ON TRIVIAL $p$-ADIC ZEROES FOR ELLIPTIC CURVES OVER KUMMER EXTENSIONS

DANIEL DELBOURGO

(Received 30 October, 2014)

Abstract. We prove the exceptional zero conjecture is true for semistable elliptic curves $E/\mathbb{Q}$ over number fields of the form $F(e^{2\pi i/q^n}, \Delta_1^{1/q^n}, \ldots, \Delta_d^{1/q^n})$ where $F$ is a totally real field, and the split multiplicative prime $p \neq 2$ is inert in $F(e^{2\pi i/q^n}) \cap \mathbb{E}$.

In 1986 Mazur, Tate and Teitelbaum [9] attached a $p$-adic $L$-function to an elliptic curve $E/\mathbb{Q}$ with split multiplicative reduction at $p$. To their great surprise, the corresponding $p$-adic object $L_p(E,s)$ vanished at $s = 1$ irrespective of how the complex $L$-function $L(E,s)$ behaves there. They conjectured a formula for the derivative

$$L'_p(E,1) = \frac{\log_p(q_E)}{\text{ord}_p(q_E)} \times \frac{L(E,1)}{\text{period}}$$

where $E(\mathbb{Q}_p) \cong \mathbb{Q}_p^\times / \mathbb{Z}_E$, and this was subsequently proven for $p \geq 5$ by Greenberg and Stevens [6] seven years later.

In recent times there has been considerable progress made on generalising this formula, both for elliptic curves over totally real fields [10, 15], and for their adjoint $L$-functions [12]. In this note, we outline how the techniques in [3] can be used to establish some new cases of the exceptional zero formula over solvable extensions $K/\mathbb{Q}$ that are not totally real.

1. Constructing the $p$-adic $L$-function

Let $E$ be an elliptic curve defined over $\mathbb{Q}$, and $p \geq 3$ a prime of split multiplicative reduction. First we fix a finite normal extension $K/\mathbb{Q}$ whose Galois group is a semi-direct product

$$\text{Gal}(K/\mathbb{Q}) = \Gamma \ltimes \mathcal{H}$$

where $\Gamma, \mathcal{H}$ are both abelian groups, with $\mathcal{H} = \text{Gal}(K/K \cap \mathbb{Q}^{ab})$ and likewise $\Gamma \cong \text{Gal}(K \cap \mathbb{Q}^{ab}/\mathbb{Q})$. Secondly we choose a totally real number field $F$ disjoint from $K$, and in addition suppose:

(H1) the elliptic curve $E$ is semistable over $F$;
(H2) the prime $p$ is unramified in $K$;
(H3) the prime $p$ is inert in the compositum $F \cdot k^+$ for all CM fields $k \subset K \cap \mathbb{Q}^{ab}$.

2010 Mathematics Subject Classification 11F33, 11F41, 11F67.

Key words and phrases: $p$-adic $L$-functions, elliptic curves, Mazur-Tate-Teitelbaum conjecture.
Now consider an irreducible representation of dimension $> 1$ of the form

$$
\rho^{(\psi)}_{\chi, k} := \text{Ind}_{F_k}^F(\chi) \otimes \psi
$$

where $k$ is a CM field inside of $K \cap \mathbb{Q}^{ab}$, the character $\chi : \text{Gal}(F \cdot K/F \cdot k) \to \mathbb{C}^\times$ induces a self-dual representation, and $\psi$ is cyclotomic of conductor coprime to $p$. It is well known how to attach a bounded $p$-adic measure to the twisted motive $H^1(E/F) \otimes \rho^{(\psi)}_{\chi, k}$, as we shall describe below.

By work of Shimura [14], there exists a parallel weight one Hilbert modular form $g^{(\psi)}_\chi$ with the same complex $L$-series as the representation $\text{Ind}_{F_k}^F(\chi) \otimes \text{Res}_{F_k}(\psi)$ over the field $F \cdot k^+$. The results of Hida and Panchiskin [7, 11] furnish us with measures interpolating

$$
\int_{x \in \mathbb{Z}_p^\times} \varphi(x) \cdot d\mu_{f_E \otimes g^{(\psi)}_\chi}(x) = \varepsilon_p(\rho^{(\psi)}_{\chi, k} \otimes \varphi) \times (\text{Euler factor at } p) \times \frac{L(f_E \otimes g^{(\psi)}_\chi, \varphi, 1)}{(f_E, f_E)_{F, k^+}}
$$

where the character $\varphi$ has finite order, $f_E$ denotes the base-change to the totally real field $F \cdot k^+$ of the newform $f_E$ associated to $E/\mathbb{Q}$, and $\langle - , - \rangle_{F, k^+}$ indicates the Petersson inner product.

We now explain how to attach a $p$-adic $L$-function to $E$ over the full compositum $F \cdot K$. Let us point out that by the representation theory of semi-direct products [13, Proposition 25], every irreducible $\text{Gal}(F \cdot K/F)$-representation $\rho$ must either be isomorphic to some $\rho^{(\psi)}_{\chi, k}$ above if $\dim(\rho) > 1$, otherwise $\rho = \psi$ for some finite order character $\psi$ with prime-to-$p$ conductor. For any normal extension $N/\mathbb{Q}$, at each character $\varphi : \text{Gal}(N(\mu_p^\infty)/N) \to \mathbb{C}^\times$ one defines

$$
\mathfrak{M}_p(N, \varphi) := \prod_{\rho} (\varepsilon\text{-factor of } \rho \otimes \varphi)^{m(\rho)}
$$

where the product ranges over all the irreducible representations $\rho$ of the group $\text{Gal}(N/\mathbb{Q})$, and $m(\rho)$ counts the total number of copies of $\rho$ inside the regular representation.

**Theorem 1.** There exists a bounded measure $d\mu^{(p)}_{f_E \otimes g^{(\psi)}_\chi}$ defined on the $p$-adic Lie group $\text{Gal}(F \cdot K(\mu_p^\infty)/F \cdot K) \cong \mathbb{Z}_p^\times$, interpolating the algebraic $L$-values

$$
\int_{x \in \mathbb{Z}_p^\times} \varphi(x) \cdot d\mu^{(p)}_{f_E \otimes g^{(\psi)}_\chi}(x) = \mathfrak{M}_p(F \cdot K, \varphi) \times \frac{L(E/F \cdot K, \varphi, 1)}{(\Omega_E^+ \Omega_E^-)^{(F \cdot K)_G/2}}
$$

at almost all finite order characters $\varphi \neq 1$, while $\int_{x \in \mathbb{Z}_p^\times} d\mu^{(p)}_{f_E}(x) = 0$ when $\varphi = 1$ is trivial (here the transcendental numbers $\Omega_E^\pm$ denote real and imaginary Néron periods for $E_{/\mathbb{Z}_p}$).

To prove this result, we simply take a convolution of the measures $d\mu_{f_E \otimes g^{(\psi)}_\chi}$ over the irreducible representations $\rho^{(\psi)}_{\chi, k}$ counted with multiplicity $[k : \mathbb{Q}]$, together with a convolution of $\psi$-twists of the $p$-adic Dabrowski [2] measure $d\mu_{f_E/F} \otimes \varphi$ for each (tame) character $\psi$ of $\text{Gal}(K \cap \mathbb{Q}^{ab}/\mathbb{Q})$. After scaling by an appropriate ratio of automorphic periods $\prod (f_E, f_E)$ to Néron periods $\Omega_E^\pm$, one duly obtains $d\mu^{(p)}_{f_E \otimes g^{(\psi)}_\chi}$ above.

At almost all finite twists by $\varphi$ the Euler factor at $p$ is trivial, so Theorem 1 now follows. For the full details we refer the reader to [3, Sections 5 and 6] where
a proof is given for the number field $K = \mathbb{Q}(\mu_q, m^{1/q})$ with $q \neq p$; the argument is identical in the general case.

**Definition 1.** For every $s \in \mathbb{Z}_p$, the $p$-adic $L$-function is given by the Mazur-Mellin transform

$$L_p(E/F \cdot K, s) := \int_{x \in \mathbb{Z}_p^\times} \exp ((s-1) \log_p x) \cdot d\mu_p^{(p)}.$$ 

Since $d\mu_p^{(p)}(\mathbb{Z}_p^\times) = 0$, it follows that $L_p(E/F \cdot K, s)$ must vanish at the critical point $s = 1$. The $p$-adic Birch and Swinnerton-Dyer Conjecture then predicts

$$\text{order}_{s=1} \left( L_p(E/F \cdot K, s) \right) \geq e_p(E/F \cdot K).$$

(1)

### 2. The Order of Vanishing at $s = 1$

Let $d \geq 1$ be an integer. We now restrict ourselves to studying the $d$-fold Kummer extension

$$K = \mathbb{Q}\left(\mu_q^n, \Delta_1^{1/q^n}, \ldots, \Delta_d^{1/q^n}\right) \quad \text{with} \quad p \nmid \Delta_1 \times \cdots \times \Delta_d,$$

where $q \neq p$ is an odd prime, and the $\Delta_i$’s are pairwise coprime $q$-power free positive integers. Here $K_{ab} := K \cap Q^{ab} = \mathbb{Q}(\mu_q^n)$, and in our previous notation

$$\Gamma \simeq (\mathbb{Z}/q^n\mathbb{Z})^\times \quad \text{and} \quad \mathcal{H} = \text{Gal}(K/Q(\mu_q^n)) \simeq (\mathbb{Z}/q^n\mathbb{Z})^\oplus d.$$

Note that the full Galois group is the semidirect product $\text{Gal}(K/Q) = \Gamma \rtimes \mathcal{H}$, where $\Gamma$ acts on $\mathcal{H}$ through the cyclotomic character.

Recall that $F$ was a totally real field disjoint from $K$ over which the curve $E$ is semistable. We now assume that $\rho$ is inert in $F \cdot K_{ab}^+$ and write $\mathfrak{p}^+$ to denote the prime ideal $p \cdot \mathcal{O}_{F,K_{ab}^+}$. In particular, conditions (H1)-(H3) hold. The strategy is to employ the factorisation

$$L_p(E/F \cdot K, s) = L_p(E/F \cdot K_{ab}^+, s) \times L_p(E \oplus \theta/F \cdot K_{ab}^+, s) \times \prod_{\text{dim}(\rho) > 1} L_p(E/F, \rho, s)^{m(\rho)}$$

(2)

where $\theta$ is the quadratic character of the field $K_{ab}$ over its totally real subfield $K_{ab}^+ = \mathbb{Q}(\mu_q^n)^+$, and the product ranges over the irreducible $\text{Gal}(F \cdot K/F)$-representations $\rho$ of dimension $\geq 2$ (we refer the reader to [13, Chapter 8] and [5, Section 2] for more details on the structure of these $(\mathbb{Z}/q^n\mathbb{Z})^\times \times (\mathbb{Z}/q^n\mathbb{Z})^\oplus d$-representations).

**Case I - The prime $p^+$ is inert in $F \cdot K_{ab}/F \cdot K_{ab}^+$**

Let $n_i := \text{ord}_p\left[\mathbb{Q}(\mu_q^n, \Delta_i^{1/q^n}) : \mathbb{Q}(\mu_q^n)\right]$ and $m(\rho) = \text{dim}(\rho)$, so that $\prod_{i=1}^d q^{n_i}$ is the number of places of $K$ above $p$. The Artin representations $\rho_{\chi,k}^{(i)}$ that produce an exceptional zero in
$h^1(E/F) \otimes p^{(\psi)}_{\chi,k}$ at $p$ are precisely those where $\psi = 1$ and the character $\chi$ factors through the quotient group

$$\mathcal{H}^1 = \frac{\mathcal{H}}{\bigoplus_{t=1}^{q^r m} \mathbb{Z}}.$$  

Moreover $m(\rho^{(1)}_{\chi,k}) = \dim(\rho^{(1)}_{\chi,k}) = \phi([\mathcal{H}^1 : \text{Ker}(\chi)])$, which equals the number of generators for the image of $\chi$; therefore

$$\sum_{\dim(\rho^{(1)}_{\chi,k}) > 1, \ h^1(E) \otimes p \text{ exc} \ 1} m(\rho^{(1)}_{\chi,k}) \geq \sum_{\dim(\rho^{(1)}_{\chi,k}) > 1, \ \chi : \mathcal{H}^1 \to \mathbb{C}^\times} \# \{ \chi : \mathcal{H}^1 \to \mu_{q^r} \} = \# \mathcal{H}^1 - 1.$$

We must also include the order of $L_p(E/F \cdot K_{ab}^+, s)$ at $s = 1$ which is at least one, hence

$$\text{order}_{s=1} \left( L_p(E/F \cdot K, s) \right) \geq 1 + (\# \mathcal{H}^1 - 1) = \prod_{t=1}^{d} q^{n_t}.$$

**Case II** - The prime $p^+$ splits in $F \cdot K_{ab}^+/F \cdot K_{ab}^+$:

There are $2 \times \prod_{t=1}^{d} q^{n_t}$ places of $K$ above $p$. The rest of the calculation is the same as Case I except that both of $L_p(E/F \cdot K_{ab}^+, s)$ and $L_p(E \otimes \theta/F \cdot K_{ab}^+, s)$ have trivial zeroes at $s = 1$, whilst $\text{order}_{s=1} \left( L_p(E/F, \rho, s) \right) \geq 2$ by [3, Thm 6.3]. Consequently we obtain the lower bound

$$\text{order}_{s=1} \left( L_p(E/F \cdot K, s) \right) \geq 1 + 1 + 2 \times (\# \mathcal{H}^1 - 1) = 2 \times \prod_{t=1}^{d} q^{n_t}.$$  

Combining both cases together, we have shown

**Theorem 2.** If $p$ is inert in $F(\mu_{q^r})^+$, then

$$\text{order}_{s=1} \left( L_p(E/F \cdot K, s) \right) \geq \mathfrak{e}_p(E/F \cdot K).$$

In other words, the inequality in Equation (1) holds true for these number fields.

**3. A Higher Derivative Formula**

Henceforth we shall assume that $p \geq 5$ is inert in $K_{ab}$, corresponding to Case I mentioned on the previous page; this condition is equivalent to ensuring that $p$ is a primitive root modulo $q^2$. Let us write $\mathcal{E}_p(X) \in \mathbb{Z}[X]$ for the characteristic polynomial of a geometric Frobenius element at $p$, acting on the regular representation of $\text{Gal}(F \cdot K/Q)$, such that the highest power of $X - 1$ has already been divided out of the polynomial (it is tautologically non-zero at $X = 1$).

**Theorem 3.** If $p \geq 5$ is inert in $F(\mu_{q^r})$, then

$$\left. \frac{1}{\mathfrak{e}_p} \frac{d^{n_p} L_p(E/F \cdot K, s)}{ds^{n_p}} \right|_{s=1} = \mathcal{L}_p(E) \times \mathcal{E}_p(1) \times \frac{\sqrt{\text{disc}(F \cdot K)} \cdot L(E/F \cdot K, 1)}{(\Omega_E^2 \cdot \Omega_E)(F \cdot K, \mathbb{Q})^{1/2}}.  \quad (3)$$

where $\mathcal{L}_p(E) := \prod_{(p, q_{E, \psi})} \log_{1}(q_{E, \psi})$ denotes Jones’ $L$-invariant [8], with the product taken over the primes of $F \cdot K$ lying above $p$. 

The proof follows identical lines to the $d = 1$ situation in [3, Section 6] – more precisely:

- the special values $L_p(E \otimes \theta / F \cdot K_{ab}, 1)$ and $L_p(E/F, \rho, 1)$ at the non-exceptional $\rho$'s can be computed directly from their interpolation properties;
- the derivative $L'_p(E/F \cdot K_{ab}, 1)$ is given by Mok’s formula [10, Thm 1.1] since $p \geq 5$;
- the derivatives $L'_p(E/F, \rho, 1)$ at those exceptional $\rho$'s are calculated using [3, Thm 6.2].

Lastly the terms can then be multiplied together as in Equation (2), and the result follows. Needless to say, the hard work is contained in [3, Thm 6.2] and requires us to extend the deformation theory approach of Greenberg and Stevens to $p$-twisted Hasse-Weil $L$-functions. The main ingredient is the construction of an “improved” $p$-adic $L$-function à la [6, Prop 5.8] (a conjectural $p$-adic interpolation rule for such an object can be found in [4, §§4.4]).

In fact Jones’ $\mathcal{L}$-invariant is non-vanishing by [1] as the elliptic curve $E$ is defined over $\mathbb{Q}$. Therefore if one considers Theorems 2 and 3 in tandem, one immediately obtains the

**Corollary 1.** **If the prime $p \geq 5$ is inert in $F(\mu_{q^n})$, then**

$$L(E/F \cdot K, 1) \neq 0 \text{ if and only if } \text{order}_{s=1} \left( L_p(E/F \cdot K, s) \right) = e_p(E/F \cdot K).$$

More generally, one can replace the requirement that “$E$ be an elliptic curve defined over $\mathbb{Q}$” with the statement that “$f$ is a primitive HMF over $F$ of parallel weight 2, that is Steinberg at the primes $p’|p$” and everything works fine, except that there is no longer a nice description for the $L$-invariant. Likewise one can accommodate weight two Hilbert modular forms with non-trivial nebentypus, providing the primes above $p$ do not divide its conductor.

Of particular interest in non-commutative Iwasawa theory is to extend Theorems 2 and 3 to the situation where $q = p$, i.e. for the $p$-ramified extensions $F(\mu_{p^n}, \Delta_{1/p^n}, \ldots, \Delta_{d/p^n})/\mathbb{Q}$. The obstacles appear to be technical rather than conceptual, and a higher derivative formula should certainly be possible in this context (work in progress of Antonio Lei and the author).

**References**


Daniel Delbourgo
Department of Mathematics,
University of Waikato,
Private Bag 3105, Hamilton,
New Zealand
delbourgo@waikato.ac.nz