Journal of Number Theory **84**, 80–92 (2000)
doi:10.1006/jnth.2000.2510, available online at http://www.idealibrary.com on IDEAL®

An Analogue of Kida's Formula for the p-adic L-functions of Modular Elliptic Curves

Kazuo Matsuno[1]

Graduate School of Mathematical Sciences, University of Tokyo, 3-8-1, Komaba, Meguro-ku, Tokyo, 153-8914, Japan

Communicated by D. Goss

Received June 18, 1999

In this paper, we give a formula which describes the change of the λ-invariant of the p-adic L-function of a modular elliptic curve in a p-extension of Abelian fields. This formula is an analogue of Kida's formula.

Key Words: elliptic curve; p-adic L-function; Kida's formula.

1. INTRODUCTION

Let p be a prime number and K a CM-field. Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension and denote by K_n its nth layer. Let h_n^- be the relative class number of K_n. Then there exist integers $\lambda_K^- \geqslant 0, \mu_K^- \geqslant 0$ and ν_K^- such that

$$\mathrm{ord}_p(h_n^-) = \lambda_K^- n + \mu_K^- p^n + \nu_K^-$$

for all sufficiently large n (Iwasawa, cf. [14, Chapter 13]).

In [4], Kida gave a formula which describes the growth of λ^- in a p-extension of CM-fields under the assumption $\mu^- = 0$. (Kuz'min also gave an equivalent formula independently, cf. [5, Appendix 2].) In a special case, it is as follows: Let p be an odd prime number and L/K a p-extension of CM-fields. Assume that K contains primitive pth roots of unity and $\mu_K^- = 0$. Then we have $\mu_L^- = 0$ and the formula

$$2\lambda_L^- - 2 = [L_\infty : K_\infty](2\lambda_K^- - 2) + \sum_w (e_{L_\infty/K_\infty}(w) - 1),$$

where w runs over the primes of L_∞ which do not lie above p and split over the maximal real subfield of L_∞. For each w, we denote by $e_{L_\infty/K_\infty}(w)$ the ramification index of w in L_∞/K_∞. In [11], Sinnott gave another proof of this formula using p-adic L-functions.

[1] The author was supported by JSPS Research Fellowships for Young Scientists.

0022-314X/00 $35.00

In this paper, we study an analogue of this formula for the λ-invariants of the p-adic L-functions of modular elliptic curves. For a modular elliptic curve $E/\mathbb{Q}$, the p-adic L-function of E over an Abelian field K is constructed by Mazur and Swinnerton-Dyer [6] for the good ordinary case (the multiplicative case is due to [7]). As usual we will attach the λ-invariant $\lambda_E(K)$ and the μ-invariant $\mu_E(K)$ to it (see Section 2). Then our main result, Theorem 3.1, is as follows: Let L/K be a p-extension of Abelian fields. Assume that $\mu_E(K)=0$. Then, under the assumptions (Int) and (Add) given in Section 2, we have $\mu_E(L)=0$ and

$$\lambda_E(L) = [L_\infty : K_\infty]\, \lambda_E(K) + \sum_{w \in P_1} (e_{L_\infty/K_\infty}(w) - 1) + 2 \sum_{w \in P_2} (e_{L_\infty/K_\infty}(w) - 1),$$

where P_1 and P_2 are certain (finite) sets of primes of L_∞ defined in Theorem 3.1. We prove this formula by following the method of [11].

As in the case of number fields, it is conjectured that the p-adic L-function of E is related to the structure of the Selmer group of E (analogue of the Iwasawa main conjecture, cf. [6, Conjecture 3]). In particular, the invariants of the p-adic L-function should be equal to the invariants of "the characteristic polynomial" associated to the Selmer group of E/K_∞. Therefore there should be a similar formula for the Selmer groups. In [3], Y. Hachimori and the author gave such a formula. The result given there and the result in this paper are of the same form as expected by the main conjecture.

We note that some numerical examples of our result will be found in [2].

Notation. Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and $\mathbb{C}_p$ the completion of an algebraic closure of $\mathbb{Q}_p$. We fix an embedding of $\bar{\mathbb{Q}}$ in $\mathbb{C}_p$. Then we may regard the values of any Dirichlet character χ as lying in $\mathbb{C}_p$. We write $\mathbb{Z}_p[\chi]$ for the ring generated by all values of χ over $\mathbb{Z}_p$.

We denote by $\#M$ the number of elements of a finite set M. For any Abelian group A and any integer $n \geqslant 1$, we denote by A_n the kernel of the multiplication by n. For any finite Abelian group G, we denote by $\hat{G}$ its character group.

2. P-ADIC L-FUNCTIONS

Let p be an odd prime number. Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension with $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. Let γ_0 be a topological generator of Γ. For any finite extension $F/\mathbb{Q}$, put $F_\infty = F\mathbb{Q}_\infty$.

Let $E/\mathbb{Q}$ be a modular elliptic curve which has good ordinary reduction or multiplicative reduction at p. Let N_E be the conductor of E, and define a Dirichlet character ε by

$$\varepsilon(a) = \begin{cases} 1 & \text{if} \quad (a, N_E) = 1, \\ 0 & \text{if} \quad (a, N_E) \neq 1. \end{cases}$$

Let

$$f(z) = \sum_{n=1}^{\infty} a_n q^n \ (q = e^{2\pi i z})$$

be the normalized newform of weight 2 and of level N_E associated to E. By the assumption on the reduction type of E at p, we have $a_p \not\equiv 0 \pmod{p}$. Hence the polynomial $X^2 - a_p X + \varepsilon(p)\, p$ has a unique root which lies in $\mathbb{Z}_p^{\times}$ and we denote it by $\alpha \in \mathbb{Z}_p^{\times}$.

The p-adic L-function of E is obtained by the p-adic Mellin transform of a p-adic measure constructed using modular symbols. We recall the construction of such p-adic measures and p-adic L-functions following [7, Chapter I]. Let $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{i\infty\}$ and define $\Phi\colon \mathbb{P}^1(\mathbb{Q}) \to \mathbb{C}$ by

$$\Phi(r) = \int_{i\infty}^{r} f(q)\, \frac{dq}{q}.$$

Since f is an eigenform of Hecke operators, Φ satisfies the formula

$$a_l \Phi(r) = \sum_{u=0}^{l-1} \Phi\left(\frac{r+u}{l}\right) + \varepsilon(l)\, \Phi(lr) \tag{1}$$

for any prime l and any $r \in \mathbb{Q}$ (cf. [7, Chapter I, Proposition 4.2]). For any integer m prime to p, we put

$$\mathbb{Z}_{p,m} := \varprojlim_n (\mathbb{Z}/p^n m\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z}) \times \mathbb{Z}_p,$$

$$\mathbb{Z}_{p,m}^{\times} := \varprojlim_n (\mathbb{Z}/p^n m\mathbb{Z})^{\times} = (\mathbb{Z}/pm\mathbb{Z})^{\times} \times (1 + p\mathbb{Z}_p).$$

Then we define a measure $\nu_{E,m}^{*}$ on $\mathbb{Z}_{p,m}^{\times}$ by

$$\nu_{E,m}^{*}(a + p^n m \mathbb{Z}_{p,m}) = \alpha^{-n-1} \left(\alpha \Phi\left(\frac{a}{p^n m}\right) - \varepsilon(p)\, \Phi\left(\frac{a}{p^{n-1} m}\right) \right)$$

for $n \geqslant 1$, $a \in (\mathbb{Z}/p^n m\mathbb{Z})^\times$. This measure takes values in $\mathscr{L}(E) \otimes \mathbb{Q}_p$, where $\mathscr{L}(E)$ is the period lattice of E with respect to a Néron differential ω_E on $E/\mathbb{Q}$

$$\mathscr{L}(E) := \mathrm{Image}(H_1(E_{\mathbb{C}}, \mathbb{Z}) \xrightarrow{\int \omega_E} \mathbb{C})$$

(cf. [12, Sections 2, 4]). It is conjectured that $v^*_{E,m}$ satisfies the following integrality ([12, Conjecture IV]):

$$(\mathrm{Int})\ v^*_{E,m} \text{ takes values in } \mathscr{L}(E) \otimes \mathbb{Z}_p.$$

For the rest of this paper, we assume (Int). Stevens proved that $v^*_{E,m}$ takes values in $\mathscr{L}(E) \otimes (c_E^{-1}\mathbb{Z}_p)$ for some non-zero integer c_E which depends only on E ([12, Theorem 4.6], see also [13]). In particular, (Int) holds for almost all primes at which E has good ordinary reduction.

Let $\mathscr{L}(E)^\pm$ denote the submodules of $\mathscr{L}(E)$ on which the complex conjugation acts as multiplication by ± 1. Since p is odd, we can decompose $\mathscr{L}(E) \otimes \mathbb{Z}_p$ as

$$\mathscr{L}(E) \otimes \mathbb{Z}_p \cong (\mathscr{L}(E)^+ \otimes \mathbb{Z}_p) \oplus (\mathscr{L}(E)^- \otimes \mathbb{Z}_p).$$

Let $v^\pm_{E,m}$ be the decomposition of $v^*_{E,m}$ associated to them. By fixing isomorphisms $\mathscr{L}(E)^\pm \cong \mathbb{Z}$, we may regard $v^\pm_{E,m}$ as measures which take values in $\mathbb{Z}_p$. Thus we have a $\mathbb{Z}_p$-valued measure $v_{E,m} := v^+_{E,m} + v^-_{E,m}$.

Let $\langle\ \rangle : \mathbb{Z}^\times_{p,m} \to 1 + p\mathbb{Z}_p$ be the natural projection and $\kappa : \Gamma \to 1 + p\mathbb{Z}_p$ the cyclotomic character. Define $t : \mathbb{Z}^\times_{p,m} \to \mathbb{Z}_p$ by $\langle x \rangle = \kappa(\gamma_0)^{t(x)}$ for $x \in \mathbb{Z}^\times_{p,m}$.

Let χ be a character of $\mathbb{Z}^\times_{p,m}$ of finite order. We may regard χ as a Dirichlet character of conductor $p^n m'$ for some $n \geqslant 0$ and $m' \mid m$. Then we call this m' the p'-conductor of χ. For such a χ, we define

$$G_{p,m}(E, \chi, T) := \int_{\mathbb{Z}^\times_{p,m}} \chi(x)(1+T)^{t(x)}\, dv_{E,m}.$$

Since $v^\pm_{E,m}(-U) = \pm v^\pm_{E,m}(U)$ for any open compact set $U \subset \mathbb{Z}^\times_{p,m}$, we have

$$G_{p,m}(E, \chi, T) = \int_{\mathbb{Z}^\times_{p,m}} \chi(x)(1+T)^{t(x)}\, dv^{\mathrm{sgn}(\chi)}_{E,m}, \tag{2}$$

where $\mathrm{sgn}(\chi)$ is the sign of $\chi(-1)$ (cf. [6, p. 51]). If χ has p'-conductor m, we simply denote $G_{p,m}(E, \chi, T)$ by $G_p(E, \chi, T)$. It is known that $G_p(E, \chi, T)$ is non-zero for any χ as an immediate consequence of [8, Theorem 1].

The p-adic L-function of E associated to χ is defined as

$$L_p(E, \chi, s) = G_p(E, \chi, \kappa(\gamma_0)^{s-1} - 1)$$

(see [7, p. 19], [12, p. 93]). In this paper, we treat only $G_p(E, \chi, T)$ and we call this also the p-adic L-function of E (associated to χ).

Next, we will define the p-adic L-function of E over an Abelian field K as in [6, p. 52]. Let S_{add} be the set of prime numbers at which E has additive reduction. We assume the following condition on K:

(Add) E has also additive reduction at any prime of K lying above S_{add}.

If $E/\mathbb{Q}$ is semistable, any number field satisfies (Add) trivially. Moreover, if $p \geqslant 5$ and K satisfies (Add), any pro-p-extension of K also satisfies (Add). Indeed, if there exists a p-extension L of K which does not satisfy (Add), then p must divide $\#\mathrm{Aut}(E(\bar{\mathbb{Q}})_l) = (l^2-1)(l^2-l)$ for almost all primes $l \geqslant 3$ (cf. [9, p. 498]).

Under (Add), we define the p-adic L-function $G_p(E/K, T)$ by the formula

$$G_p(E/K, (1+T)^{p^n}-1) = \prod_{\chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})}} G_p(E, \chi, T),$$

where n is the integer such that $K \cap \mathbb{Q}_\infty = \mathbb{B}_n$, where $\mathbb{B}_n$ is the nth layer of $\mathbb{Q}_\infty/\mathbb{Q}$. Such a power series exists uniquely (cf. [14, Lemma 13.39]), and it is contained in $\mathbb{Z}_p[[T]]$ under (Int).

Let $\mathcal{O}$ be the integer ring of a finite extension of $\mathbb{Q}_p$. It is known that any non-zero power series $F(T) \in \mathcal{O}[[T]]$ is uniquely decomposed as

$$F(T) = \pi^{\mu} P(T)\, U(T),$$

where $U(T) \in \mathcal{O}[[T]]^{\times}$, $P(T) \in \mathcal{O}[T]$ is a distinguished polynomial and π is a fixed prime element of $\mathcal{O}$ (p-adic Weierstrass preparation theorem, cf. [14, Theorem 7.3]). As usual, we put $\lambda(F) := \deg(P(T))$ and $\mu(F) := \mu \operatorname{ord}_p(\pi)$ in this notation. We denote

$$\lambda_E(K) := \lambda(G_p(E/K, T)), \mu_E(K) := \mu(G_p(E/K, T)).$$

Similarly denote

$$\lambda_{E,m}(\chi) := \lambda(G_{p,m}(E, \chi, T)), \mu_{E,m}(\chi) := \mu(G_{p,m}(E, \chi, T))$$

for $G_{p,m}(E, \chi, T)$. If χ has p'-conductor m, we denote them simply by $\lambda_E(\chi), \mu_E(\chi)$.

We now remark how the p-adic L-function changes by isogenies. Let $E'/\mathbb{Q}$ be an elliptic curve and $\varphi: E \to E'$ an isogeny over $\mathbb{Q}$.

PROPOSITION 2.1. *Let K be an Abelian field which satisfies* (Add). *Then there exists a non-zero $c \in \mathbb{Q}$ such that $G_p(E'/K, T) = cG_p(E/K, T)$. In particular, we have $\lambda_{E'}(K) = \lambda_E(K)$.*

Remark. The μ-invariant may change by isogeny. An explicit formula of the change is given in [12] (Proposition 4.12).

Proof. Since φ is extended to the morphism between the Néron models of E and E', there exists a non-zero integer a such that $\varphi^*\omega_{E'} = a\omega_E$. By the definition of $\mathscr{L}(E)$, we have $a\mathscr{L}(E)^{\pm} \subset \mathscr{L}(E')^{\pm}$. In particular, $\mathscr{L}(E)^{\pm} \otimes \mathbb{Q} \cong \mathscr{L}(E')^{\pm} \otimes \mathbb{Q}$. On the other hand, the modular symbol Φ does not change by φ since Φ is defined by $f(z)$ which depends only on the isogeny class. Therefore $v^{\pm}_{E',m}$ is equal to $v^{\pm}_{E,m}$ up to multiplication by a rational constant. By (2), we have the assertion of this proposition. ∎

At the end of this section, we give a lemma needed for the proof of our main theorem. This is already given in [6] (Section 8, Lemma 2) although the proof is omitted. Since there seems to be a slight error in the statement, we will correct it and give a proof here. Let l be a prime such that $l \nmid pm$ and let $\phi\colon \mathbb{Z}^{\times}_{p,ml} \to \mathbb{Z}^{\times}_{p,m}$ be the natural projection.

LEMMA 2.2. *For any open compact set $U \subset \mathbb{Z}^{\times}_{p,m}$, we have*

$$v_{E,ml}(\phi^{-1}(U)) = a_l v_{E,m}(U) - v_{E,m}(l^{-1}U) - \varepsilon(l)\, v_{E,m}(lU).$$

Proof. It suffices to treat the case $U = a + p^n m\mathbb{Z}_{p,m}$, $(a, pm) = 1$. Furthermore, we may choose a such that $l \nmid a$. Then we have

$$\phi^{-1}(U) = \coprod_{\substack{b \in (\mathbb{Z}/p^n ml\mathbb{Z})^{\times} \\ b \equiv a (\mathrm{mod}\, p^n m)}} b + p^n ml\mathbb{Z}_{p,ml}.$$

By (1), we have

$$a_l v^*_{E,m}(U) = \sum_{u=0}^{l-1} \left(\alpha^{-n} \Phi\left(\frac{a + up^n m}{p^n ml}\right) - \varepsilon(p)\, \alpha^{-n-1} \Phi\left(\frac{a + up^{n-1} m}{p^{n-1} ml}\right)\right)$$
$$+ \varepsilon(l)\left(\alpha^{-n} \Phi\left(\frac{al}{p^n m}\right) - \varepsilon(p)\, \alpha^{-n-1} \Phi\left(\frac{al}{p^{n-1} m}\right)\right).$$

Since $a + up^n m$ runs through a complete set of residue class modulo $p^n ml$ which is congruent to a (mod $p^n m$), we have

$$\sum_{u=0}^{l-1} \Phi\left(\frac{a + up^n m}{p^n ml}\right) = \sum_{\substack{b \in (\mathbb{Z}/p^n ml\mathbb{Z})^{\times} \\ b \equiv a (\mathrm{mod}\, p^n m)}} \Phi\left(\frac{b}{p^n ml}\right) + \Phi\left(\frac{al'}{p^n m}\right)$$

for $l' \in \mathbb{Z}$ such that $ll' \equiv 1$ (mod $p^n m$). We have a similar formula for $a + up^{n-1} m$. Hence we get

$$a_l v^*_{E,m}(U) = v^*_{E,ml}(\phi^{-1}(U)) + v^*_{E,m}(l^{-1}U) + \varepsilon(l)\, v^*_{E,m}(lU).$$

Decomposing this by the action of the complex conjugation, we have the statement of Lemma 2.2. ∎

3. AN ANALOGUE OF KIDA'S FORMULA

In this section, we will give the following theorem which is an analogue of Kida's formula for the p-adic L-functions of elliptic curves. We follow the notations in the preceding section and keep the assumption (Int).

THEOREM 3.1. *Let L/K be a p-extension of Abelian fields satisfying the assumption* (Add). *We further assume that $\mu_E(K)=0$. Then, under* (Int), *we have $\mu_E(L)=0$ and*

$$\lambda_E(L) = [L_\infty : K_\infty]\, \lambda_E(K) + \sum_{w \in P_1} (e_{L_\infty/K_\infty}(w)-1) + 2 \sum_{w \in P_2} (e_{L_\infty/K_\infty}(w)-1),$$

where P_1 and P_2 are the sets of primes of L_∞ which are defined as

$$P_1 = \{ w \mid w \nmid p,\ E\text{: split multiplicative reduction at } w \},$$

$$P_1 = \{ w \mid w \nmid p,\ E\text{: good reduction at } w,\ E(L_{\infty,w})_p \neq 0 \},$$

and $e_{L_\infty/K_\infty}(w)$ denotes the ramification index of w in L_∞/K_∞.

Remark. By Proposition 2.1, the formula of the λ-invariants in the above theorem holds without the assumption $\mu_E(K)=0$ if there exists an elliptic curve E' isogenous to E such that $\mu_{E'}(K)=0$.

For each prime l and any algebraic extension $F/\mathbb{Q}$, we denote by $g_F(l)$ the number of primes of F lying above l (if it is finite). Let χ be a character of $\mathbb{Z}_{p,m}^{\times}$ of finite order and π a prime element of $\mathbb{Z}_p[\chi]$. We define an integer $g_\chi(l)$ as follows:

(i) If $\chi(l) \neq 0$ and $l \nmid N_E$,

$$g_\chi(l) = \begin{cases} 0 & \text{if } a_l \not\equiv \chi(l) + \chi^{-1}(l) \pmod{\pi}, \\ g_{\mathbb{Q}_\infty}(l) & \text{if } a_l \equiv \chi(l) + \chi^{-1}(l),\ a_l \not\equiv \pm 2 \pmod{\pi}, \\ 2g_{\mathbb{Q}_\infty}(l) & \text{otherwise.} \end{cases}$$

(ii) If $\chi(l) \neq 0$ and $l \mid N_E$,

$$g_\chi(l) = \begin{cases} 0 & \text{if } a_l \not\equiv \chi^{-1}(l) \pmod{\pi}, \\ g_{\mathbb{Q}_\infty}(l) & \text{if } a_l \equiv \chi^{-1}(l) \pmod{\pi}. \end{cases}$$

(iii) If $\chi(l) = 0$, then $g_\chi(l) = 0$.

We now prove the following two lemmas needed to prove Theorem 3.1. These lemmas correspond to [11, Proposition 2.1], [11, Lemma 2.1] respectively, and one can prove these in the similar way. We use Lemma 2.2 to prove the latter.

LEMMA 3.2. *Let χ and ψ be characters of $\mathbb{Z}_{p,m}^\times$ of finite order. Assume that ψ has a p-power order and $\mu_{E,m}(\chi) = 0$. Then we have*

$$\lambda_{E,m}(\chi\psi) = \lambda_{E,m}(\chi), \qquad \mu_{E,m}(\chi\psi) = 0.$$

Proof. Let π be a prime element of $\mathbb{Z}_p[\chi\psi]$. Since ψ has a p-power order, $\psi(x)$ is congruent to 1 modulo π for any $x \in \mathbb{Z}_{p,m}^\times$. Hence we have

$$G_{p,m}(E, \chi\psi, T) \equiv G_{p,m}(E, \chi, T) \pmod{\pi}.$$

Therefore we have $\mu_{E,m}(\chi\psi) = 0$ by the assumption $\mu_{E,m}(\chi) = 0$, and then we have $\lambda_{E,m}(\chi\psi) = \lambda_{E,m}(\chi)$ by the definition of the λ-invariants. ∎

LEMMA 3.3. *Let χ be a character of $\mathbb{Z}_{p,m}^\times$ of finite order and l a prime number such that $l \nmid pm$. Assume that the order of χ is prime to p. Then we have*

$$\lambda_{E,ml}(\chi) = \lambda_{E,m}(\chi) + g_\chi(l), \qquad \mu_{E,ml}(\chi) = \mu_{E,m}(\chi).$$

Proof. Since $t(ab) = t(a) + t(b)$ for any $a, b \in \mathbb{Z}_{p,m}^\times$, we have

$$\begin{aligned} &G_{p,ml}(E, \chi, T) \\ &\quad = \int_{\mathbb{Z}_{p,ml}^\times} \chi(x)(1+T)^{t(x)}\, dv_{E,ml} \\ &\quad = \int_{\mathbb{Z}_{p,m}^\times} \left(a_l \chi(x)(1+T)^{t(x)} - \chi\left(\frac{x}{l}\right)(1+T)^{t(x/l)} \right. \\ &\qquad \left. - \varepsilon(l)\, \chi(lx)(1+T)^{t(lx)} \right) dv_{E,m} \\ &\quad = (a_l - \chi^{-1}(l)(1+T)^{-t(l)} - \varepsilon(l)\, \chi(l)(1+T)^{t(l)})\, G_{p,m}(E, \chi, T) \end{aligned}$$

by Lemma 2.2. Hence, if we put

$$h_l(E, \chi, T) = a_l - \chi^{-1}(l)(1+T)^{-t(l)} - \varepsilon(l)\, \chi(l)(1+T)^{t(l)}$$

then we have

$$\lambda_{E,ml}(\chi)=\lambda_{E,m}(\chi)+\lambda(h_l(E,\chi,T)),$$
$$\mu_{E,ml}(\chi)=\mu_{E,m}(\chi)+\mu(h_l(E,\chi,T)).$$

Write $t(l)=up^a$ with $a\geqslant 0$, $u\in\mathbb{Z}_p^\times$. Then we have $p^a=g_{\mathbb{Q}_\infty}(l)$. Indeed, we have

$$\kappa(\gamma_0)^{t(l)}=\langle l\rangle=\kappa(\sigma_l),$$

where $\sigma_l\in\Gamma$ is the Frobenius element of l, thus the index of the decomposition group of l in Γ is p^a.

We calculate the λ,μ-invariant of $h_l(E,\chi,T)$.

(i) If $l\nmid N_E$,

$$\begin{aligned}h_l(E,\chi,T)&=a_l-\chi^{-1}(l)(1+T)^{-up^a}-\chi(l)(1+T)^{up^a}\\&\equiv a_l-(\chi(l)+\chi^{-1}(l))-(\chi(l)-\chi^{-1}(l))\,uT^{p^a}\\&\quad-\left(\frac{\chi(l)+\chi^{-1}(l)}{2}u^2-\frac{\chi(l)-\chi^{-1}(l)}{2}u\right)T^{2p^a}\\&\qquad\qquad(\mathrm{mod}(p,T^{2p^a+1})).\end{aligned}$$

If $\chi(l)-\chi^{-1}(l)$ is divisible by π, we have $\chi(l)\equiv\pm 1\pmod{\pi}$. Then $\chi(l)+\chi^{-1}(l)$ is not divisible by π since p is odd. Thus we have $\mu(h_l(E,\chi,T))=0$ and, by the definition of the λ-invariant, $\lambda(h_l(E,\chi,T))=g_\chi(l)$.

(ii) If $l\mid N_E$,

$$h_l(E,\chi,T)\equiv a_l-\chi^{-1}(l)+\chi^{-1}(l)\,uT^{p^a}\qquad(\mathrm{mod}(p,T^{p^a+1})).$$

Hence we have $\mu(h_l(E,\chi,T))=0$, $\lambda(h_l(E,\chi,T))=g_\chi(l)$.

This completes the proof. ∎

Next, we prove the following lemma.

LEMMA 3.4. *Let K be an Abelian field which satisfies* (Add). *Let l be a prime number and v a prime of K lying above l. Assume that $p\nmid[K:\mathbb{Q}]$ and $l\equiv 1\pmod{p}$. Then we have*

$$\sum_{\chi\in\widehat{\mathrm{Gal}(K/\mathbb{Q})}}g_\chi(l)=\begin{cases}2g_{K_\infty}(l) & \text{if } E\text{: good reduction at } v \text{ and } E(K_v)_p\neq 0,\\ g_{K_\infty}(l) & \text{if } E\text{: split multiplicative reduction at } v,\\ 0 & \text{otherwise.}\end{cases}$$

Remark. Let M be a non-zero finite abelian p-group with an action of a p-group G. Then the subgroup of G-invariant elements M^G is also non-zero. By this fact, we can show that $E(K_{\infty,\bar{v}})_p \neq 0 \Leftrightarrow E(K_v)_p \neq 0$ for any prime $\bar{v}$ of K_∞ above v.

Proof. We denote $\chi(l) \pmod{\pi}$ by $\zeta_\chi \in \bar{\mathbb{F}}_p$ for each χ. Since $p \nmid [K:\mathbb{Q}]$, the order of ζ_χ coincides with that of $\chi(l)$. We first assume that $l \nmid N_E$, i.e., E has good reduction at l. Let $\alpha \in \bar{\mathbb{F}}_p$ be one of the root of the polynomial $x^2 - a_l x + 1 \pmod{p}$. By the definition of $g_\chi(l)$, we have

$$\sum_\chi g_\chi(l) = g_{\mathbb{Q}_\infty}(l)\,(\#\{\chi \mid \zeta_\chi = \alpha\} + \#\{\chi \mid \zeta_\chi = \alpha^{-1}\}).$$

Here we note that $\alpha = \alpha^{-1}$ is equivalent to $a_l \equiv \pm 2 \pmod{p}$. Let

$$Y = \{\chi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})} \mid \chi(l) \neq 0\}, \qquad Z = \{\chi \in Y \mid \chi(l) = 1\},$$

and denote by f the residue degree of l in $K/\mathbb{Q}$. Then the following facts (A) and (B) are well-known (cf. [14, Theorem 3.7]):

(A) Y/Z is cyclic of order f,

(B) the order of Z is equal to $g_K(l)$.

By these facts, we can easily show that

$$\sum_\chi g_\chi(l) = \begin{cases} 2g_{\mathbb{Q}_\infty}(l)\, g_K(l) & \text{if } \alpha^f = 1, \\ 0 & \text{if } \alpha^f \neq 1. \end{cases}$$

Since $p \nmid [K:\mathbb{Q}]$, we have $g_{K_\infty}(l) = g_{\mathbb{Q}_\infty}(l)\, g_K(l)$. Hence it suffices to show that $E(K_v)_p \neq 0 \Leftrightarrow \alpha^f = 1$. Let $\tilde{E}$ be the reduction of E modulo l and k_v the residue field of K_v. Then $E(K_v)_p$ is isomorphic to $\tilde{E}(k_v)_p$, (cf. [10, Chapter VII, Proposition 3.1]). Since $l \equiv 1 \pmod{p}$, the characteristic polynomial of the action of the Frobenius element of l on $\tilde{E}(\bar{\mathbb{F}}_l)_p$ is just $x^2 - a_l x + 1 \pmod{p}$. Hence α^f is one of the eigenvalues of the action of the Frobenius of v on $\tilde{E}(\bar{\mathbb{F}}_l)_p$. Thus $\tilde{E}(k_v)_p \neq 0$ is equivalent to $\alpha^f = 1$.

Assume that $l \mid N_E$. Let $\alpha := (a_l \bmod p)$ in this case. Then, again by the definition of $g_\chi(l)$ and by the facts (A), (B),

$$\begin{aligned} \sum_\chi g_\chi(l) &= g_{\mathbb{Q}_\infty}(l) \#\{\chi \in Y \mid \zeta_\chi^{-1} = \alpha\} \\ &= \begin{cases} g_{\mathbb{Q}_\infty}(l)\, g_K(l) & \text{if } \alpha^f = 1, \\ 0 & \text{if } \alpha^f \neq 1. \end{cases} \end{aligned}$$

If E has split multiplicative reduction at l, then $\alpha = 1$. Assume that E has non-split multiplicative reduction at l. Then $\alpha = -1$. Hence $\alpha^f = 1$ if and

only if f is even, and this is equivalent to the condition that E has split multiplicative reduction at v. If E has additive reduction at l, then $\alpha = 0$ and E has also additive reduction at v by (Add). Thus we have

$$\sum_{\chi} g_{\chi}(l) = \begin{cases} g_{K_\infty}(l) & \text{if } E \text{ has split multiplicative reduction at } v, \\ 0 & \text{otherwise} \end{cases}$$

in the case $l \mid N_E$. The proof is completed. ∎

Now we begin the proof of Theorem 3.1. By the following lemma, we may assume that $p \nmid [K : \mathbb{Q}]$ without loss of generality:

LEMMA 3.5. *Let K, L and M be Abelian fields satisfying* (Add). *Assume that $K \subset L \subset M$ and $[M : K]$ is a power of p. If the assertion of Theorem* 3.1 *holds for two of the extensions L/K, M/L, M/K, it holds for the remaining one.*

Proof. Let v be a prime of L_∞ which does not lie above p. Let g be the number of primes of M_∞ lying above v. Since there exists no p-extension of the residue field of L_∞ at v, we have $[M_\infty : L_\infty] = e_{M_\infty/L_\infty}(w)\, g$. Hence we have a formula

$$[M_\infty : L_\infty](e_{L_\infty/K_\infty}(v) - 1) = \sum_{w} (e_{M_\infty/K_\infty}(w) - e_{M_\infty/L_\infty}(w)),$$

where w runs over all primes of M_∞ lying above v. This implies Lemma 3.5. ∎

Take the maximal subfield L' of L such that $[L' : \mathbb{Q}]$ is a p-power. Then $K \cap L' = \mathbb{Q}$ by the assumption $p \nmid [K : \mathbb{Q}]$, and hence any character of $\mathrm{Gal}(L/\mathbb{Q})$ is uniquely written as a product of a character χ of $\mathrm{Gal}(K/\mathbb{Q})$ and a character ψ of $\mathrm{Gal}(L'/\mathbb{Q})$. We regard these characters as Dirichlet characters. Let n denote the integer such that $L \cap \mathbb{Q}_\infty = \mathbb{B}_n$, where $\mathbb{B}_n$ is the nth layer of $\mathbb{Q}_\infty/\mathbb{Q}$. Note that $K \cap \mathbb{Q}_\infty = \mathbb{Q}$. Then we have

$$p^n \lambda_E(L) = \sum_{\psi} \sum_{\chi} \lambda_E(\chi\psi), \qquad \lambda_E(K) = \sum_{\chi} \lambda_E(\chi),$$

$$\mu_E(L) = \sum_{\psi} \sum_{\chi} \mu_E(\chi\psi), \qquad \mu_E(K) = \sum_{\chi} \mu_E(\chi).$$

Let m (resp. m') denote the p'-conductor of χ (resp. $\chi\psi$). Since the order of χ is prime to p and that of ψ is a p-power, m' is divisible by m and m'/m is square-free. By Lemmas 3.2 and 3.3, we have $\mu_E(\chi\psi) = 0$ and

$$\lambda_E(\chi\psi) = \lambda_{E,m'}(\chi) = \lambda_E(\chi) + \sum_{l \mid m'} g_{\chi}(l)$$

(recall that $g_\chi(l)=0$ if $l \mid m$). Hence we have $\mu_E(L)=0$ and

$$p^n \lambda_E(L) = [L' : \mathbb{Q}]\, \lambda_E(K) + \sum_{l \neq p} \#\{\psi \mid \psi(l)=0\} \sum_{\chi} g_\chi(l). \tag{3}$$

Since $L' \cap K = \mathbb{Q}$ and $L \cap K_\infty = K_n$, we have $[L' : \mathbb{Q}] = p^n [L_\infty : K_\infty]$. Furthermore, since l is unramified in $\mathbb{Q}_\infty/\mathbb{Q}$, we have $e_{L'/\mathbb{Q}}(l) = e_{L_\infty/K_\infty}(w)$, where w is any prime of L_∞ lying above l. By the facts (A) and (B) in the proof of Lemma 3.4, we have

$$\begin{aligned} \#\{\psi \mid \psi(l)=0\} &= [L' : \mathbb{Q}](1 - e_{L'/\mathbb{Q}}(l)^{-1}) \\ &= p^n [L_\infty : K_\infty](1 - e_{L_\infty/K_\infty}(w)^{-1}). \end{aligned}$$

On the other hand, by Lemma 3.4, we have $\sum_\chi g_\chi(l) = \delta_w\, g_{K_\infty}(l)$, where

$$\delta_w = \begin{cases} 2 & \text{if} \quad w \in P_2, \\ 1 & \text{if} \quad w \in P_1, \\ 0 & \text{otherwise} \end{cases}$$

(see the remark after Lemma 3.4, and that L_∞ satisfies (Add) since L_∞/L is unramified outside the primes above p). Hence, for each $l \neq p$, we have

$$\begin{aligned} &\#\{\psi \mid \psi(l)=0\} \sum_{\chi} g_\chi(l) \\ &\quad = p^n [L_\infty : K_\infty]\, g_{K_\infty}(l)\, \delta_w (1 - e_{L_\infty/K_\infty}(w)^{-1}) \\ &\quad = p^n [L_\infty : K_\infty]\, g_{K_\infty}(l)\, g_{L_\infty}(l)^{-1} \sum_{w \mid l} \delta_w (1 - e_{L_\infty/K_\infty}(w)^{-1}). \end{aligned}$$

As in the proof of Lemma 3.5, $g_{L_\infty}(l) = [L_\infty : K_\infty]\, e_{L_\infty/K_\infty}(w)^{-1}\, g_{K_\infty}(l)$. Hence we have

$$\lambda_E(L) = [L_\infty : K_\infty]\, \lambda_E(K) + \sum_{w \nmid p} \delta_w (e_{L_\infty/K_\infty}(w) - 1)$$

by (3). We have completed the proof of Theorem 3.1.

ACKNOWLEDGMENTS

This paper is based on the master's thesis of the author. He expresses his sincere gratitude to his advisor Professor Shoichi Nakajima for appropriate advice and warm encouragement. Thanks are also due to Yoshitaka Hachimori for many valuable discussions and suggestions.

REFERENCES

1. G. Gras, "Sur les invariants "lambda" d'Iwasawa des corps abéliens," Théorie des Nombres, Besançon, 1978–1979, Exp. no. 5.
2. Y. Hachimori, Computation of the invariants of p-adic L-functions attached to modular elliptic curves, in preparation.
3. Y. Hachimori and K. Matsuno, An analogue of Kida's formula for the Selmer groups of elliptic curves, *J. Algebraic Geom.* **8** (1999), 581–601.
4. Y. Kida, l-extensions of CM-fields and cyclotomic invariants, *J. Number Theory* **12** (1980), 519–528.
5. L. V. Kuz'min, Some duality theorems for cyclotomic Γ-extensions of algebraic number fields of CM type, *Izv. Akad. Nauk. SSSR* **43** (1979), 483–546; (English transl.) *Math. USSR-Izv.* **14** (1980), 441–498.
6. B. Mazur and P. Swinnerton-Dyer, Arithmetic of Weil curves, *Invent. Math.* **25** (1974), 1–61.
7. B. Mazur, J. Tate, and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. Math.* **84** (1986), 1–48.
8. D. E. Rohrlich, L-functions and division towers, *Math. Ann.* **281** (1988), 611–632.
9. J.-P. Serre and J. Tate, Good reduction of abelian varieties, *Ann. of Math.* **88** (1968), 492–517.
10. J. H. Silverman, "The Arithmetic of Elliptic Curves," Graduate Texts in Math., Vol. 106, Springer-Verlag, Berlin/New York, 1986.
11. W. M. Sinnott, On p-adic L-functions and the Riemann–Hurwitz genus formula, *Compositio Math.* **53** (1984), 3–17.
12. G. Stevens, Stickelberger elements and modular parametrizations of elliptic curves, *Invent. Math.* **98** (1989), 75–106.
13. S.-L. Tang, Congruences between modular forms, cyclic isogenies of modular elliptic curves, and integrality of p-adic L-functions, *Trans. Amer. Math. Soc.* **349** (1997), 837–856.
14. L. C. Washington, "Introduction to Cyclotomic Fields," 2nd ed., Graduate Texts in Math., Vol. 83, Springer-Verlag, Berlin/New York, 1997.