<table>
<thead>
<tr>
<th>Title</th>
<th>On p-adic L-functions attached to elliptic curves with complex multiplication and the Riemann-Hurwitz genus formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>AIBA, Akira</td>
</tr>
<tr>
<td>Citation</td>
<td>Bulletin of the Faculty of Science, Ibaraki University. Series A, Mathematics, 22: 23-28</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1990</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10109/3014">http://hdl.handle.net/10109/3014</a></td>
</tr>
</tbody>
</table>

このリポジトリに収録されているコンテンツの著作権は、それぞれの著作権者に帰属します。引用、転載、複製等される場合は、著作権法を遵守してください。
On $p$-adic $L$-functions attached to elliptic curves with complex multiplication and the Riemann-Hurwitz genus formula

AKIRA AIBA*

§0. Introduction

Let $K$ be a quadratic imaginary field and let $p$ be a prime number which splits in $K$, say $(p) = p^2$. Let $K_{\infty}$ be the unique $\mathbb{Z}_p$-extension of $K$ unramified outside $p$. Let $F$ be an abelian extension of $K$ of order prime to $p$ and $F_{\infty} = FK_{\infty}$. Let $M_{\infty}$ be the maximal abelian $\mathbb{Z}_p$-extension of $F_{\infty}$ unramified outside $p$. Write $X_{\infty}$ for the Galois group of $M_{\infty}$ over $F_{\infty}$, endowed with its natural action of the Galois group $Gal(F_{\infty}/K)$. Let $\Gamma = Gal(F_{\infty}/F)$. It is well known that $X_{\infty}$ is a finitely generated $\mathbb{Z}_p[\Gamma]$-torsion $\mathbb{Z}_p[\Gamma]$-module.


§1. Notations

Let $K$ be an imaginary quadratic field with the integer ring $\mathcal{O}$. Let $p$ be a rational prime which splits in $K$, say $(p) = p^2$. Let $K_{\infty}$ be the unique $\mathbb{Z}_p$-extension of $K$ unramified outside $p$ and let $K_n$ ($n = 0, 1, \ldots$) be the unique subfield of $K_{\infty}$ such that $[K_n : K] = p^n$. Let $F$ be an abelian extension of $K$ of order prime to $p$. Let $F_n = FK_n$ and $F_{\infty} = FK_{\infty}$. Let $\Gamma = Gal(F_{\infty}/F)$ be the Galois group of $F_{\infty}$ over $F$. Let $M_{\infty,F}$ be the maximal $p$-extension of $F_{\infty}$ unramified outside $p$. Write $X_{\infty,F} = Gal(M_{\infty,F}/F_{\infty})$, endowed with its natural action of $Gal(F_{\infty}/K)$. Let $f$ be an integral ideal of $K$ and let $K(f)$ be the ray class field mod $f$ of $K$. Let $K(fp) = \bigcup_n K(fp^n)$ and $G(f) = Gal(K(fp)/K)$. Let $\chi$ be a finite order character from $Gal(F_{\infty}/K)$ to $\mathbb{C}^\times$. Fix a homomorphism

$$\kappa : Gal(F_{\infty}/K) \simeq Gal(F_{\infty}/K_{\infty}) \times Gal(K_{\infty}/K) \rightarrow Gal(K_{\infty}/K) \simeq (1 + p\mathbb{Z}_p) \quad if \quad p \neq 2$$

$$\simeq (1 + 4\mathbb{Z}_p) \quad if \quad p = 2$$

Received March 27, 1990.

* Department of Mathematics, Ibaraki University, Mito, Ibaraki 310, Japan.
Suppose that \( f \) divides non \( p \)-part of the conductor of \( \chi \). We may assume that \( F \) is contained in \( K(\chi) \). Let \( E \) be an elliptic curve defined over \( K(\chi) \) with fixed Weierstrass model, satisfying the following two conditions. (1) \( E \) has complex multiplication by \( \mathfrak{a} \) with \( \text{grössencharacter} \ \psi \). Thus \( \psi \) is a homomorphism from the group of all fractional ideal of \( K(\chi) \) relatively prime to some ideal into \( \mathbb{Q} \).

(2) \( \psi(\mathfrak{a}) = \kappa(\mathfrak{a}N_{K(\chi)/K}^{\mathfrak{a}}) \) where \( \mathfrak{a} \) is an ideal relatively prime to \( pf \) and \( \mathfrak{a} = (a, F_{\infty}/K) \) is the Artin symbol of \( a \). Let \( L \) be the period lattice of \( E \). Replacing \( E \) by one of its conjugates, if necessary, we assume

\[
L = \Omega_f, \quad \Omega \in \mathbb{C}^\times
\]

Let \( \Omega_p \) be a \( p \)-adic period of \( E \). (See [1]) Let

\[
L_{\infty, f}(\chi \kappa^{-k}, s) = \frac{(s + k)}{(2\pi)^{s+k}} \sum_{(a, f) = 1} \frac{\chi \kappa^{-k}(\mathfrak{a})}{Na^s}
\]

where \( \mathfrak{a} = (a, F_{\infty}/K) \) be the Artin symbol of \( a \) and \( \Gamma(s) \) be the gamma function.

We follow the notation of [1] in reviewing the construction of the \( p \)-adic \( L \)-function \( L_{p, f}(\chi, s) \),

\[
\Omega_p^k L_{p, f}(\chi, k) = \Omega_p^k G(\chi \kappa^{-1})(1 - (\chi^{-1} \kappa^k(\mathfrak{a})) / \mathfrak{p}) L_{\infty, f}(\chi \kappa^{-k}, 0)
\]

\( 1 \leq k \in \mathbb{Z} \)

Here \( G(\chi \kappa^{-k}) \) is defined as follows. Let

\[
S = \{ \gamma \in \text{Gal}(K(\mathfrak{p}^n p^{\infty})/K) | \gamma|_{\text{Gal}(K(\mathfrak{p}^n)/K)} = (\mathfrak{p}^n, K(F_{\infty}/K)) \}
\]

where \( n \) is the exact power of \( p \) dividing the conductor of \( \chi \kappa^{-k} \) and \( \zeta_n \) is a primitive \( p \)-th root of unity. Then

\[
G(\chi \kappa^{-1}) = \frac{\kappa(\mathfrak{p}^n)}{p^n} \sum_{\gamma \in S} \chi(\gamma)(\zeta_n)^{-1}
\]

It is known that there exists a measure \( \mu_f \) on \( G(\chi) \) such that

\[
L_{p, f}(\chi, s) = \int_{G(\chi)} \chi^{-1} \kappa^*(\sigma) d\mu_f
\]

and a power series \( G_{p, f}(\chi, T) = \int_{G(\chi)} \chi^{-1}(\sigma)(1 + T)^{\kappa(\sigma)} d\mu_f \) such that

\[
L_{p, f}(\chi, s) = G_{p, f}(\chi; u^s - 1)
\]

where \( u = \kappa(\gamma_0) \) and \( \gamma_0 \) is a generator of \( \text{Gal}(K_{\infty}/K) \cong \text{Gal}(F_{\infty}/F) \). Let \( \mathfrak{o}' \) be the ring of integers in a finite extension of \( \mathbb{Q}_p \). Let \( f(T) = a_0 + a_1 T + a_2 T^2 + \ldots \in \Lambda = \mathfrak{o}'[[T]] \) be a non zero power series with coefficients in \( \mathfrak{o}' \). Let \( \mu(f) = \min\{\text{ord}_p a_i : i \geq 0\} \) be the \( \mu \)-invariant of \( f \) and \( \lambda(f) = \min\{i \geq 0 : \text{ord}_p a_i = \mu(f)\} \) be the \( \lambda \)-invariant of \( f \).
Two \( \Lambda \)-modules are said to be pseudo-isomorphic if there is a map between them with finite kernel and cokernel. Any finitely generated torsion \( \Lambda \)-module \( Y \) is pseudo-isomorphic to a module of the form \( \bigoplus \Lambda / f_i \Lambda \) for certain \( f_i \in \Lambda \), and the characteristic power series \( (\prod f_i) \) is a well-defined invariant of \( Y \) which we will denote by \( \text{char}(Y) \). It is well known that \( X_{\infty,F} \) is a finitely generated torsion \( \Lambda \)-module, with the action \( T x = (\gamma_0 - 1)x \). Let \( \mu_F = \mu(\text{char}(X_{\infty,F})) \) and let \( \lambda_F = \lambda(\text{char}(X_{\infty,F})) \). Let \( \mu_\chi(\chi) = \mu(G_{p,\chi}(\chi,T)) \) and let \( \lambda_\chi(\chi) = \lambda(G_{p,\chi}(\chi,T)) \).

If \( f \) is the non \( p \)-part of the conductor \( \chi \), we omit the subscript \( f \) from our notations: thus \( L_p(\chi,s) \), \( G_p(\chi,s) \), \( \mu(\chi) \), \( \lambda(\chi) \). If \( G \) is a group \( G \) denotes the character group of \( G \).

§2.

We use the next two important lemmas.

**Lemma 1.**

\[ \mu_F = 0 \]


The next lemma is a link between \( \mathbb{Z}_p \)-extension and \( L \)-function.

**Lemma 2.**

\[
\mu_F = \sum_{\alpha \in \text{Gal}(F_\infty/K_\infty)} \mu(\chi) \\
\lambda_F = \sum_{\chi \in \text{Gal}(F_\infty/K_\infty)} \lambda(\chi) + 1
\]

**Proof.** See de Shalit [1]

The next lemma gives some information on \( \lambda_\chi(\chi) \) when \( f \) is varied.

**Lemma 3.** Let \( \chi \) be a finite order character of \( \text{Gal}(F/K) \). Let \( f \) and \( f' \) be integral ideals of \( K \) which are divisible by the non-\( p \)-part of the conductor of \( \chi \), and suppose that \( f \) is divisible by \( f' \). Then

\[ \lambda_{f'}(\chi) = \lambda_f(\chi) + \sum g(q) \]

where the summation is taken over primes \( q \) which divides \( f'f^{-1} \) in \( K \) such that \( \chi(\sigma_q) \) has \( p \)-power order and \( g(q) \) denotes the number of places of \( K_\infty \) lying above \( q \).

**Proof.** Define a \( p \)-adic integer \( t(q) \) by \( \sigma_q \equiv \gamma_0^{\gamma_0^{t(q)}} \mod \text{Gal}(F/K) \) where \( \gamma_0 \) is a generator of \( \text{Gal}(K_\infty/K) \). Write

\[ -t(q) = p^a u \quad a \geq 0, \quad u \in \mathbb{Z}_p^\times. \]
From the definition,

\[ L_{p,t'}(\chi, s) = L_{p,t}(\chi, s) \prod (1 - \chi q^{-s}(q)) \]

\[ G_{p,t'}(\chi, T) = G_{p,t}(\chi, T) \prod E_q(T) \]

where the product is taken over primes \( q \) which divide \( f'f^{-1} \) in \( K \) and

\[ E_q(T) = (1 - \chi(q)(1 + T)^{-t(q)}) \]

Then

\[ E_q(T) \equiv 1 - \chi(q)(1 + T^{p^a})^u \mod p \sigma'(T) \]

\[ \equiv 1 - \chi(q) - \chi(q)uT^{p^a} \mod (p, T^{p^a+1} \sigma'(T)) \]

It follows that

\[ \mu(E_q(T)) = 0 \]

\[ \lambda(E_q(T)) = p \text{ if } \chi(q) \text{ is a } p \text{-power root of unity} \]

\[ = 0 \text{ otherwise} \]

Let \( D_q \) (resp. \( I_q \)) be the decomposition (resp. inertia) group of \( q \) for the extension \( K_{\infty}/K \). Then \( D_q/I_q \) is generated by

\[ \gamma_0 \mod \text{Gal}(F/K) \]

It follows that \( g(q) \) is finite and equal to \( p^a \)

q.e.d.

The next lemma gives some information on \( \lambda_f(\chi) \) when \( \chi \) is varied.

**Lemma 4.** Let \( \chi \) be a finite order character of \( \text{Gal}(F_{\infty}/K) \) and let \( \psi \) be a finite order character of \( \text{Gal}(F_{\infty}/K) \) of \( p \)-power order. Then

\[ \lambda_f(\chi) = \lambda_f(\chi \psi) \]

**Proof.** Let \( o_{\chi,\psi} \) be the ring of integers in a finite extension of \( \mathbb{Q}_p \) containing the values of both \( \chi \) and \( \psi \) and let \( \pi \) be a local parameter in \( o_{\chi,\psi} \).

Then since \( \psi \) has a \( p \)-power order,

\[ G_{p,f}(\chi \psi, T) - G_{p,f}(\chi, T) = \int (\psi^{-1}(\sigma) - 1)\chi^{-1}(\sigma)(1 + T)^{\kappa(\sigma)} d\mu_f \in \pi o_{\chi,\psi}[[T]] \]

Since \( \mu_f(\chi) = \mu_f(\chi \psi) = 0 \), the result is obtained.

q.e.d.

**Lemma 5.** Let \( \chi \) be a finite order character of \( \text{Gal}(F_{\infty}/K) \) and let \( \psi \) be a finite order character of \( \text{Gal}(F_{\infty}/K) \) of \( p \)-power order. Suppose that the order
of $\chi$ be prime to $p$. Let $L$ be the extension of $K$ corresponding to $\chi$ and let $L_\infty = LK_\infty$. Then

$$\lambda(\chi\psi) = \lambda(\chi) + N$$

where $N$ is the number of places $v$ on $K_\infty$ such that (1) $v$ doesn't lie above $p$ and $v|_K$ is ramified for $\psi$. (2) $v$ splits completely in $L_\infty$.

**Proof.** Let $f$ (resp. $f'$) be the non $p$-part of the conductor of $\chi$ (resp. $\chi\psi$). Since $\chi$ and $\psi$ have relatively prime orders, $f'$ is divisible by $f$. By Lemma 3 and Lemma 4,

$$\lambda(\chi\psi) = \lambda_{f'}(\chi\psi) = \lambda_f(\chi) = \lambda(\chi) + M$$

where $M = \sum g(q)$, the summation taken over places $q$, which divides $f'f^{-1}$ for which $\chi(\sigma_q)$ has $p$-power.

Since $\chi$ has order prime to $p$, $\chi(\sigma_q)$ is $p$-power order if and only if $\chi(\sigma_q) = 1$, that is $q$ splits completely in $L$. Then from the definition of $g(q)$, $M$ is the number of places $v$ on $K_\infty$ which split completely in $L_\infty$ and $v|_K = q$ is prime number which divides $f'f^{-1}$. Such $v$ satisfy (1) and (2). Conversely in $L$ and from the condition that order of $\chi$ is prime to order of $\psi$, $v|_K$ divides $f'f^{-1}$ q.e.d.

The next result is the main theorem.

**Theorem 6.** Notations are as usual as in §1. Let $H \supset F \supset K$ be a tower of abelian extensions such that $\text{Gal}(H/F)$ is $p$-power order and the order of $\text{Gal}(F/K)$ is prime to $p$. Let $\lambda_F$ and $\lambda_H$ be the $\lambda$-invariant of $X_{\infty,F}$ and $X_{\infty,H}$, respectively. Then

$$\lambda_H - 1 = [H_\infty : F_\infty](\lambda_F - 1) + \sum_w (e(w/v) - 1)$$

where the summation is taken over all places $w$ on $H_\infty$ which don't lie above $p$ and $v = w|_{F_\infty}$ and $e(w/v)$ denotes the ramification index of $w$ over $v$.

**Proof.** If $H \cap F_\infty$ doesn't contain $F$, take the subfield $H''$ of $H$ containing $F$ such that $H'' \cap F_\infty = F$, $H''_{\infty} = H_\infty$ and we may assume $H \cap F_\infty = F$.

We prove only the case when $[H : F] = p$ and $[F : K] = q$ ($p, q$: prime numbers of $p \neq q$). The other cases are the same way to prove.

Define $H'$ the subfield of $H$ such that $H \cong H' \times F$. We have a factorization

$$\prod_{\theta \in \text{Gal}(H/K)} L_p(\theta, s) = \prod_{\psi \in \text{Gal}(H'/K)} \prod_{\chi \in \text{Gal}(F/K)} L_p(\chi\psi, s)$$

and

$$G_p(\theta, T) = \prod \prod G_p(\chi\psi, T)$$

then

$$\sum \lambda(\theta) = \sum \sum \lambda(\chi\psi)$$

Let $N$ be the number of places $v$ of $K_\infty$ such that (1) $v$ doesn't lie above $p$ and $v|_K$ is ramified for $\psi$, where $\psi$ denotes a non-trivial character of $\text{Gal}(H'/K)$. 


Let $N'$ be the number of places $v$ of $K$ such that (1) and (2) $v$ splits completely in $F$. Then from the lemmas,

$$\sum_{\theta \in \text{Gal}(H/K)} \lambda(\theta) = \sum_{1 \neq \chi \in \text{Gal}(F/K)} (p\lambda(\chi) + (p - 1)N') + p\lambda(1) + (p - 1)N$$

$$= p \sum_{\chi \in \text{Gal}(F/K)} \lambda(\chi) + (p - 1)((q - 1)N' + N)$$

$$= p \sum_{\omega} \lambda(\chi) + \sum_{\omega} (e(w/v) - 1)$$

where the second summation is taken over the places $w$ of $H_\infty$ which don't lie above $p$. From Lemma 2, we obtain the result. q.e.d.

References