

## CONSEQUENCES OF THE FUNCTIONAL EQUATION OF THE $p$ -ADIC $L$ -FUNCTION OF AN ELLIPTIC CURVE

FRANCESCA BIANCHI

**Abstract:** We prove that the first two coefficients in the series expansion around  $s = 1$  of the  $p$ -adic  $L$ -function of an elliptic curve over  $\mathbb{Q}$  are related by a formula involving the conductor of the curve. This is analogous to a recent result of Wuthrich for the classical  $L$ -function [6], which makes use of the functional equation. We present a few other consequences for the  $p$ -adic  $L$ -function and a generalisation to the base-change to an abelian number field.

**Keywords:** elliptic curves,  $p$ -adic  $L$ -functions.

### 1. Introduction

In [6], Wuthrich proves a relation between the leading and sub-leading coefficients of the Taylor series expansion at  $s = 1$  of the  $L$ -function of an elliptic curve over a number field, under the assumptions that the series admits an analytic continuation to  $s = 1$  and satisfies a functional equation. Wuthrich remarks that a similar result can potentially be obtained for any  $L$ -function which satisfies a functional equation.

In this paper, we consider the  $p$ -adic  $L$ -function of an elliptic curve over  $\mathbb{Q}$  and its twist by a quadratic character and explore the analogue of Wuthrich’s result. The prime  $p$  will be assumed to be odd and of semistable reduction for the curve. We start in Section 2 by reviewing the definition of the  $p$ -adic  $L$ -function and of its twists by Dirichlet characters  $\psi$ . Indeed, we define two  $p$ -adic  $L$ -functions, namely  $L_p(E, \alpha, \psi, s)$ , which is a function of  $s \in \mathbb{Z}_p$ , and  $\mathcal{L}_p(E, \alpha, \psi, T)$ , a power series in  $T$ . We state in Proposition 2.1 and Corollary 2.2 the functional equation for  $L_p(E, \alpha, \psi, s)$  and the corresponding result for  $\mathcal{L}_p(E, \alpha, \psi, T)$ . Proofs of the interpolation property and of the functional equation satisfied, more generally, by the twists of the  $p$ -adic  $L$ -function of a weight  $k$  cuspidal eigenform of Nebentypus  $\epsilon$  are provided in [3, Chapter 1, §§13, 17].

Subsequently, in Section 3, we prove the analogue of [6, Theorem 1] for  $L_p(E, \alpha, \psi, s)$  when  $\psi$  is a real character (i.e. when  $\psi$  is either the trivial char-

acter or a quadratic character). In particular, we prove in Theorem 3.3 that the sub-leading coefficient in the Taylor expansion of  $L_p(E, \alpha, \psi, s)$  at  $s = 1$  is equal to the leading coefficient multiplied by a constant dependent exclusively on the conductor of  $E$ , on the conductor of  $\psi$  and on the prime  $p$ . The assumption that  $\psi$  is a real character is necessary, since the functional equation relates the values of  $L_p(E, \alpha, \psi, s)$  to those of  $L_p(E, \alpha, \bar{\psi}, 2 - s)$ .

Although the latter result is perhaps of some interest on its own, when studying  $p$ -adic  $L$ -functions one is often concerned about the corresponding power series  $\mathcal{L}_p(E, \alpha, \psi, T)$ , because of its central importance in Iwasawa theory of elliptic curves. In Theorem 4.1 we thus translate the results of Section 3 into a relation between the first two leading coefficients of  $\mathcal{L}_p(E, \alpha, \psi, T)$ . In Section 4, we also prove another consequence of the relation between  $\mathcal{L}_p(E, \alpha, \psi, T)$  and  $\mathcal{L}_p(E, \alpha, \bar{\psi}, (1 + T)^{-1} - 1)$ , namely that the  $\mu$ -invariant of  $\mathcal{L}_p(E, \alpha, \psi, T)$  is the same as that of  $\mathcal{L}_p(E, \alpha, \bar{\psi}, T)$ . This is Theorem 4.2.

We end the article with a generalisation of some of the results to the  $p$ -adic  $L$ -function of the base-change of an elliptic curve to an abelian number field.

**Acknowledgements.** The author is very grateful to her adviser Jennifer Balakrishnan for suggesting the question, for giving careful feedback on some previous drafts and for constant guidance. She would also like to thank Chris Wuthrich for reading an earlier version of this article and providing extremely useful comments. Finally, she thanks Thanasis Bouganis for the very helpful conversations and the anonymous referee for the suggestions. The author is supported by EPSRC and by Balliol College through a Balliol Dervorguilla scholarship.

## 2. Notation and statement of the functional equation

In this section, we recall the definition of the  $p$ -adic  $L$ -function and the statement of the functional equation it satisfies. We follow the notation of [4] for the modular symbols and measures as well as the construction of the  $p$ -adic  $L$ -function, although we also allow non-trivial twists. We fix once and for all embeddings of  $\bar{\mathbb{Q}}$  into  $\mathbb{C}$  and  $\bar{\mathbb{Q}}_p$ .

Let  $E/\mathbb{Q}$  be an elliptic curve of conductor  $N$  and assume that  $p$  is an odd prime at which  $E$  has semistable reduction. Let  $f(z)$  be the newform of weight 2 corresponding to  $E$  by modularity and denote its  $q$ -expansion  $\sum_{n=1}^{\infty} a_n q^n$ .

We now define a quantity  $\alpha$ , dependent on the reduction type of  $E$  at  $p$ . In particular, if  $E$  has good ordinary reduction, we let  $\alpha$  be the unique  $p$ -adic unit in  $\mathbb{Z}_p$  which is a root of the characteristic polynomial of Frobenius  $P(X) = X^2 - a_p X + p$ . When  $E$  has good supersingular reduction, we denote by  $\alpha$  an arbitrarily fixed root of  $P(X)$ . Finally, if  $E$  has multiplicative reduction, we set  $\alpha = a_p$ , so that, in particular,  $\alpha = 1$  (resp.  $\alpha = -1$ ) if the reduction type is split (resp. non-split). We call  $\alpha$  an *allowable  $p$ -root (for  $E$ )* and we emphasize that  $\alpha$  is uniquely determined, unless  $E$  has good supersingular reduction at  $p$ .

For  $r \in \mathbb{Q}$ , we let

$$\lambda^\pm(r) = \mp \pi i \left( \int_r^{i\infty} f(z) dz \pm \int_{-r}^{i\infty} f(z) dz \right).$$

Normalising  $\lambda^+(r)$  (resp.  $\lambda^-(r)$ ) by the real period  $\Omega_E^+$  (resp. imaginary period  $\Omega_E^-$ ) of  $E$  gives the rational numbers  $[r]^\pm = \frac{\lambda^\pm(r)}{\Omega_E^\pm}$ .

Any unit  $x$  in  $\mathbb{Z}_p$  has a unique decomposition as a product of the form  $\omega(x) \langle x \rangle$  where  $\omega(x)$  is a  $(p - 1)^{\text{st}}$  root of unity and  $\langle x \rangle \in 1 + p\mathbb{Z}_p$  (note the running assumption that  $p$  is odd).

As in [3, I §§11, 13], for a positive integer  $M$ , we let  $\mathbb{Z}_{p,M}^* = \varprojlim_n (\mathbb{Z}/p^n M\mathbb{Z})^*$  and define a  $p$ -adic character as a continuous homomorphism  $\mathbb{Z}_{p,M}^* \rightarrow \mathbb{C}_p^*$ . In particular, since we have fixed an embedding of  $\bar{\mathbb{Q}}$  into  $\bar{\mathbb{Q}}_p$ , we may regard the notion of a finite order  $p$ -adic character and a Dirichlet character as equivalent and hence, even in the  $p$ -adic setting, we may use the notation  $\bar{\psi}$  for the inverse of the finite order character  $\psi$  and say  $\psi$  is *real-valued* if it is real-valued as a Dirichlet character, i.e.  $\psi = \bar{\psi}$ .

We then define the measures

$$\mu_\alpha^\pm(a + p^k M\mathbb{Z}_p) = \frac{1}{\alpha^k} \left[ \frac{a}{Mp^k} \right]^\pm - \frac{(1 - \delta)}{\alpha^{k+1}} \left[ \frac{a}{Mp^{k-1}} \right]^\pm,$$

where  $\delta = 0$  if  $E$  has good reduction and 1 otherwise.

Let  $\psi$  be a finite order  $p$ -adic character (possibly the identity) of conductor  $p^k M$ , with  $(M, p) = 1$ , and write

$$\langle x \rangle^{s-1} = \exp((s - 1) \log \langle x \rangle) = \sum_{n=0}^\infty \frac{(s - 1)^n}{n!} (\log \langle x \rangle)^n,$$

where  $\exp$  and  $\log$  are the  $p$ -adic exponential and logarithm maps. Then we define

$$L_p(E, \alpha, \psi, s) = \int_{\mathbb{Z}_{p,M}^*} \psi(x) \langle x \rangle^{s-1} d\mu_\alpha(x),$$

where  $\mu_\alpha = \mu_\alpha^+$  if the sign of  $\psi$  is  $+1$  and  $\mu_\alpha = \mu_\alpha^-$  otherwise. The  $p$ -adic  $L$ -function  $L_p(E, \alpha, \psi, s)$  is a locally analytic function of  $s \in \mathbb{Z}_p$  (see the first proposition in [3, I §13]).

We now perform a change of variable in the definition of  $L_p(E, \alpha, \psi, s)$ . Consider the extension  $\mathbb{Q}(\mu_{p^\infty})$  of  $\mathbb{Q}$ , obtained by adjoining to  $\mathbb{Q}$  all roots of unity of  $p$ -power order. Furthermore, let  $\Gamma$  denote the Galois group of the cyclotomic  $\mathbb{Z}_p$ -extension  $\mathbb{Q}^\infty$  of  $\mathbb{Q}$  and let  $\mathbb{Q}^n$  be the  $n^{\text{th}}$  layer in the cyclotomic tower.

Then there is a canonical homomorphism

$$\kappa : \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \rightarrow \mathbb{Z}_p^*$$

defined by the relation  $\sigma(\zeta) = \zeta^{\kappa(\sigma)}$  for all  $\sigma \in \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$  and  $\zeta \in \mu_{p^\infty}$ . The homomorphism  $\kappa$  is called the *cyclotomic character* and it induces an isomorphism

$\Gamma \rightarrow 1 + p\mathbb{Z}_p$ . Indeed, the group  $\Gamma$  is naturally identified with the quotient of  $\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$  by the subgroup which is mapped, under  $\kappa$ , to  $(\mathbb{Z}/p\mathbb{Z})^* \times \{0\} < (\mathbb{Z}/p\mathbb{Z})^* \times (1 + p\mathbb{Z}_p) \cong \mathbb{Z}_p^*$ . We may choose a topological generator  $\gamma \in \Gamma$  and define  $T = \kappa(\gamma)^{s-1} - 1$ . The result is a power series in  $T$ , with coefficients in  $\mathbb{Q}_p[\psi](\alpha)$ ,

$$\mathcal{L}_p(E, \alpha, \psi, T) = \int_{\mathbb{Z}_{p,M}^*} \psi(x)(1 + T)^{\frac{\log(x)}{\log \kappa(\gamma)}} d\mu_\alpha(x).$$

When the character  $\psi$  is trivial, we write simply  $L_p(E, \alpha, s)$  and  $\mathcal{L}_p(E, \alpha, T)$ .

Denote by  $Q$  the largest divisor of  $N$  coprime to  $pM$ . Then there exists  $c_Q = \pm 1$  such that  $w_Q(f) = c_Q f$ , where

$$w_Q(f) = f \Big|_{\begin{pmatrix} Qa & b \\ Nc & Qd \end{pmatrix}}(z)$$

for some integers  $a, b, c, d$  satisfying  $Qad - (N/Q)bc = 1$ . Note that, when  $Q = N$ , we have  $w_E = -c_Q$  where  $w_E$  is the sign in the functional equation of the complex  $L$ -function  $L(E, s)$ .

**Proposition 2.1 (Functional equation).** *Let  $E$  be an elliptic curve of conductor  $N$  with semistable reduction at the odd prime  $p$  and let  $\psi$  be a Dirichlet character of conductor  $p^k M$ , for some non-negative integers  $k$  and  $M$ , with  $(M, p) = 1$ . For each allowable  $p$ -root  $\alpha$ , the  $p$ -adic  $L$ -function  $L_p(E, \alpha, \psi, s)$  satisfies the functional equation*

$$L_p(E, \alpha, \psi, 2 - s) = -c_Q \cdot \bar{\psi}(-Q) \langle Q \rangle^{s-1} L_p(E, \alpha, \bar{\psi}, s),$$

where  $Q$  is the largest divisor of  $N$  coprime to  $pM$ .

**Proof.** See [3, I §17, Corollary 2]. ■

**Corollary 2.2.** *With the assumptions as in Proposition 2.1, we have*

$$\mathcal{L}_p(E, \alpha, \psi, T) = -c_Q \cdot \bar{\psi}(-Q) \langle Q \rangle^{\frac{\log(1+T)^{-1}}{\log \kappa(\gamma)}} \mathcal{L}_p(E, \alpha, \bar{\psi}, (1 + T)^{-1} - 1).$$

### 3. Relation between the leading and sub-leading coefficients of the $p$ -adic $L$ -function of an elliptic curve

We adopt the same notation as in Section 2.

**Lemma 3.1.** *Let  $\psi$  be a real-valued Dirichlet character. Then*

$$-c_Q \cdot \psi(-Q) = (-1)^{\text{ord}_{s=1} L_p(E, \alpha, \psi, s)}.$$

**Proof.** This is a standard exercise given the functional equation. Indeed, since  $\psi$  is assumed to be real-valued, Proposition 2.1 becomes

$$\Lambda_p(E, \alpha, \psi, 2 - s) = -c_Q \cdot \psi(-Q) \Lambda_p(E, \alpha, \psi, s), \tag{1}$$

where we put  $\Lambda_p(E, \alpha, \psi, s) = f(s) \cdot L_p(E, \alpha, \psi, s)$  with  $f(s) = \langle Q \rangle^{s/2}$ . Let  $m = \text{ord}_{s=1} L_p(E, \alpha, \psi, s)$ , so that  $\frac{d^i}{ds^i} L_p(E, \alpha, \psi, s)|_{s=1} = 0$  for all  $i < m$  and  $\frac{d^m}{ds^m} L_p(E, \alpha, \psi, s)|_{s=1} \neq 0$ . Then differentiating both sides of (1) and evaluating at  $s = 1$  yields

$$((-1)^m + c_Q \cdot \psi(-Q)) \frac{d^m}{ds^m} \Lambda_p(E, \alpha, \psi, s)|_{s=1} = 0.$$

By the definition of  $m$ , one has

$$\frac{d^m}{ds^m} \Lambda_p(E, \alpha, \psi, s)|_{s=1} = f(1) \frac{d^m}{ds^m} L_p(E, \alpha, \psi, s)|_{s=1} \neq 0, \tag{2}$$

which forces  $-c_Q \cdot \psi(-Q) = (-1)^m$ . ■

**Remark 3.2.** Assume that the conductor of  $\psi$  is not divisible by any prime of additive reduction for  $E$ . A “refined” version of the  $p$ -adic Birch and Swinnerton-Dyer conjecture then predicts that

$$\text{ord}_{s=1} L(E, \alpha, \psi, s) = m(E, \psi) + \delta,$$

where  $\psi$  is now viewed as a one-dimensional representation of  $\text{Gal}(K/\mathbb{Q})$  for some number field  $K$ ,  $m(E, \psi)$  is the multiplicity of  $\psi$  in the decomposition of  $E(K) \otimes_{\mathbb{Z}} \mathbb{C}$  into irreducible representations of  $\text{Gal}(K/\mathbb{Q})$  and  $\delta$  vanishes except for when the  $p$ -adic multiplier of the pair  $(\alpha, \psi)$  is zero, in which case  $\delta = 1$ .

In particular, when  $\psi$  is trivial,  $m(E, \psi) = \text{rank} E(\mathbb{Q})$ .

We now state and prove the result analogous to Wuthrich [6, Theorem 1].

**Theorem 3.3.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  and  $p$  an odd prime of semistable reduction for  $E$ . Let  $\psi$  be either the trivial character or a quadratic character of conductor  $p^k M$ . Let  $\alpha$  be an allowable  $p$ -root and denote by  $m$  the order of vanishing at  $s = 1$  of  $L_p(E, \alpha, \psi, s)$ . Then*

$$L_p(E, \alpha, \psi, s) = a_m (s - 1)^m + a_{m+1} (s - 1)^{m+1} + \dots$$

with

$$a_{m+1} = -\frac{1}{2} \log \langle Q \rangle a_m.$$

**Proof.** By Lemma 3.1, we have

$$\Lambda_p(E, \alpha, \psi, 2 - s) = (-1)^m \Lambda_p(E, \alpha, \psi, s),$$

where, as in the proof of the lemma,  $\Lambda_p(E, \alpha, \psi, s) = f(s) \cdot L_p(E, \alpha, \psi, s)$  with  $f(s) = \langle Q \rangle^{s/2}$ . We can now follow Wuthrich’s proof nearly identically.

In particular, for  $i \equiv m + 1 \pmod{2}$ , one has

$$\frac{d^i}{ds^i} \Lambda_p(E, \alpha, \psi, s)|_{s=1} = 0. \tag{3}$$

Choosing  $i = m + 1$ , this gives

$$\begin{aligned} 0 &= \frac{d^{m+1}}{ds^{m+1}} (f(s)L_p(E, \alpha, \psi, s)) \Big|_{s=1} \\ &= \left( \sum_{k=0}^{m+1} \binom{m+1}{k} \frac{d^{m+1-k}}{ds^{m+1-k}} f(s) \cdot \frac{d^k}{ds^k} L_p(E, \alpha, \psi, s) \right) \Big|_{s=1} \\ &= \left( (m+1)f'(s) \cdot \frac{d^m}{ds^m} L_p(E, \alpha, \psi, s) + f(s) \cdot \frac{d^{m+1}}{ds^{m+1}} L_p(E, \alpha, \psi, s) \right) \Big|_{s=1} \\ &= (m+1)!(f'(1) \cdot a_m + f(1) \cdot a_{m+1}). \end{aligned}$$

Therefore,  $a_{m+1} = -\frac{f'(1)}{f(1)}a_m = -\frac{1}{2} \log \langle Q \rangle a_m$ . ■

Let  $E$  be as in Theorem 3.3. The twist of  $E$  by a quadratic character  $\psi$  of conductor coprime to  $p$  can be realised as an elliptic curve  $E'/\mathbb{Q}$  which has semistable reduction at  $p$ . Therefore, if the conductor of  $\psi$  is coprime to  $p$ , the statement of Theorem 3.3 for  $L_p(E, \alpha, \psi, s)$  is implicitly included in the statement of Theorem 3.3 for the  $p$ -adic  $L$ -function of  $E'$  with trivial twist.

On the other hand, the twist of  $E$  by a quadratic character of conductor divisible by  $p$  is an elliptic curve  $E'$  with additive reduction at  $p$ . In other words, the quadratic character case in Theorem 3.3 is not completely exhausted by the result for the trivial character.

Note that Wuthrich’s method can be generalised also to obtain the coefficient  $a_{m+k}$  for every positive odd  $k$  in terms of the coefficients  $a_{m+j}$ , where  $0 \leq j < m$ , just by considering (3) for  $i = m + k$ . Recursively, this gives a way of expressing  $a_{m+k}$  for odd  $k$  in terms of  $a_{m+\ell}$  for even  $\ell$  with  $\ell < k$ . In particular, we may consider Theorem 3.3 as a special case of the following result.

**Theorem 3.4.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  and  $p$  an odd prime of semistable reduction for  $E$ . Let  $\psi$  be either the trivial character or a quadratic character of conductor  $p^k M$ . Denote by  $m$  the order of vanishing at  $s = 1$  of  $L_p(E, \alpha, \psi, s)$ . Then*

$$L_p(E, \alpha, \psi, s) = a_m(s - 1)^m + a_{m+1}(s - 1)^{m+1} + \dots,$$

where, for odd  $k > 0$ , we have

$$a_{m+k} = - \sum_{i=0}^{k-1} \frac{1}{(k-i)!} \cdot \left( \frac{\log \langle Q \rangle}{2} \right)^{k-i} a_{m+i}.$$

Therefore, for odd  $k$ ,  $a_{m+k}$  can be expressed as a linear combination of  $a_{m+\ell}$  for even  $\ell$ ,  $0 \leq \ell < k$ .

**Proof.** Using (3) with  $i = m + k$  and the fact that  $\frac{d^k}{ds^k} L_p(E, \alpha, \psi, s) \Big|_{s=1} = 0$  for all  $k < m$  gives

$$\sum_{r=m}^{m+k} \frac{(m+k)!}{(m+k-r)!} f^{(m+k-r)}(1) a_r = 0.$$

It remains to notice that, for all  $j \geq 0$ ,  $f^{(j)}(s) = \left( \frac{\log \langle Q \rangle}{2} \right)^j \langle Q \rangle^{s/2}$ . ■

**Remark 3.5.** There are essentially two reasons why we did not simply state Theorem 3.3 as a corollary of Theorem 3.4. The first one is that we wanted to mimic the proof in [6] as much as possible. The second one is that, although Theorem 3.4 is more general than Theorem 3.3, the latter is perhaps the more interesting result. Indeed, the  $p$ -adic version of the Birch and Swinnerton-Dyer conjecture (see Conjecture (BSD( $p$ )) I. in [3, II §10]) gives an explicit expression for  $a_m$ , involving, among other factors, the order of the Tate-Shafarevich group. Thus, a similar observation to Wuthrich’s in [6] also holds here, i.e. what Theorem 3.3 really states is that, if BSD( $p$ ) holds, then not only the leading but also the sub-leading coefficient of  $L_p(E, \alpha, s)$  is known. Under some extra assumptions, a similar result follows for the quadratic character case (see Conjecture (BSD( $p, \psi$ )) I. in [3, II §11]).

**4. Results for  $\mathcal{L}_p(E, \alpha, \psi, T)$**

The starting point for this section is Corollary 2.2. The first result is then

**Theorem 4.1.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  and  $p$  an odd prime of semistable reduction for  $E$ . Let  $\psi$  be either the trivial character or a quadratic character of conductor  $p^k M$ . Let  $\alpha$  be an allowable  $p$ -root and denote by  $m$  the order of vanishing at  $T = 0$  of  $\mathcal{L}_p(E, \alpha, \psi, T)$ . Then*

$$\mathcal{L}_p(E, \alpha, \psi, T) = c_m T^m + c_{m+1} T^{m+1} + \dots$$

where

$$c_{m+1} = -\frac{c_m}{2} \left( \frac{\log \langle Q \rangle}{\log \kappa(\gamma)} + m \right).$$

**Proof.** By Corollary 2.2, we have

$$\mathcal{L}_p(E, \alpha, \psi, (1 + T)^{-1} - 1) = (-c_Q) \psi(-Q) (1 + T)^{\frac{\log \langle Q \rangle}{\log \kappa(\gamma)}} \mathcal{L}_p(E, \alpha, \psi, T). \tag{4}$$

Differentiating  $m$  times and evaluating at  $T = 0$  yields the equality  $-c_Q \psi(-Q) = (-1)^m$ , similarly to Lemma 3.1.

Then, differentiating  $m + 1$  times the right hand side resp. the left hand side of (4) and evaluating at  $T = 0$  gives

$$(-1)^m (m + 1)! \left( \frac{\log \langle Q \rangle}{\log \kappa(\gamma)} c_m + c_{m+1} \right)$$

resp.

$$(-1)^{m+1} (m + 1)! (c_{m+1} + m c_m). \quad \blacksquare$$

Assume now that  $E$  has ordinary semistable reduction at the odd prime  $p$ , that is, either good ordinary or multiplicative reduction. Since, in this case, there is a unique  $p$ -admissible root  $\alpha$  for  $E$ , we may drop  $\alpha$  from the notation and simply write  $\mathcal{L}_p(E, \psi, T)$  for the  $p$ -adic  $L$ -function of  $E$ , twisted by  $\psi$ . By [5],

$\mathcal{L}_p(E, \psi, T) \in \Lambda = \mathbb{Z}_p[\psi][[T]]$  and we define the  $\mu$ -invariant of  $\mathcal{L}_p(E, \alpha, \psi, T)$  as the  $p$ -adic valuation of the highest power of  $\pi$  dividing  $\mathcal{L}_p(E, \alpha, \psi, T)$ , where  $\pi$  is a uniformiser for  $\mathbb{Z}_p[\psi]$ .

The relation between  $\mathcal{L}_p(E, \alpha, \psi, T)$  and  $\mathcal{L}_p(E, \alpha, \bar{\psi}, T)$  allows us to derive a result concerning the relation between the  $\mu$ -invariant of  $\mathcal{L}_p(E, \alpha, \psi, T)$  and that of  $\mathcal{L}_p(E, \alpha, \bar{\psi}, T)$ .

**Theorem 4.2.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  and  $p$  an odd prime of ordinary semistable reduction for  $E$ . Let  $\psi$  be a character of conductor  $p^k M$ . The  $\mu$ -invariant of  $\mathcal{L}_p(E, \psi, T)$  equals the  $\mu$ -invariant of  $\mathcal{L}_p(E, \bar{\psi}, T)$ .*

**Proof.** By Corollary 2.2,

$$\mathcal{L}_p(E, \psi, T) = -c_Q \cdot \bar{\psi}(-Q) \langle Q \rangle^{\frac{\log(1+T)^{-1}}{\log \kappa(\gamma)}} \mathcal{L}_p(E, \bar{\psi}, (1+T)^{-1} - 1).$$

Now  $c_Q = \pm 1$ ,  $\bar{\psi}(-Q)$  is a root of unity and  $\langle Q \rangle^{\frac{\log(1+T)^{-1}}{\log \kappa(\gamma)}}$  is a unit power series. Therefore the  $\mu$ -invariant of  $\mathcal{L}_p(E, \psi, T)$  is the same as the  $\mu$ -invariant of  $\mathcal{L}_p(E, \bar{\psi}, (1+T)^{-1} - 1)$ .

It remains to show that the  $\mu$ -invariant of a power series in  $\Lambda$  is unchanged under the substitution  $T \mapsto (1+T)^{-1} - 1$ . For this purpose, let  $f(T) = \sum_{k=0}^{\infty} a_k T^k$  and  $g(T) = f((1+T)^{-1} - 1)$ . Then  $g(T) = \sum_{k=0}^{\infty} b_k T^k$ , where

$$b_0 = a_0 \quad \text{and} \quad b_k = (-1)^k \sum_{i=0}^{k-1} \binom{k-1}{i} a_{i+1} \text{ for } k \geq 1.$$

This comes from the fact that, for  $j \geq 1$ , we have the equality of formal power series  $((1+T)^{-1} - 1)^j = \sum_{k=j}^{\infty} \binom{k-1}{j-1} (-1)^k T^k$ .

Let now  $k$  be the minimum integer such that the  $\mu$ -invariant of  $f(T)$  equals the  $p$ -adic valuation of  $a_k$ , denoted  $\nu_p(a_k)$ . Then

$$\nu_p(b_0) = \nu_p(a_0) \geq \nu_p(a_k), \quad \nu_p(b_i) \geq \min_{1 \leq j \leq i} \nu_p(a_j) \geq \nu_p(a_k) \quad \forall i \geq 1$$

and

$$\nu_p(b_k) = \nu_p(a_k).$$

This completes the proof. ■

### 5. Generalisations to the base-change of an elliptic curve

Let  $E$  be an elliptic curve over  $\mathbb{Q}$  of conductor  $N$ . Let  $K$  be an abelian number field such that the additive primes for  $E/\mathbb{Q}$  remain additive in the base-change of  $E$  to  $K$ . Denote by  $p$  an odd prime of semistable reduction for  $E$  and assume further that the field  $K$  is disjoint from the cyclotomic  $\mathbb{Z}_p$ -extension of  $\mathbb{Q}$ . Fix a choice of an allowable  $p$ -root  $\alpha$  for  $E/\mathbb{Q}$  as in Section 2. We can then define the  $p$ -adic  $L$ -function for the base-changed curve  $E/K$  as (cf. [2] and [1])

$$\mathcal{L}_p(E/K, \alpha, T) = \prod_{\psi \in \widehat{\text{Gal}(K/\mathbb{Q})}} \mathcal{L}_p(E, \alpha, \psi, T), \tag{5}$$



where  $\widehat{\text{Gal}}(K/\mathbb{Q})$  is the group of characters on  $\text{Gal}(K/\mathbb{Q})$  and  $\mathcal{L}_p(E, \alpha, \psi, T)$  is the  $p$ -adic  $L$ -function of  $E/\mathbb{Q}$  twisted by  $\psi$ , as defined in Section 2. From the interpolation property for each  $\mathcal{L}_p(E, \alpha, \psi, T)$  and the assumption on the behaviour of the additive places in  $K/\mathbb{Q}$ , it is easy to see that  $\mathcal{L}_p(E/K, \alpha, T)$  interpolates the values at  $s = 1$  of the complex  $L$ -function  $L(E/K, s)$ , twisted by characters of the  $\mathbb{Z}_p$ -cyclotomic extension of  $K$ .

Furthermore, using Corollary 2.2 on each factor of the right hand side of (5), we find the following transformation property for  $\mathcal{L}_p(E/K, \alpha, T)$

$$\begin{aligned} \mathcal{L}_p(E/K, \alpha, T) &= \left[ \prod_{\psi} (-c_{Q_{\psi}}) \cdot \prod_{\psi} \bar{\psi}(-Q_{\psi}) \right] \\ &\times \left[ \prod_{\psi} \langle Q_{\psi} \rangle^{\frac{\log(1+T)^{-1}}{\log \kappa(\gamma)}} \right] \cdot \mathcal{L}_p(E/K, \alpha, (1+T)^{-1} - 1), \end{aligned} \tag{6}$$

where the products run over all characters  $\psi$  of  $\widehat{\text{Gal}}(K/\mathbb{Q})$  and  $Q_{\psi}$  is the largest divisor of  $N$  coprime with  $p$  and with the conductor of  $\psi$ .

Recall from Section 2 that the variables  $T$  and  $s$  are related by the identity  $T = \kappa(\gamma)^{s-1} - 1$ . The analogue of Proposition 2.1 for  $E/K$  is then

$$L_p(E/K, \alpha, 2-s) = \left[ \prod_{\psi} (-c_{Q_{\psi}}) \cdot \prod_{\psi} \bar{\psi}(-Q_{\psi}) \right] \cdot \left[ \prod_{\psi} \langle Q_{\psi} \rangle^{s-1} \right] L_p(E/K, \alpha, s). \tag{7}$$

Equations (7) and (6) allow us to deduce analogues of Theorem 3.3 and Theorem 4.1 for  $E/K$ . The proofs are essentially identical, so we include only the statements of the results.

**Theorem 5.1.** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  of conductor  $N$  and  $p$  an odd prime of semistable reduction for  $E$ . Denote by  $E/K$  the base-change of  $E$  to an abelian number field  $K$ , where  $K$  is assumed to be disjoint from the  $\mathbb{Z}_p$ -extension of  $\mathbb{Q}$  and such that additive reduction is preserved everywhere in the extension  $K/\mathbb{Q}$ . For each allowable  $p$ -root  $\alpha$ , let  $m$  be the order of vanishing of  $L_p(E/K, \alpha, s)$  at  $s = 1$ . Then*

$$L_p(E/K, \alpha, s) = a_m(s-1)^m + a_{m+1}(s-1)^{m+1} + \dots$$

with

$$a_{m+1} = -\frac{\sum_{\psi} \log \langle Q_{\psi} \rangle}{2} a_m,$$

where  $\psi$  runs through the characters of  $\text{Gal}(K/\mathbb{Q})$  and  $Q_{\psi}$  is the largest divisor of  $N$  which is coprime with  $p$  and with the conductor of  $\psi$ .

**Theorem 5.2.** *With the assumptions of Theorem 5.1, we have*

$$\mathcal{L}_p(E/K, \alpha, T) = c_m T^m + c_{m+1} T^{m+1} + \dots$$

with

$$c_{m+1} = -\frac{c_m}{2} \left( \frac{\sum_{\psi} \log \langle Q_{\psi} \rangle}{\log \kappa(\gamma)} + m \right).$$

## References

- [1] K. Matsuno, *An analogue of Kida's formula for the  $p$ -adic  $L$ -functions of modular elliptic curves*, J. Number Theory **84**(1) (2000), 80–92.
- [2] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.
- [3] B. Mazur, J. Tate, and J. Teitelbaum, *On  $p$ -adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84**(1) (1986), 1–48.
- [4] W. Stein and C. Wuthrich, *Algorithms for the arithmetic of elliptic curves using Iwasawa theory*, Math. Comp. **82**(283) (2013), 1757–1792.
- [5] C. Wuthrich, *On the integrality of modular symbols and Kato's Euler system for elliptic curves*, Doc. Math. **19** (2014), 381–402.
- [6] C. Wuthrich, *The sub-leading coefficient of the  $L$ -function of an elliptic curve*, in Publications mathématiques de Besançon. Algèbre et théorie des nombres, 2016, volume 2016 of Publ. Math. Besançon Algèbre Théorie Nr., pages 95–96, Presses Univ. Franche-Comté, Besançon, 2017.

**Address:** Francesca Bianchi: Mathematical Institute, University of Oxford, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, UK.

**E-mail:** francesca.bianchi@maths.ox.ac.uk

**Received:** 9 November 2016; **revised:** 21 November 2017