-4}{p}\right)\left(\frac{\pi+\bar{\pi}}{7}\right)(\pi + \bar{\pi})$ points when reduced mod $p$. Note that since 4 is a square modulo $p$, $N_p$ for $E'$ is the same as $E$. Note that $\left(\frac{-4}{p}\right) = \left(\frac{7}{p}\right)$ since $\left(\frac{-4}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p-1)/2} = 1$. Hence, in this case, we can write $N_p = p + 1 - \left(\frac{7}{p}\right)\left(\frac{\pi+\bar{\pi}}{7}\right)(\pi + \bar{\pi})$.

# 4 Hecke Character and L-function

In this section, we first define the associated Hecke character, then we'll demonstrate that it has the same $L-$ function as $E$.

## 4.1 Hecke Character

Let $K = \mathbb{Q}(\sqrt{7})$ and let $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{7}}{2}]$ be its ring of integer. We find a Hecke character in $\mathcal{O}$. We define it by specifying the value of $\chi$ on prime ideals $(P)$ of $\mathcal{O}$. Similar to [Tam14], we define $\chi$ in the following manner:

1. If $P|14, \chi(P) = 0$.

2. If $P \nmid 14$ and $N(P) = p$, then $p$ is a square mod 7 and $(P) = (\pi)$ for some $\pi \in \mathcal{O}$ such that $\pi\bar{\pi} = p$. Then $\chi(P) = \left(\frac{7}{p}\right)\left(\frac{\pi+\bar{\pi}}{7}\right) \cdot \pi$. Denote the prime ideals of this type by $P_1$.

3. If $P \nmid 14$ and $N(P) = p^2$ then $p$ is a nonsquare mod 7 and $(P) = (p)$. Then $\chi(P) = -p$. Denote the prime ideals of this type by $P_2$.

We must show that this is indeed a Hecke character. Following the definition in [§ 2], we will show for $\theta = 1$ and $M = (28)$, the axioms are satisfied. It is sufficient to show that for $\alpha \in \mathcal{O}$, if $\alpha = 1 \mod M$, then $\chi((\alpha)) = \alpha$. For this, we'll need the following lemma.

**Lemma 4.1.** *Let $\alpha = a\sqrt{-7} + b \in \mathcal{O}$. Then, $\alpha$ is a square mod 7 if and only if $b$ is a square mod 7.*

*Proof.* First, suppose $\alpha$ is a square modulo 7 and $\alpha \equiv \beta^2 \mod 7$ where $\beta = c\sqrt{-7} + d$; we can choose a $\beta$ where $c, d$ are integers. Let $\beta^2 = c'\sqrt{-7} + d'$. Then, $d' = d^2 - 7c^2 \equiv d^2 \mod 7$. Further, since $d'$ and $b$ are both integers, since $\alpha \equiv \beta^2 \mod 7$, $d' \equiv b \mod 7$, so $b$ is a square mod 7. Now suppose $b$ is a square mod 7, and let $b \equiv d^2 \mod 7$. If $d = 0$, $b$ is a power of 7, then $\alpha^2 \equiv 0 \mod 7$ in this case. Now, $d \neq 0$, let $c = 2^{-1}d^{-1}x$, so $b \equiv d^2 - 7c^2 \mod 7$ and $a \equiv 2cd \mod 7$. Then letting $a' = 2cd$ and $b' = d^2 - 7c^2$, we have $a'\sqrt{-7} + b' = (c\sqrt{-7} + d)^2$. Note that if $a \equiv a' \mod 7$ and $b \equiv b' \mod 7$ then $a\sqrt{-7} + b \equiv a'\sqrt{-7} + b' \mod 7$. Hence, $\alpha$ is a square mod 7. □

This means that for $\pi = a\sqrt{-7}+b \in \mathcal{O}$, $\left(\frac{\pi+\bar{\pi}}{7}\right) = \left(\frac{2b}{7}\right) = \left(\frac{b}{7}\right) = \left(\frac{\pi}{7}\right)$. Here we generalize the Legendre symbol over the ring of integers based on whether $\pi$ is a square modulo the ideal generated by 7.

We now show that for $\alpha = a\sqrt{-7} + b \in \mathcal{O}$, if $\alpha \equiv 1 \mod (28)$, then $\chi((\alpha)) = \alpha$. First, notice that if, for a non-splitting prime $p \in \mathbb{Z}$ where $p \nmid 14$, $\chi((p)) = -p = \left(\frac{p^2}{7}\right)\left(\frac{p}{7}\right)p$. Hence, if $\alpha$ factors as $\alpha = \pi_1 ... \pi_m \cdot \pi_{m+1}\pi_{m+2}...\pi_{k-1}\pi_k \cdot p_{k+1}...p_n$, where if $i \leq k - m$ is even, $\pi_{m+i} = \bar{\pi}_{m+i-1}$ and $\pi_{m+i}\pi_{m+i-1}$ are split integer primes and $p_i$ are non-split integer primes, we have

$$\chi((\alpha)) = \prod_{i=1}^{k}\left(\frac{7}{p_i}\right)\left(\frac{\pi_i + \bar{\pi}_i}{7}\right) \cdot \pi_i \prod_{j=k+1}^{n}\left(\frac{p_j^2}{7}\right)\left(\frac{p_j}{7}\right) \cdot p_j.$$

This means that

$$\chi((\alpha)) = \alpha \cdot \left(\frac{\alpha}{7}\right) \cdot \prod_{i=1}^{k} \left(\frac{7}{p_i}\right) \prod_{j=k+1}^{n} \left(\frac{p_j^2}{7}\right).$$

So by quadratic reciprocity,

$$\chi((\alpha)) = \alpha \cdot \left(\frac{\alpha}{7}\right) \cdot \left(\frac{\alpha\bar{\alpha}}{7}\right) \cdot \prod_{i=1}^{m} (-1)^{(p_i-1)/2}.$$

Now note that $\alpha \equiv 1 \mod 7$ so it is a square mod 7, and hence $\bar{\alpha}$ is also a square mod 7 by Lemma 4.1, so we have

$$\chi((\alpha)) = \alpha \cdot \prod_{i=1}^{m} (-1)^{(p_i-1)/2}.$$

Now, note that since $\alpha \equiv 1 \mod 4$, $q = \pi_1 ... \pi_m$ is either 1 or 3 mod 4. Let $q = a_q\sqrt{-7} + b_q$. In either case, $a_q$ must be even and $b_q$ must be odd; this means that since $q\bar{q} = (\pi_1 ... \pi_m)(\overline{\pi_1 ... \pi_m}) = 7a_q^2 + b_q^2 \equiv b_q^2 - a_q^2 \mod 4 = (b_q + a_q)(b_q - a_q) \mod 4$, and $b_q + a_q \equiv b_q - a_q \mod 4$, so $p_1 ... p_m = q\bar{q} = b_q^2 - a_q^2 \equiv 1 \mod 4$. Hence, there are an even number of $p_i$ that are 3 mod 4, so $\chi((\alpha)) = \alpha$, as desired.

## 4.2 L-function

Now, we demonstrate that the $L-$function of $E$ is the same as the $L-$function of the Hecke character we defined.

Let $E$ be the curve whose affine equation is $y^2 = x^3 - 35x + 98$, so $\Delta = -2^{12}7^3$, so the places of bad reduction are $p = 2$ and $p = 7$. Let $c_4 = b_2^2 - 24b_4$, where $b_2 = a_1^2 + 5a_2$ and $b_4 = a_1a_3 + 2a_4$ and $a_1, ..., a_6$ are the Weierstrass coefficients. We can use the value of $c_4$ to determine the type of bad reduction. We can calculate $c_4$ in these two situations; in both cases, $c_4 \equiv 0$, so the reduction of $E$ has a cusp, and hence, $a_p$ is defined to be 0 in these cases. Hence, the $L-$function for $E$ is

$$L_E(s) = \prod_{p \nmid 14} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

where $a_p = p + 1 - N_p$ and $N_p$ is the number of points on $E$ in the reduction modulo $p$,

which we found in [§ 3]. Then, we would have

$$L_E(s) = \prod_{p\nmid 14, p=3,5,6 \mod 7} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p\nmid 14, p=1,2,4 \mod 7} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

substituting in our values for $a_p$, we have

$$L_E = \prod_{p\nmid 14, p=3,5,6 \mod 7} (1+p^{1-2s})^{-1} \prod_{p\nmid 14, p=1,2,4 \mod 7} (1+\left(\frac{7}{p}\right)\left(\frac{\pi+\bar{\pi}}{7}\right)\pi p^{-s})^{-1}(1+\left(\frac{7}{p}\right)\left(\frac{\pi+\bar{\pi}}{7}\right)\bar{\pi}p^{-s})^{-1}$$

$$= \prod_{(P)\in P_2} (1 - \chi(P)N(P)^{-s})^{-1} \prod_{(P)\in P_1} (1 - \chi(P)N(P)^{-s})^{-1} = L_\chi(s),$$

as desired: we have now found a $\chi$ with the same $L-$function as our elliptic curve.

## 5 Generalization and Future Work

Theorem 3.3 allows for the generalization of this result to certain classes of functions. In particular, suppose $a$ is a negative even square and $D$ is still $-7$, and consider the curves that are isomorphic to

$$E : y^2 = x^3 - 5 \cdot 7a^2x/16 - 7^2a^3/32.$$

Then, its discriminant $-343a^2$ has factors of 7 and 2. Suppose it factors as $\Delta = p_1^{n_1}...p_k^{n_k}$, and let $d = p_1...p_k$.

**Counting points modulo $p$:** When $p$ is a non-square mod 7, $N_p = p + 1$, and when $p$ is a square mod 7, $N_p = p + 1 - \left(\frac{a}{p}\right)\left(\frac{\pi+\bar{\pi}}{7}\right)(\pi + \bar{\pi})$. Note that $\left(\frac{a}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{-7}{p}\right) = 1$, so $N_p = p + 1 - \left(\frac{7}{p}\right)\left(\frac{\pi+\bar{\pi}}{7}\right)(\pi + \bar{\pi})$.

**Hecke Character:** We find a Hecke character in the endomorphism ring of $E$ by defining its value on the prime ideals $P$, with $M = (28)$:

1. If $P|d, \chi(P) = 0$.
2. If $P \nmid d$ and $N(P) = p$, then $p$ is a square mod 7, so $P = (\pi)$ and $\pi\bar{\pi} = p$. Then $\chi(P) = \left(\frac{7}{p}\right)\left(\frac{\pi+\bar{\pi}}{7}\right) \cdot \pi$.
3. If $P \nmid d$ and $N(P) = p^2$ then is a nonsquare mod 7, so $P = (p)$. Then $\chi(P) = -p$.

The proof that this is an algebraic Hecke character is the same as in [§ 4].

**$L$-function:** Note that $c_4 = 105a^2$, so in the bad reductions mod $p_i$, since $p_i$ is either $2, 7$, or a factor of $a$, $c_4 \equiv 0 \mod p_i$, so there is a cusp, and $a_p = 0$ in these cases. Hence the $L$-function is

$$L_E(s) = \prod_{p \nmid d} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

The proof that this is the same $L$-function as that of the Hecke character is the same as in [§ 4].

There are other generalizations that are immediately possible based on the other cases of theorem 3.3. In addition, the generalization of the construction to other elliptic curves is also a topic of interest.

## 6 Acknowledgements

This research was carried out as part of the Summer Program in Undergraduate Research (SPUR) at MIT. I would like to thank Prof. Wei Zhang for the suggestion of the project and my mentor Gefei Dang for the invaluable guidance she provided over the course of the program. In addition, I would like to thank Prof. Bjorn Poonen for his very helpful remarks and references, as well as Prof. Ankur Moitra and Prof. David Jerison for organizing the program and for their encouragement and support throughout the process.

## References

[BM02] Ezra Brown and Bruce T Myers. Elliptic curves from mordell to diophantus and back. *The American mathematical monthly*, 109(7):639–649, 2002.

[Lan87] Serge Lang. *The l-adic and p-adic Representations of Deuring*, page 182. Springer, 1987.

[LMF21a] The LMFDB Collaboration. A history of l-functions (reviewed). https://www.lmfdb.org/knowledge/show/lfunction.history, 2021. [Online; accessed 3 August 2021].

[LMF21b] The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2021. [Online; accessed 7 July 2021].

[Sil09] Joseph Silverman. *Elliptic Curves over Finite Fields*, page 154. Springer, 2009.

[Sta96] HM Stark. Counting points on cm elliptic curves. *The Rocky Mountain Journal of Mathematics*, 26(3):1115–1138, 1996.

[Tam14] Matteo Tamiozzo. Zeta and l-functions of elliptic curves. Master's thesis, Bologna, Italy, 2014.