The L-series Attached to a CM Elliptic Curve

Corina E. Pătraşcu
patrascu@fas.harvard.edu

May 19, 2005

Abstract

In this paper we present the L-series attached to an elliptic curve with complex multiplication. The L-series is an analytic function which encodes arithmetic information about the curve. One hopes that by studying the L-series from the analytic point of view, this might reveal important information about the curve. The purpose of the paper is to show that in the case of elliptic curves with complex multiplication, the L-series can be expressed in terms of Hecke L-series with Grössencharacter and thus to show that it has an analytic continuation to the whole complex plane and that it satisfies some functional equation.

1 The Idelic Formulation of Class Field Theory – A Brief Review

In this section we will present, without proof, the results from class field theory that will be necessary for the rest of the paper.

Let K be a number field and for each absolute value v on K, let K_v be the completion of K at v. Moreover, let $\mathcal{O}_v$ be the ring of integers of K_v if v is non-archimedean and let $\mathcal{O}_v = K_v$ otherwise. The idele group of k is the group $\mathbb{A}_K^* = \prod_v' K_v^*$, where prime indicates the fact that the product is restricted relative to the $\mathcal{O}_v$'s. Thus, an element $s \in \prod K_v^*$ in the unrestricted product is in $\mathbb{A}_K^*$ if and only if $x_v \in \mathcal{O}_v^*$ for all but finitely many v's. We can embed K^* into $\mathbb{A}_K^*$ by using the natural embedding:

$$K \hookrightarrow \mathbb{A}_K^*, \quad \alpha \mapsto (..., \alpha, \alpha, \alpha, ...),$$

since any $\alpha \in K^*$ is in $\mathcal{O}_v^*$ for all but finitely many K.

Also, for any given v we embed K_v^* as a subgroup of $\mathbb{A}_K^*$ as follows:

$$K_v^* \hookrightarrow \mathbb{A}_K^*, \quad t \mapsto (..., 1, 1, t, 1, 1, ...),$$

where t appears in the v-th component.

Definition 1. *Let $s \in \mathbb{A}_K^*$ be an idele. We define the* ideal of s *to be the fractional ideal of K given by:*

$$(s) = \prod_{\mathfrak{p}} \mathfrak{p}^{ord_{\mathfrak{p}} s_{\mathfrak{p}}}$$

where the product is taken over all prime ideals of K.

In order to make $\mathbb{A}_K^*$ into a topological group we do the following: for every integral ideal $\mathfrak{c}$ of K, let $U_{\mathfrak{c}}$ be the subgroup of $\mathbb{A}_K^*$ defined by:

$$U_{\mathfrak{c}} = \{s \in \mathbb{A}_K^* : s_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^* \text{ and } s_{\mathfrak{p}} \equiv 1 (\text{mod } \mathfrak{c}R_{\mathfrak{p}}) \text{ for all primes } \mathfrak{p}\}.$$

Then, $U_{\mathfrak{c}}$ is an open subgroup of $\mathbb{A}_K^*$ and it is easy to show that $K^* U_{\mathfrak{c}}$ is a subgroup of finite index in $\mathbb{A}_K^*$.

Definition 2 (Norm). *If L/K is a finite extension, then there is a natural* norm *map from $\mathbb{A}_L^*$ to $\mathbb{A}_K^*$. This is a continuous homomorphism $N_K^L : \mathbb{A}_L^* \to \mathbb{A}_K^*$ defined by the fact that the v component of $N_K^L x$ is $\prod_{w|v} N_{K_v}^{L_w} x_w$.*

The idelic formulation of class field theory is based on the reciprocity map described in the following theorem.

Theorem 3. *Let K be a number field and let K^{ab} be the maximal abelian extension of K. There exists a unique continuous homomorphism $\mathbb{A}_K^* \to Gal(K^{ab})/K$ sending $s \mapsto [s, K]$, with the property that:*

> *Let L/K be a finite abelian extension and let $s \in \mathbb{A}_K^*$ be an idele whose ideal (s) is not divisible by any primes that ramify in L. Then $[s, K] \mid_L = ((s), L/K)$.*

Here $(\cdot, L/K)$ is the Artin map and $Gal(K^{ab}/K)$ is given the usual profinite topology. The homomorphism $[\cdot, K]$ is called the reciprocity map *for K.*

Properties of the Reciprocity Map

- It is surjective and K^* is contained in its kernel.
- It is compatible with the norm map, i.e. $[x, L] \mid_{K^{ab}} = [N_K^L x, K]]$ for all $x \in \mathbb{A}_L^*$.
- Let $\mathfrak{p}$ be a prime ideal of K, let $I_{\mathfrak{p}}^{ab} \subset Gal(K^{ab}/K)$ be the inertia group of $\mathfrak{p}$ for the extension K^{ab}/K, let $\pi_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$ be a uniformizer at $\mathfrak{p}$ and let L/K be any abelian extension that is unramified at $\mathfrak{p}$. Then, $[\pi_{\mathfrak{p}}, K] \mid_L = (\mathfrak{p}, L/K) =$ Frobenius for L/K at $\mathfrak{p}$, and $[\mathcal{O}_{\mathfrak{p}}^*, K] = I_{\mathfrak{p}}^{ab}$.

2 The Associated Grössencharacter

On a number field $L/\mathbb{Q}$, a Grössencharacter is defined as a continuous homomorphism $\psi : \mathbb{A}_L^* \to \mathbb{C}^*$ with the property that $\psi(L^*) = 1$. If β is a prime of L, then we say that a Grössencharacter $\psi : \mathbb{A}_L^* \to \mathbb{C}^*$ is unramified at β if $\psi(\mathcal{O}_\beta^*) = 1$.

In this section, we want to give the definition of a Grössencharacter associated to an elliptic curve with complex multiplication. We begin by giving a map which, with small modifications, will be the desired Grössencharacter.

Theorem 4. *Let E/L be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of K, and assume that $L \supset K$. Let $x \in \mathbb{A}_L^*$ be an idele of L and let $s = N_K^L x \in \mathbb{A}_K^*$. Then there exists a unique $\alpha = \alpha_{E/L}(x) \in K^*$ with the following two properties:*

(i) $\alpha\mathcal{O}_K = (s)$, where $(s) \subset K$ is the ideal of s.

(ii) For any fractional ideal $\mathfrak{a} \subset K$ and any analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$, the following diagram commutes:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\alpha s^{-1}} & K/\mathfrak{a} \\ \downarrow f & & \downarrow f \\ E(L^{ab}) & \xrightarrow{[x,L]} & E(L^{ab}) \end{array}$$

Proof. For the proof of this theorem, we refer the reader to [2]. □

The above theorem gives us a well-defined homomorphism $\alpha_{E/L} : \mathbb{A}_L^* \to K^* \subset \mathbb{C}^*$. However, $\alpha_{E/L}(L^*) \neq 1$, so $\alpha_{E/L}$ is not a Grössencharacter. To make this more precise, note that given $\beta \in L^*$ and $x_\beta \in \mathbb{A}_L^*$ to be its corresponding idele, then $[x_\beta, L] = 1$. Thus, the above theorem tells us that $\alpha = \alpha_{E/L}(x_\beta)$ is the unique element of K^* such that $\alpha\mathcal{O}_K = N_K^L((x_\beta))\mathcal{O}_K = N_K^L(\beta)\mathcal{O}_K$ and such that if we multiply by $\alpha N_K^L x_\beta^{-1}$, it induces the identity map on $K/\mathfrak{a}$. This unique α is precisely $N_K^L\beta$ which implies that:

$$\alpha_{E/L}(x_\beta) = N_K^L\beta \quad \text{for all } \beta \in L^*.$$

Using this information, we can start proving the following important result which will give us the Grössencharacter that we want.

Theorem 5. *Let E/L be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of K. Assume that $L \supset K$ and let $\alpha_{E/L} : \mathbb{A}_L^* \to K^*$ be the map described in (4). For any idele $s \in \mathbb{A}_K^*$, let $s_\infty \in \mathbb{C}^*$ be the component of s corresponding to the unique archimedean absolute value on K. Define a map:*

$$\psi_{E/L} : \mathbb{A}_L^* \to \mathbb{C}^*, \quad \psi_{E/L}(x) = \alpha_{E/L}(x) N_K^L(x^{-1})_\infty.$$

(i) $\psi_{E/L}$ *is a Grössencharacter of* L*;*

(ii) Let β *be a prime of* L*. Then* $\psi_{E/L}$ *is unramified at* β *if and only if* E *has good reduction at* β*.*

Proof. **(a)** We saw already that if $\beta \in L^*$, then $\alpha_{E/L}(x_\beta) = N_K^L\beta$. On the other hand, from the definition of the norm map, we get $N_K^L(x_\beta)_\infty = \prod_{\tau:L\hookrightarrow\mathbb{C}\tau|_K=1}\beta^\tau = N_K^L\beta$. Hence, $\psi_{E/L}(x_\beta) = 1$. Since this is true for all β, then we clearly have that $\psi_{E/L}(L^*) = 1$. Moreover, it is clear that $\psi_{E/L}$ is a homomorphism, so we are left to verify that it is also continuous on $\mathbb{A}_L^*$. That will prove that $\psi_{E/L}$ is a Grössencharacter.

First, we verify that $\alpha_{E/L} : \mathbb{A}_L^* \to \mathbb{C}$ is continuous. Fix an integer $m \geq 3$. It is proved in [2] that $L(E[m])$ is a finite abelian extension of L. let $B_m \subset \mathbb{A}_L^*$ be the open subgroup corresponding to $L(E[m])$, i.e., B_m is the subgroup such that the reciprocity map induces an isomorphism:

$$\begin{array}{ccc} \mathbb{A}_L^*/B_m & \longrightarrow & Gal(L(E[m])/L) \\ x & \mapsto & [x,L]\,|_{L(E[m])} \end{array}$$

Now consider the sets:

$$W_m = \{s \in \mathbb{A}_K^* : s_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^* \text{ and } s_\mathfrak{p} \equiv 1(\text{mod } m\mathfrak{p}) \text{ for all } \mathfrak{p}\},$$

and

$$U_m = B_m \cap \{x \in \mathbb{A}_l^* : N_K^L x \in W_m\}.$$

U_m is an open subgroup of finite index in $\mathbb{A}_L^*$. Next, we are going to prove that $\alpha_{E/L}(x) = 1$ for all $x \in U_m$. Take some $x \in U_m$ and let $\alpha = \alpha_{E/L}(x)$. Also, fix an analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \longrightarrow E(\mathbb{C})$ as the one described in (4). For $t \in m^{-1}\mathfrak{a}/\mathfrak{a}$ we have $f(t) \in E[m]$ so:

$$\begin{array}{rcll} f(t) & = & f(t)^{[x,L]} & \text{since } x \in B_m, \text{ so } [x,L] \text{ fixes } L(E[m]) \\ & = & f(\alpha N_K^L x^{-1} t) & \text{from } (4ii) \\ & = & f(\alpha t) & \text{since} t \in m^{-1}\mathfrak{a}/\mathfrak{a} \text{ and } (N_K^L x)_\mathfrak{p} \in 1 + m\mathfrak{p} \text{ for all } \mathfrak{p}. \end{array}$$

In conclusion, multiplication by α fixes $m^{-1}\mathfrak{a}/\mathfrak{a}$ which equivalently can be expressed as $(\alpha - 1)m^{-1}\mathfrak{a} \subset \mathfrak{a}$. This implies that $(\alpha - 1)\mathcal{O}_K \subset m\mathcal{O}_K$ so $\alpha \in \mathcal{O}_K$ and $\alpha \equiv 1(\text{mod } m\mathcal{O}_K)$. However, from (4i) we have that $\text{ord}_\mathfrak{p}\,\alpha = \text{ord}_\mathfrak{p}(N_K^L x)_\mathfrak{p}$ and the latter quantity is equal to 1 because the $\mathfrak{p}$-component of $N_K^L x \in W_m$ is a unit. Since this holds for all primes $\mathfrak{p}$, we must have that α is a unit, i.e. $\alpha \in \mathcal{O}_K^*$. However, since we showed above that $\alpha \equiv 1(\text{mod } m\mathcal{O}_K)$, we conclude that the only possibility is that $\alpha = 1$.

From the definition of $\psi_{E/L}$ we then have that $\psi_{E/L}(x) = N_K^L(x^{-1})_\infty$ for all $x \in U_m$. This clearly implies that $\psi_{E/L}$ is continuous on U_m, but since U_m is an open subgroup of finite index of $\mathbb{A}_L^*$, $\psi_{E/L}$ must be continuous on all of $\mathbb{A}_L^*$ which is what we wanted. Thus, $\psi_{E/L}$ is a Grössencharacter.

(b) Let $I_\beta^{ab} \subset Gal(L^{ab}/L)$ be the inertia group for β. If we embed $\mathcal{O}_\beta^*$ into $\mathbb{A}_L^*$ by taking:

$$\mathcal{O}_\beta^* \hookrightarrow \mathbb{A}_L^*, \quad u \mapsto [..., 1, 1, u, 1, 1, ...]$$

with a u on the β-component, then the reciprocity map takes $\mathcal{O}_\beta^*$ to I_β^{ab}, i.e $[\mathcal{O}_\beta^*, L] = I_\beta^{ab}$.

Now let m be an integer such that $\beta \nmid m$. It is shown in [2] that in this case, $E[m] \subset E(L^{ab})$ so we know that we have an action of I_β^{ab} will act on $E[m]$. Our next goal is to characterize when this action is trivial in terms of the Grössencharacter $\psi_{E/L}$. We have that:

$$\begin{array}{lcll} I_\beta^{ab} \text{ acts trivially on } E[m] & \iff & f(t)^\sigma = f(t) & \text{for all } \sigma \in I_\beta^{ab} \text{ and all } t \in m^{-1}\mathfrak{a}/\mathfrak{a} \\ & \iff & f(t)^{[x,L]} = f(t) & \text{for all } x \in \mathcal{O}_\beta^* \text{ and all } t \in m^{-1}\mathfrak{a}/\mathfrak{a} \\ & \iff & f(\alpha_{E/L}(x)(N_K^L x^{-1})t) = f(t) & \text{for all } x \in \mathcal{O}_\beta^* \text{ and all } t \in m^{-1}\mathfrak{a}/\mathfrak{a} \end{array}$$

Note that $\psi_{E/L}(x) = \alpha_{E/L}(x)$ for all $x \in \mathcal{O}_\beta^*$ since the archimedean components of $x \in \mathcal{O}_\beta^*$ are all 1. Note furthermore that multiplication by $N_K^L x^{-1}$ induces the identity map on $m^{-1}\mathfrak{a}/\mathfrak{a}$ which follows from the fact $\beta \nmid m$ and the fact that if $\mathfrak{a}$ is a fractional ideal and $\mathfrak{c}$ is an integral ideal of K, and if $s \in \mathbb{A}_K^*$ is an idele with the property that $s_\mathfrak{p} = 1$ for all primes $\mathfrak{p}$ dividing $\mathfrak{c}$, then the multiplication by s map $s : K/\mathfrak{a} \to K/\mathfrak{a}$ induces the identity map on $\mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a}$ (i.e. $st = t$ for all $t \in \mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a}$). This statement can be proved by using the decomposition of $\mathfrak{c}^{-1\mathfrak{a}/\mathfrak{a}}$ into $\mathfrak{p}$-primary components. A detailed proof of this is given in [2].

Returning to our proof, we find that:

$$\begin{array}{lcll} I_\beta^{ab} \text{ acts trivially on } E[m] & \iff & f(\psi_{E/L}(x)t) = f(t) & \text{for all } x \in \mathcal{O}_\beta^* \text{ and all } t \in m^{-1}\mathfrak{a}/\mathfrak{a} \\ & \iff & \psi_{E/L}(x) \equiv 1 (\text{mod } m\mathcal{O}_K) & \text{for all } x \in \mathcal{O}_\beta^*, \\ & & & \text{since } f : m^{-1}\mathfrak{a}/\mathfrak{a} \longrightarrow E[m]. \end{array}$$

Applying now the Néron-Shafarevich-Ogg criterion which says that I_β^{ab} acts trivially on $E[m]$ for infinitely many m prime to β if and only if E has good reduction at β we obtain the desired result:

$$\begin{array}{lcl} E \text{ has good reduction at } \beta & \iff & \text{there are infinitely many } m \text{ with } \beta \nmid m \\ & & \text{such that } \psi_{E/L}(x) \equiv 1 (\text{mod } m\mathcal{O}_K) \text{ for all } x \in \mathcal{O}_\beta^* \\ & \iff & \psi_{E/L}(x) = 1 \text{ for all } x \in \mathcal{O}_\beta^* \\ & \iff & \psi_{E/L} \text{ is unramified at } \beta. \end{array}$$

□

3 The Hecke L-series

Suppose that $\psi : \mathbb{A}_L^* \to \mathbb{C}^*$ is a Grössencharacter on L, i.e. ψ is a continuous homomorphism which is trivial on L^*. Let β be a prime of L at which ψ is unramified, i.e. $\psi(\mathcal{O}_\beta^*) = 1$. Then, define $\psi(\beta)$ to be:

$$\psi(\beta) = \psi(..., 1, 1, \pi, 1, 1, ...)$$

having $1'$s everywhere and π on the β-component, where π is a uniformizer at β. Since ψ is unramified at $\beta, \psi(\beta)$ is well-defined independent of the choice of π. If ψ is ramified at β, we set $\psi(\beta) = 0$. Now, we can make the following definition:

Definition 6. *The* Hecke L-series attached to the Grössencharacter $\psi : \mathbb{A}_L^* \to \mathbb{C}^*$ *is defined by the Euler product:*

$$L(s, \psi) = \prod_{\beta} (1 - \psi(\beta) q_\beta^{-s})^{-1},$$

where the product is over all primes of L.

The Hecke L-series have the following important property whose proof we will not give. It was first proved by Hecke and it was then reformulated and proved by Tate [4] using Fourier analysis on the adele ring $\mathbb{A}_L$.

Theorem 7 (Hecke). *Let $L(s, \psi)$ be the Hecke L-series attached to the Grössencharacter ψ. Then, $L(s, \psi)$ has an analytic continuation to the entire complex plane and satisfies a functional equation relating its values at s and $N - s$ for some real number $N = N(\psi)$.*

4 The L-series Attached to a CM Elliptic Curve

Let $L/\mathbb{Q}$ be a number field and let E/L be an elliptic curve. For each prime β of L, define:

- $\mathbb{F}_\beta$ = residue field of L at β;
- $q_\beta = N_{\mathbb{Q}}^L \beta = \#\mathbb{F}_\beta$.

Definition 8. *If E has good reduction at β, we define* local L-series of E at β *to be:*

$$L_\beta(E/L, T) = 1 - a_\beta T + q_\beta T^2$$

where $a_\beta = q_\beta + 1 - \#\widetilde{E}(\mathbb{F}_\beta)$.
If E has bad reduction at β, we define the local L-series as follows:

$$L_\beta(E/L, T) = \begin{cases} 1 - T & \text{if } E \text{ has split multiplicative reduction at } \beta \\ 1 + T & \text{if } E \text{ has non-split multiplicative reduction at } \beta \\ 1 & \text{if } E \text{ has additive reduction at } \beta \end{cases}$$

Definition 9. *The (global) L-series attached to the elliptic curve E/L is defined by the Euler product*

$$L(E/L, s) = \prod_{\beta} L_\beta(E/L, q_\beta^{-s})^{-1}$$

where the product is over all primes of L.

Using the estimate $|a_\beta| \leq 2\sqrt{q_\beta}$, one can show that this product converges and gives an analytic function for all s for which $Re(s) > \frac{3}{2}$. It is conjectured however, that far more is true.

Conjecture 10. *Let E/L be an elliptic curve defined over a number field. The L-series of E/L has an analytic continuation to the entire complex plane and satisfies a functional equation relating its values at s and $2-s$.*

For elliptic curves with complex multiplication, this conjecture can be verified by showing that the global L-series can be written as a product of Hecke L-series with Grössencharacter, for which we know from Hecke's Theorem (7) that it has an analytic continuation to the entire complex plane and that it satisfies a functional equation relating its values at s and $N-s$ for some real number $N = N(\psi)$.

In order to be able to express $L(E/L, s)$ in terms of Hecke L-series, we want to express the number of points in $\widetilde{E}(\mathbb{F}_\beta)$ in terms of the Grössencharacter attached to E/L.

Proposition 11. *Let E/L be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of K and assume that $L \subset K$. Let β be a prime of L at which E has good reduction, let $\widetilde{E}$ be the reduction of E modulo β and let $\phi_\beta : \widetilde{E} \to \widetilde{E}$ be the associated q_β-power Frobenius map. Finally, let $\psi_{E/L} : \mathbb{A}_L^* \to K^*$ be the Grössencharacter attached to E/L. Then, the following diagram commutes:*

$$\begin{array}{ccc} E & \xrightarrow{\psi_{E/L}(\beta)} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\phi_\beta} & \widetilde{E} \end{array}$$

where the vertical maps are reduction modulo β.

Proof. First note that from (5ii) we know that $\psi_{E/L}$ is unramified at β, so $\psi_{E/L}(\beta)$ is well-defined. Second, since $\psi_{E/L}(\beta)$ is the value of $\psi_{E/L}$ at an idele which has 1's in all its archimedean components, then we have $\psi_{E/L}(\beta) = \alpha_{E/L}(\beta) \in \mathcal{O}_K$ so we can talk about $[\psi_{E/L}(\beta)]$ as an endomorphism of E.

If we let $x \in \mathbb{A}_L^*$ to be an idele with a uniformizer on the β-component and with 1's everywhere else, then as remarked before, $\psi_{E/L}(\beta) = \psi_{E/L}(x) = \alpha_{E/L}(x) \in \mathcal{O}_K$ and now using the definition of $\alpha_{E/L}$ from the commutative diagram from (4), we get that:

$$f(t)^{[x,L]} = [\psi_{E/L}(x)] f(N_K^L x^{-1} t) \quad \text{for all } t \in K/\mathfrak{a}.$$

Now if we again fix some integer m with $\beta \nmid m$, we know from the proof of theorem 5 that $N_K^L x^{-1} t = t$ for all $t \in m^{-1}\mathfrak{a}/\mathfrak{a}$ so we get that $f(t)^{[x,L]} = [\psi_{E/L(x)}] f(t)$ for all $t \in m^{-1}\mathfrak{a}/\mathfrak{a}$.

Now from theorem (3) we have that $[x, L] = (\beta, L^{ab})/L$ and so if we reduce everything modulo β, $[x, L]$ reduces to the q_β-power Frobenius map. So,

$$\phi_\beta(\widetilde{f(t)}) = \widetilde{f(t)^{[x,L]}} = [\widetilde{\psi_{E/L}(x)}]\widetilde{f(t)}$$

for all $t \in m^{-1}\mathfrak{a}/\mathfrak{a}$. Here, $\sim$ symbolizes reduction modulo β.

But now since we know that this holds true for any m prime to β, and since an endomorphism of $\widetilde{E}$ is determined completely by its action on the torsion, we conclude that $\phi_\beta = [\widetilde{\psi_{E/L}(x)}]$.

□

Corollary 12. *With notation as in (11), we have:*

- $q_\beta = N_{\mathbb{Q}}^L \beta = N_{\mathbb{Q}}^K(\psi_{E/L}(\beta))$;
- $\#\widetilde{E}(\mathbb{F}_\beta) = N_{\mathbb{Q}}^L \beta + 1 - \psi_{E/L}(\beta)$;
- $a_\beta = \psi_{E/L}(\beta) + \overline{\psi_{E/L}(\beta)}$.

Proof. **(a)** From [1] we know that $N_K^L \beta = \deg \phi_\beta$ and from (11) we know that $\deg \phi_\beta = \deg[\widetilde{\psi_{E/L}(\beta)}] = \deg[\psi_{E/L}(\beta)]$. The latter equality follows from the theory of the Hilbert class field and in particular from Proposition 4.4 in [2]. Finally, we know that $N_{\mathbb{Q}}^K(\psi_{E/L}(\beta)) = \deg[\psi_{E/L}(\beta)]$ and so we obtain the desire result: $N_{\mathbb{Q}}^L \beta = N_{\mathbb{Q}}^K(\psi_{E/L}(\beta))$.

(b) From [1] we note that $\#\widetilde{E}(\mathbb{F}_\beta) = \#\ker(1 - \phi_\beta) = \deg(1 - \phi_\beta)$. From (11), the latter quantity is equal to $\deg[1 - \widetilde{\psi_{E/L}(\beta)}]$ and again from Proposition 4.4 in [2] we have that this latter quantity is equal to $\deg[1 - \psi_{E/L}(\beta)]$. Finally, as before, this is equal to $N_{\mathbb{Q}}^K(1 - \psi_{E/L}(\beta)) = (1 - \psi_{E/L}(\beta))(1 - \overline{\psi_{E/L}(\beta)})$. Finally, from part (a), this is equal to $1 - \psi_{E/L}(\beta) - \overline{\psi_{E/L}(\beta)} + N_{\mathbb{Q}}^L \beta$.

(c) Combining the first two parts with the definition of a_β, we obtain the desired result.

□

Theorem 13 (Deuring). *Let E/L be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of K.*

(a) Assume that K is contained in L. Let $\psi_{E/L} : \mathbb{A}_L^* \to K^*$ be the Grössencharacter attached to E/L. Then

$$L(E/L, s) = L(s, \psi_{E/L}) L(s, \overline{\psi_{E/L}}).$$

(b) Suppose that K is not contained in L and let $L' = LK$. Further, let $psi_{E/L'} : \mathbb{A}_{L'}^* \to K^*$ be the Grössencharacter attached to E/L'. Then,

$$L(E/L, s) = L(s, \psi_{E/L'}).$$

Sketch of Proof. **(a)** One can show that E has potential good reduction at every prime of L and thus conclude that E has no multiplicative reduction. Thus, we have that:

$$L_\beta(E/L,T) = \begin{cases} 1 - a_\beta T + q_\beta T^2 & \text{if } E \text{ has good reduction at } \beta \\ 1 & \text{if } E \text{ has bad reduction at } \beta \end{cases}$$

Now if we assume that E has good reduction at β, then by the definition of L_β and (12), we have that: $L_\beta(E/L,T) = 1 - a_\beta T + q_\beta T^2 = 1 - (\psi_{E/L}(\beta) + \overline{\psi_{E/L}(\beta)})T + (N_{\mathbb{Q}}^K \psi_{E/L}(\beta))T^2 = (1 - \psi_{E/L}(\beta)T)(1 - \overline{\psi_{E/L}(\beta)}T)$.

But, from (5b) we know that $\psi_{E/L}$ is unramified at β if and only if E has good reduction at β and the same holds for $\overline{\psi_{E/L}}$. So, this implies that $\psi_{E/L}(\beta) = \overline{\psi_{E/L}(\beta)} = 0$ if E has bad reduction at β. So the formula for $L_\beta(E/L,T)$ is also true for primes of bad reduction because it reduces to $L_\beta(E/L,T) = 1$. So,

$$\begin{aligned} L(E/L,s) &= \textstyle\prod_\beta L_\beta(E/L, q_\beta^{-s})^{-1} \\ &= \textstyle\prod_\beta (1 - \psi_{E/L}(\beta) q_\beta^{-s})^{-1} (1 - \overline{\psi_{E/L}(\beta)} q_\beta^{-s})^{-1} \\ &= L(s, \psi_{E/L}) L(s, \overline{\psi_{E/L}}). \end{aligned}$$

(b) In order to prove this part, we start by assuming that E has good reduction at β. Now if β splits in L' as $\beta\mathcal{O}_{L'} = \beta'\beta''$, then one can show that $q_\beta = q_{\beta'} = q_{\beta''}$ and moreover that $a_\beta = \psi_{E/L'}(\beta') + \psi_{E/L'}(\beta'')$. If, on the other hand, β remains inert in L', say $\beta\mathcal{O}_{L'} = \beta'$, then one can show that $q_\beta^2 = q_{\beta'}$ and that $a_\beta = 0$ and $\psi_{E/L'}(\beta') = -q_\beta$.

Finally, one can show that if $\widetilde{E}$ is the reduction of E modulo β, then $\widetilde{E}$ is ordinary if β splits in L' and supersingular if β is inert or ramifies in L'.

Now let β' be a prime of L' lying over β. If β ramifies in L', then E has bad reduction at β and if β is unramified in L', then E has good reduction at β if and only if E has good reduction at β'.

Finally, one shows that that the local L-series of E at β is given by:

$$L_\beta(E/L,T) = \begin{cases} (1 - \psi_{E/L'}(\beta')T)(1 - \psi_{E/L'}(\beta'')T) & \text{if } \beta\mathcal{O}_{L'} = \beta'\beta'' \text{ splits in } L' \\ 1 - \psi_{E/L'}(\beta')T & \text{if } \beta\mathcal{O}_{L'} = \beta' \text{ is inert in } L' \\ 1 & \text{if } \beta\mathcal{O}_{L'} = \beta'^2 \text{ ramifies in } L' \end{cases}$$

And, ultimately, one gets that the global L-series of E/L is given by $L(E/L,s) = L(s, \psi_{E/L'})$ which is the desired result.

□

Further analysis leads to the following stronger result.

Corollary 14. *Let E/L be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of K. The L-series of E admits an analytic continuation to the entire complex plane and satisfies a functional equation relating its values at s and $2 - s$. More precisely, define a function $\Lambda(E/L,s)$ as follows:*

(i) If $K \subset L$, let

$$\Lambda(E/L, s) = (N_{\mathbb{Q}}^{L}(\mathcal{D}_{L/\mathbb{Q}} c_{\psi}))^{s}((2\pi)^{-s}\Gamma(s))^{[L:\mathbb{Q}]} L(E/L, s),$$

where c_ψ is the conductor of the Grössencharacter $\psi_{E/L}$, $\mathcal{D}_{L/\mathbb{Q}}$ is the different of $L/\mathbb{Q}$ and $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt$ is the usual Γ-function.

(ii) If $K \not\subseteq L$, let $L' = LK$ and

$$\Lambda(E/L, s) = (N_{\mathbb{Q}}^{L'}(\mathcal{D}_{L'/\mathbb{Q}} c'_{\psi}))^{s}((2\pi)^{-s}\Gamma(s))^{[L:\mathbb{Q}]} L(E/L, s),$$

where c'_ψ is the conductor of the Grössencharacter $\psi_{E/L'}$.

Then Λ satisfies the functional equation

$$\Lambda(E/L, s) = w\Lambda(E/L, 2-s),$$

where the quantity $w = w_{E/L} \in \{\pm 1\}$ is called the sign of the functional equation of E/L.

References

[1] J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, New York, 1986.

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

[3] J.H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.

[4] J. Tate, *Fourier Analysis in Number Fields and Hecke's Zeta-Functions*, Algebraic Number Theory, J.W.S. Cassels and A. Frölich, eds., Academic Press, London, 1967, 305-347.