ON THE p-ADIC L-FUNCTION OF A MODULAR FORM AT A SUPERSINGULAR PRIME

ROBERT POLLACK

Abstract

In this paper we study the two p-adic L-functions attached to a modular form $f = \sum a_n q^n$ at a supersingular prime p. When $a_p = 0$, we are able to decompose both the sum and the difference of the two unbounded distributions attached to f into a bounded measure and a distribution that accounts for all of the growth. Moreover, this distribution depends only upon the weight of f (and the fact that a_p vanishes). From this description we explain how the p-adic L-function is controlled by two Iwasawa functions and by two power series with growth which have a fixed infinite set of zeros (Theorem 5.1). Asymptotic formulas for the p-part of the analytic size of the Tate-Shafarevich group of an elliptic curve in the cyclotomic direction are computed using this result. These formulas compare favorably with results established by M. Kurihara in [11] and B. Perrin-Riou in [23] on the algebraic side. Moreover, we interpret Kurihara's conjectures on the Galois structure of the Tate-Shafarevich group in terms of these two Iwasawa functions.

Contents

DUKE MATHEMATICAL JOURNAL
Vol. 118, No. 3, © 2003
Received 5 December 2001. Revision received 17 July 2002.
2000 *Mathematics Subject Classification*. Primary 11R23; Secondary 11F67.

1. Introduction

In the early 1970s, B. Mazur and P. Swinnerton-Dyer constructed a p-adic L-function attached to a modular elliptic curve $E/\mathbf{Q}$ for each prime p of good, ordinary reduction (see [18]). This L-function can be represented as a power series in $\mathbf{Z}_p[[T]] \otimes \mathbf{Q}_p$ which p-adically interpolates the special values of the complex L-series of E twisted by various characters. Since this power series has bounded coefficients, by the p-adic Weierstrass preparation theorem, it has finitely many zeros. The number of zeros of the p-adic L-function and the slopes of these zeros are conjecturally related to certain arithmetic invariants of E via the main conjecture.

In [2] and [27] (see also [19]), the construction of p-adic L-functions was generalized to higher weight modular forms, to supersingular primes, and to primes of bad reduction. At an ordinary prime for the modular form, the p-adic L-function is an element of $\mathscr{O}_K[[T]] \otimes K$ with K some finite extension of $\mathbf{Q}_p$, and therefore the L-function has finitely many zeros. At a supersingular prime, however, the situation is quite different. The L-function can have unbounded coefficients and infinitely many zeros. For each supersingular prime p, there are two p-adic L-functions corresponding to the two nonunit roots of $x^2 - a_p x + p^{k-1}$, where a_p is the eigenvalue of the Hecke operator T_p acting on our modular form. When the slopes of the two roots are different, Mazur has shown that at least one of the two L-functions has infinitely many zeros (Theorem 3.3). In the equal slope case, it is known that if a_p vanishes, then one of the two L-functions has infinitely many zeros (Theorem 3.5).

The infinitude of the zeros of these L-functions makes their arithmetic nature more mysterious, especially in the context of a main conjecture. This paper attempts to shed some light on the case $a_p = 0$. (Note that this includes the case of a supersingular prime of an elliptic curve for $p > 3$.) We sketch here our methods and results in the elliptic curve case, though in the main body of the paper we work with modular forms of arbitrary weight having $a_p = 0$.

Let $E/\mathbf{Q}$ be an elliptic curve, and let p be a supersingular prime with $a_p = 0$. Let α and $\overline{\alpha}$ be the two roots of $x^2 + p$. We then have two p-adic L-functions $L_p(E, \alpha, T)$ and $L_p(E, \overline{\alpha}, T) \in \mathbf{Q}_p(\alpha)[[T]]$. Write

$$L_p(E, \alpha, T) = G^+(T) + G^-(T) \cdot \alpha \quad \text{with } G^\pm(T) \in \mathbf{Q}_p[[T]].$$

As observed by Perrin-Riou in [21], the interpolation property defining these L-functions forces $G^+(T)$ to vanish at $\zeta_{2n} - 1$ and $G^-(T)$ to vanish at $\zeta_{2n-1} - 1$ for all $n \geq 1$, where ζ_m is a p^mth root of unity (Theorem 3.5). (There is a change in parity for $p = 2$.) Hence the power series $G^+(T)$ and $G^-(T)$ have an infinite set of trivial zeros. Note that these zeros are even independent of E.

We then go on to construct p-adic power series $\log_p^+(T)$ and $\log_p^-(T)$ which vanish precisely at the forced zeros of $G^+(T)$ and $G^-(T)$, respectively (Corollary 4.2). These power series are constructed as an infinite product of cyclotomic polynomials and are named after the p-adic logarithm since their product is nearly $\log_p(1 + T)$. The next step is to examine the functions

$$L_p^+(E, T) := \frac{G^+(T)}{\log_p^+(T)} \qquad \text{and} \qquad L_p^-(E, T) := \frac{G^-(T)}{\log_p^-(T)}.$$

The relation of $\log_p^\pm(T)$ to $L_p(E, \alpha, T)$ can be compared to the relation of the gamma function to the Riemann zeta function. The gamma function forces the zeta function to vanish at all of the negative even integers, and the interesting zeros of the zeta function are discovered only after these zeros are removed from consideration. In our setting, we divide $G^\pm(T)$ by $\log_p^\pm(T)$ hoping to uncover its more interesting zeros. The properties of these half-logarithms are studied in Section 4.2.

By analyzing the rate of growth of $G^\pm(T)$ and $\log_p^\pm(T)$, one sees that $L_p^\pm(E, T)$ is bounded and actually has integral coefficients. Hence $L_p^\pm(E, T)$ has only finitely many zeros, and $G^\pm(T)$ vanishes at only finitely many places apart from its fixed set of forced roots. The integrality of $L_p^+(E, T)$ and $L_p^-(E, T)$ is the main result of the paper and is proven in Theorem 5.6.

We have

$$L_p(E, \alpha, T) = L_p^+(E, T) \cdot \log_p^+(T) + L_p^-(E, T) \cdot \log_p^-(T) \cdot \alpha \tag{1}$$

with $L_p^\pm(E, T) \in \mathbf{Z}_p[[T]]$. The functions $L_p^+(E, T)$ and $L_p^-(E, T)$ can be thought of as p-adic L-functions themselves; they are Iwasawa functions, satisfy a functional equation, and are completely determined by an interpolation property involving special values of L-series. Furthermore, from (1) we see that $L_p(E, \alpha, T)$ is completely determined by $L_p^+(E, T)$ and $L_p^-(E, T)$ up to the purely local functions $\log_p^+(T)$ and $\log_p^-(T)$.

In [22], Perrin-Riou constructed an algebraic p-adic L-function (defined up to a unit Iwasawa function) and formulated a main conjecture in the supersingular case. The algebraic p-adic L-function is again a power series with growth, and in the same manner as described above, one can extract from it two Iwasawa functions that encode all of the algebraic data up to the functions $\log_p^+(T)$ and $\log_p^-(T)$ (Theorem 5.17). These two Iwasawa functions should equal $L_p^{\pm}(E, T)$ up to a unit via the main conjecture. In this context, K. Kato's result on the divisibility of $L_p(E, \alpha, T)$ by the algebraic p-adic L-function translates immediately into a divisibility of $L_p^{\pm}(E, T)$ by these Iwasawa functions (Corollary 5.18).

Now let $\mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. The above results can be used to study the analytic and algebraic invariants of an elliptic curve E along this extension. This is done in Section 6. Let $\mathbf{Q}_n$ be the unique subextension of $\mathbf{Q}_\infty$ of degree p^n. Using Theorem 5.1, we compute asymptotic formulas for the analytic size of $\text{Ш}(E/\mathbf{Q}_n)_{p^\infty}$ (i.e., the size predicted by the Birch and Swinnerton-Dyer conjecture). This is done in Proposition 6.10. In the ordinary case, these formulas involve the Iwasawa invariants of the p-adic L-function. In the supersingular case, these formulas are based upon the Iwasawa invariants of $L_p^+(E, T)$ and $L_p^-(E, T)$. This result should be compared to [20] (a short and overlooked paper of A. Nasybullin from 1974), where similar formulas are stated.

The case where $\operatorname{ord}_p(L(E, 1)/\Omega_E) = 0$ has been studied deeply by Kurihara in [11]. By using Kato's Euler system for the Tate module of E, he produces exact formulas for the algebraic size of $\text{Ш}(E/\mathbf{Q}_n)_{p^\infty}$ along the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Under this hypothesis, the Iwasawa invariants of $L_p^+(E, T)$ and $L_p^-(E, T)$ are all zero, and the asymptotic analytic formulas derived in this paper compare favorably with those of Kurihara. Assuming the finiteness of $\text{Ш}(E/\mathbf{Q}_n)_{p^\infty}$, Perrin-Riou has proven asymptotic formulas for its size in terms of the Iwasawa invariants attached to the algebraic p-adic L-function. These formulas also compare well to the analytic ones derived in this paper assuming that the algebraic and analytic Iwasawa invariants agree (i.e., assuming the main conjecture in the supersingular case).

Since writing this paper, we have learned that S. Kobayashi in [10] has constructed two restricted Selmer groups sitting inside the full Selmer group of E over $\mathbf{Q}_\infty$ which are torsion over the Iwasawa algebra. He formulates a main conjecture (in the spirit of classical Iwasawa theory) that compares the characteristic power series of these modules to $L_p^+(E, T)$ and $L_p^-(E, T)$. Using Kato's Euler system, he proves a divisibility of $L_p^{\pm}(E, T)$ by the corresponding characteristic power series. This formulation of the main conjecture gives a concrete arithmetic interpretation of $L_p^{\pm}(E, T)$.

2. The p-adic L-function of a modular form

The p-adic L-function of a modular form is a function on continuous $\mathbf{C}_p$-valued characters of $\mathbf{Z}_p^\times \times (\mathbf{Z}/M)^\times$ (with M prime to p) defined by integration against a fixed distribution (i.e., a measure that is possibly unbounded). This distribution is constructed to encode the arithmetic properties of the modular form. In particular, by integrating against characters of finite order, the special values of the L-series of the modular form can be recovered.

In this section we first review the theory of integration against admissible measures (which are certain tempered p-adic distributions). Since these measures are unbounded, naive Riemann sums do not necessarily converge and a more technical approach is needed. We then construct admissible measures attached to a modular form out of modular symbols and define the p-adic L-function of a modular form by integration against this measure. Finally, we describe the p-adic L-function as a p-adic power series determined by an interpolation property and a bound on its growth (for more details, see [2], [19], [27]).

2.1. Integration against admissible measures

Let $\mathbf{Z}_{p,M}^\times = \mathbf{Z}_p^\times \times (\mathbf{Z}/M)^\times$ for some integer M prime to p, and let $x_p : \mathbf{Z}_{p,M}^\times \to \mathbf{Z}_p^\times$ be the natural projection. Denote by $C^h(\mathbf{Z}_{p,M}^\times)$ the space of $\mathbf{C}_p$-valued functions on $\mathbf{Z}_{p,M}^\times$ which are locally polynomials in x_p of degree less than or equal to h. Here h is any nonnegative real number.

Definition 2.1

An *h-admissible measure* μ on $\mathbf{Z}_{p,M}^\times$ is a linear map from $C^h(\mathbf{Z}_{p,M}^\times)$ to $\mathbf{C}_p$ such that

$$\sup_{a \in \mathbf{Z}_{p,M}^\times} \left| \mu\big((x_p - a_p)^i \cdot \chi_{a+p^n\mathbf{Z}_{p,M}}\big) \right|$$

is $\mathrm{O}(p^{n(h-i)})$ for $0 \le i \le h$. Here χ_U is the characteristic function of U.

Remark 2.2

Definition 2.1 differs from [27, Definition 1.3], where the stronger bound of $\mathrm{o}(p^{n(h-i)})$ is required.

Remark 2.3

If $h = 0$, then Definition 2.1 describes a (bounded) measure.

THEOREM 2.4

An h-admissible measure μ extends to a linear map on the space of all locally analytic functions on $\mathbf{Z}_{p,M}^\times$.

Proof

This is proven by approximating a locally analytic function by the first $[h]+1$ terms of its Taylor series expansion and forming a generalized Riemann sum out of the data of μ. For a detailed proof, see [27, Lemma 1.6]. □

For f locally analytic, denote $\mu(f)$ by $\int_{\mathbf{Z}_{p,M}^\times} f\,d\mu$. From Theorem 2.4, we can integrate characters of $\mathbf{Z}_{p,M}^\times$ against μ since they are locally analytic functions. Define a map

$$L(\mu,\cdot) : \mathrm{Hom}_{\mathrm{cont}}(\mathbf{Z}_{p,M}^\times, \mathbf{C}_p^\times) \to \mathbf{C}_p$$

by the formula

$$L(\mu,\chi) := \int_{\mathbf{Z}_{p,M}^\times} \chi\,d\mu.$$

The space $\mathrm{Hom}_{\mathrm{cont}}(\mathbf{Z}_{p,M}^\times, \mathbf{C}_p^\times)$ has a natural analytic structure under which the above map is analytic. We now describe this structure.

Set $q=p$ for odd primes p, and set $q=4$ for $p=2$. Fix a topological generator γ of $1+q\mathbf{Z}_p$. Call characters on $\mathbf{Z}_{p,M}^\times \cong (\mathbf{Z}/Mq)^\times \times (1+q\mathbf{Z}_p)$ *tame* if they factor through $(\mathbf{Z}/Mq)^\times$ and *wild* if they factor through $1+q\mathbf{Z}_p$. Each character of $\mathbf{Z}_{p,M}^\times$ can be uniquely written as the product of a tame character and a wild character. For $u \in \mathbf{C}_p$ with $|u-1|_p < 1$, define a particular wild character $\chi_u \in \mathrm{Hom}_{\mathrm{cont}}(\mathbf{Z}_{p,M}^\times, \mathbf{C}_p^\times)$ by

$$\chi_u : \mathbf{Z}_{p,M}^\times \twoheadrightarrow \mathbf{Z}_p^\times \twoheadrightarrow 1+q\mathbf{Z}_p \to \mathbf{C}_p^\times,$$

where the first and second maps are the natural projections and the third map simply sends our chosen generator γ onto u. Note that the set $\{\chi_u : |u-1|_p < 1\}$ accounts for all wild characters since $1+q\mathbf{Z}_p$ is topologically cyclic and the continuity of the characters requires that $|\chi(\gamma)-1|_p < 1$.

Let ψ be a tame character on $\mathbf{Z}_{p,M}^\times$. The mapping $u \mapsto \psi\chi_u$ identifies the open unit disc of $\mathbf{C}_p$ with the set of characters on $\mathbf{Z}_{p,M}^\times$ with tame part equal to ψ. Since there are only finitely many tame characters on $\mathbf{Z}_{p,M}^\times$, we have that $\mathrm{Hom}_{\mathrm{cont}}(\mathbf{Z}_{p,M}^\times, \mathbf{C}_p^\times)$ is the union of finitely many open unit discs of $\mathbf{C}_p$.

We now state the analytic properties of $L(\mu,\chi)$ with respect to χ.

Definition 2.5

For F and G locally analytic functions on the open unit disc of $\mathbf{C}_p$, we say that F is $\mathrm{O}(G)$ if

$$\sup_{|z|<r} |F(z)|_p \text{ is } \mathrm{O}\Big(\sup_{|z|<r} |G(z)|_p\Big) \text{ as } r \to 1^-.$$

THEOREM 2.6 (see Višik [27], Amice and Vélu [2])
For μ an h-admissible measure on $\mathbf{Z}_{p,M}^{\times}$ and ψ a fixed tame character of $\mathbf{Z}_{p,M}^{\times}$, the function $L(\mu, \psi\chi_u)$ is analytic in u and is $\mathrm{O}(\log_p(1+T)^h)$.

Proof
This is essentially proven in [27, Theorem 2.3]. There h is required to be integral, and the estimate of $\mathrm{o}(\log_p(1+T)^{[h]+1})$ is obtained. However, applying the arguments of [27] with this paper's notion of h-admissible yields the $\mathrm{O}(\log_p(1+T)^h)$ bound (see also [5, Proposition I.4.5]). □

2.2. Admissible measures attached to modular forms

Let f be a modular form of weight k, level N, and character ε which is an eigenform for each Hecke operator T_n with eigenvalue a_n. Let $K(f)$ be the number field generated by the a_n and the values of ε; denote by $\mathscr{O}(f)$ its ring of integers.

Define the periods of f by

$$\phi(f, P, r) := 2\pi i \int_{i\infty}^{r} f(z)P(z)\,dz$$

for $r \in \mathbf{Q}$ and $P \in \mathbf{Z}[T]$ of degree less than or equal to $k-2$. Let L_f be the $\mathbf{Z}$-module generated by $\phi(f, P, r)$ for all $r \in \mathbf{Q}$. Then L_f is finitely generated over $\mathbf{Z}$. In fact, $L_f \cdot K(f)$ has dimension at most 2 over $K(f)$ (see Theorem 2.7). Let

$$\eta(f, P; a, m) := \phi\Big(f, P(mz-a), \frac{a}{m}\Big),$$

and fix the positive and negative parts of η by

$$\eta^{+}(f, P; a, m) := \frac{\eta(f, P; a, m) + \eta(f, P; -a, m)}{2},$$
$$\eta^{-}(f, P; a, m) := \frac{\eta(f, P; a, m) - \eta(f, P; -a, m)}{2}.$$

The following theorem expresses the algebraic properties of $\eta^{\pm}$.

THEOREM 2.7
There exist two nonzero complex numbers Ω_f^{+} and Ω_f^{-} such that

$$\frac{\eta^{\pm}(f, P; a, m)}{\Omega_f^{\pm}} \in \mathscr{O}(f)$$

for all $a, m \in \mathbf{Z}$ and $P \in \mathbf{Z}[T]$ with degree less than or equal to $k-2$.

Proof
See [8, Theorem 3.5.4]. □

Define the modular symbols of f by

$$\lambda^{\pm}(f, P; a, m) := \frac{\eta^{\pm}(f, P; a, m)}{\Omega_f^{\pm}} \in \mathscr{O}(f).$$

We build admissible measures out of the data of these modular symbols. First we set some notation. Fix a prime number p and an embedding of $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$. Let $\operatorname{ord}_p(\cdot)$ be the associated valuation at p normalized so that $\operatorname{ord}_p(p) = 1$. Let v be the prime of $K(f)$ over p determined by $\operatorname{ord}_p(\cdot)$, and let $K := K(f)_v$. Call a root α of $x^2 - a_p x + \varepsilon(p)p^{k-1} = 0$ *allowable* if $\operatorname{ord}_p(\alpha) < k - 1$.

For a fixed allowable α, we define two admissible measures on $\mathbf{Z}_{p,M}^{\times}$ by the formulas

$$\mu_{f,\alpha}^{\pm}(P, a + p^n M\mathbf{Z}_{p,M}) = \frac{1}{\alpha^n}\lambda^{\pm}(f, P; a, p^n M) - \frac{\varepsilon(p)p^{k-2}}{\alpha^{n+1}}\lambda^{\pm}(f, P; a, p^{n-1}M),$$

where a is prime to Mp.

In the ordinary case, $\operatorname{ord}_p(a_p) = 0$ and there is a unique allowable α. This α is also a unit, and the above distribution is bounded. In the supersingular case, $\operatorname{ord}_p(a_p) > 0$ and there are two allowable choices for α. Note that $\mu_{f,\alpha}^{\pm}$ grows at a faster rate for larger values of $\operatorname{ord}_p(\alpha)$ since powers of α appear in denominators in the definition of $\mu_{f,\alpha}^{\pm}$.

PROPOSITION 2.8
If $h = \operatorname{ord}_p(\alpha) < k - 1$, then $\mu_{f,\alpha}^{\pm}$ is an h-admissible measure.

Proof
The additivity property of $\mu_{f,\alpha}^{\pm}$ follows from the fact that f is an eigenform for T_p (see [19, Section 10]). The bound on the growth of $\mu_{f,\alpha}^{\pm}$ follows from [27, Lemma 3.8]. □

2.3. The p-adic L-function

We can now define the p-adic L-function of a modular form (with respect to some allowable root α).

Definition 2.9
With f and α defined as in Section 2.2, the p-adic L-function of f and α is

$$L_p(f, \alpha, \chi) := L\left(\mu_{f,\alpha}^{\operatorname{sgn}(\chi)}, \chi\right).$$

From Theorem 2.6, we know that $L_p(f, \alpha, \chi)$ is analytic in χ, and hence we can form its power series expansion about a tame character ψ. If we denote this power series by $L_p(f,\alpha,\psi,T)$, then for $T = u-1$ we have

$$L_p(f,\alpha,\psi,u-1) = L_p(f,\alpha,\psi\chi_u) = \int_{\mathbf{Z}_{p,M}^\times} \psi\chi_u \, d\mu_{f,\alpha}^{\mathrm{sgn}(\psi)}.$$

Note that the expression of the L-function as a power series depends upon a choice of γ generating $1+q\mathbf{Z}_p$. However, the dependence is not serious, and γ is always suppressed from the notation. If ψ is the trivial character, then we write $L_p(f,\alpha,T)$ for $L_p(f,\alpha,\psi,T)$.

The power series $L_p(f,\alpha,\psi,T)$ converges on the open unit disc. Furthermore, if the tame part of χ is ψ, then $\int_{\mathbf{Z}_p^\times} \chi \, d\mu_{f,\alpha}^{\pm} \in K(\alpha,\psi)$. From this it follows that

$$L_p(f,\alpha,\psi,T) \in K(\alpha,\psi)[[T]].$$

Remark 2.10
The p-adic L-function of f also depends upon a choice of $\Omega_f^{\pm}$, which are defined only up to an element of $\mathscr{O}(f)$. In the case of elliptic curves, we specify a particular choice of periods and pin down the L-function up to sign.

We now make explicit the values of $L_p(f,\alpha,\cdot)$ at characters of the form $x_p^j \cdot \varphi$ for $0 \le j \le k-2$, where x_p is the natural projection from $\mathbf{Z}_{p,M}^\times$ to $\mathbf{Z}_p^\times$ and φ is a character of finite order. This is equivalent to computing the values

$$L_p(f,\alpha,\psi,\gamma^j \cdot \zeta_n - 1) \quad \text{for } 0 \le j \le k-2,$$

where ζ_n is a p^nth root of unity and ψ is a tame character. In this way, $L_p(f,\alpha,\psi,T)$ can be thought of as a solution to an interpolation problem. In the ordinary case this completely determines $L_p(f,\alpha,\psi,T)$. In the supersingular case this also completely determines the L-function with the added condition that it be $\mathrm{O}(\log_p(1+T)^h)$, where $h = \mathrm{ord}_p(\alpha)$. (Any two functions satisfying the interpolation property differ by a function that vanishes so often that it must grow at least as fast as $\log_p(1+T)^h$.)

Let $\chi = x_p^j \cdot \varphi$, where φ is some finite order character of conductor $m = p^\nu M$ with M prime to p, and let $\tau(\varphi)$ be a Gauss sum. Define the p-adic multiplier by

$$e_p(\alpha,\chi) = \frac{1}{\alpha^\nu}\Big(1 - \frac{\varphi^{-1}(p)\varepsilon(p)p^{k-2-j}}{\alpha}\Big)\Big(1 - \frac{\varphi(p)p^j}{\alpha}\Big).$$

PROPOSITION 2.11
For χ as above,

$$L_p(f,\alpha,\chi) = e_p(\alpha,\chi) \cdot \frac{m^{j+1}}{(-2\pi i)^j} \cdot \frac{j!}{\tau(\varphi^{-1})} \cdot \frac{L(f_{\varphi^{-1}}, j+1)}{\Omega_f^{\pm}},$$

where $L(f_\varphi, s)$ is the complex L-series attached to f twisted by φ. Furthermore, $L_p(f, \alpha, \chi)$ is uniquely characterized by this interpolation property and the fact that it is $\mathrm{O}(\log_p(1+T)^h)$.

Proof
See [19, Section 14]. □

Remark 2.12
Note that the above formula depends only upon α in the first factor. If $\nu > 0$, the above formula simplifies greatly since $e_p(\alpha, \chi) = 1/\alpha^\nu$.

3. Results on the infinitude of zeros of supersingular L-functions

Assume for the moment that we are in the ordinary case, so that $\mathrm{ord}_p(a_p) = 0$. Then there is a unique allowable root α to $x^2 - a_p x + \varepsilon(p)p^{k-1} = 0$ which is necessarily a unit. In fact, $\alpha \in \mathscr{O}_K^\times$, and hence $\mu^\pm_{f,\alpha}$ takes its values in $\mathscr{O}_K$. Therefore $L_p(f, \alpha, \psi, T)$ has integral coefficients, and by the p-adic Weierstrass preparation theorem, we can write

$$L_p(f, \alpha, \psi, T) = p^\mu \cdot P(T) \cdot U(T)$$

with $P(T)$ a distinguished polynomial and $U(T)$ a unit power series. In particular, this L-function has only finitely many zeros, all encoded in the polynomial $P(T)$. This is remarkably different from the supersingular case, where we see in many instances that the coefficients of $L_p(f, \alpha, \psi, T)$ are unbounded and that this power series has infinitely many zeros.

Assume now that $\mathrm{ord}_p(a_p) > 0$ and that $(p, N) = 1$. Then there are two allowable roots to $x^2 - a_p x + \varepsilon(p)p^{k-1} = 0$. Call these roots α_1 and α_2; for each we have an associated p-adic L-function. The relationship between these two L-functions allows us in many cases to prove that one (or both) have infinitely many zeros.

Let $h_1 = \mathrm{ord}_p(\alpha_1)$ and $h_2 = \mathrm{ord}_p(\alpha_2)$ be ordered so that $h_1 \leq h_2$. Then h_1 ranges from zero to $(k-1)/2$. When $h_1 = 0$, we are in the ordinary case, and when $h_1 = (k-1)/2$, then $h_2 = h_1$ and we are in the most supersingular case. The first result of this section discusses the case when $0 < h_1 \neq h_2$, and the second result discusses the case when $a_p = 0$, which is a special subcase of the most supersingular case.

Definition 3.1
For K a finite extension of $\mathbf{Q}_p$, set

$$\mathscr{A}(K) := \left\{ f \in K[[T]] \,\middle|\, f \text{ is convergent on the open unit disc of } \mathbf{C}_p \right\}.$$

The following lemma says that if such a p-adic power series has finitely many zeros, then its coefficients are bounded. We would like to thank Adrian Iovita for showing us the following argument.

LEMMA 3.2
Let K be a finite extension of $\mathbf{Q}_p$. Then $f(T) \in \mathscr{A}(K)$ has finitely many zeros if and only if $f(T) \in \mathscr{O}_K[[T]] \otimes K$.

Proof
By the Weierstrass preparation theorem, any element of $\mathscr{O}_K[[T]] \otimes K$ has only finitely many zeros. Conversely, take $f(T) \in \mathscr{A}(K)$ with only finitely many zeros. Then all of its zeros must be algebraic over K. Let $P(T)$ be a polynomial in $K[T]$ with the same roots (counting multiplicity) as $f(T)$. Then from [12, Lemma 1], there is some $g(T) \in \mathscr{A}(K)$ such that $f(T) = P(T) \cdot g(T)$. Since $g(z)$ is nonzero for all z in the open unit disc, $g(T)$ is a unit in $\mathscr{A}(K)$ (see [12, Proposition 4.1]). Finally, by [12, (4.8)], the units of $\mathscr{A}(K)$ are $K^\times \cdot (1 + T\mathscr{O}_K[[T]])$, which completes the proof. □

THEOREM 3.3 (Mazur)
Suppose that $h_1 > 0$ and $h_1 \neq h_2$. Then for a fixed tame character ψ on $\mathbf{Z}_{p,M}^\times$, at least one of $L_p(f, \alpha_1, \psi, \cdot)$ and $L_p(f, \alpha_2, \psi, \cdot)$ has infinitely many zeros in the open unit disc.

Proof
From Remark 2.12, we have

$$L_p(f, \alpha_1, \psi, \zeta_n - 1) = \frac{c_n}{{\alpha_1}^{n+1}},$$
$$L_p(f, \alpha_2, \psi, \zeta_n - 1) = \frac{c_n}{{\alpha_2}^{n+1}}$$

for some constant c_n independent of α_i. (Here we are implicitly assuming that $p \neq 2$. For $p = 2$, the exponent on the α_i would be $n + 2$, making little difference in the argument below.)

Suppose that both $L_p(f, \alpha_1, \psi, T)$ and $L_p(f, \alpha_2, \psi, T)$ have finitely many zeros. Then Lemma 3.2 says that they both have bounded coefficients. By the Weierstrass preparation theorem, we can write

$$L_p(f, \alpha_1, \psi, T) = p^{r_1} P_1(T) U_1(T)$$

and

$$L_p(f, \alpha_2, \psi, T) = p^{r_2} P_2(T) U_2(T),$$

where the P_i are distinguished polynomials of degree d_i and the U_i are unit power series. Then for large n, $L_p(f, \alpha_i, \psi, \zeta_n - 1)$ has valuation $r_i + d_i \cdot \operatorname{ord}_p(\zeta_n - 1)$. We also know that

$$\alpha_1^{n+1} \cdot L_p(f, \alpha_1, \psi, \zeta_n - 1) = \alpha_2^{n+1} \cdot L_p(f, \alpha_2, \psi, \zeta_n - 1).$$

Taking valuations yields

$$h_1 \cdot (n+1) + r_1 + d_1 \cdot \operatorname{ord}_p(\zeta_n - 1) = h_2 \cdot (n+1) + r_2 + d_2 \cdot \operatorname{ord}_p(\zeta_n - 1)$$

for large n. Since $\operatorname{ord}_p(\zeta_n - 1)$ tends to zero for large n and $h_1 \neq h_2$, we have a contradiction. Hence one of the two power series has infinitely many zeros. □

Remark 3.4
Note that this proof does not indicate which of the two L-functions vanishes infinitely often. It is conjectured that both of these L-functions have infinitely many zeros.

We now consider f with $a_p = 0$, which puts us in a special case of the most supersingular case. Again we prove that one of the two L-functions has infinitely many zeros, and in some cases we see that both have infinitely many.

THEOREM 3.5 (Perrin-Riou)
Suppose that $a_p = 0$ (and hence that $h_1 = h_2$). Then for a tame character ψ on $\mathbf{Z}_{p,M}^{\times}$, one of $L_p(f, \alpha_1, \psi, \cdot)$ and $L_p(f, \alpha_2, \psi, \cdot)$ has infinitely many zeros in the open unit disc. If $\alpha_1 \notin K(\psi)$, then both L-functions have infinitely many zeros.

Proof
Let

$$G_\psi^+(T) = \frac{L_p(f, \alpha_1, \psi, T) + L_p(f, \alpha_2, \psi, T)}{2} \in K(\psi)[[T]]$$

and

$$G_\psi^-(T) = \frac{L_p(f, \alpha_1, \psi, T) - L_p(f, \alpha_2, \psi, T)}{2\alpha_1} \in K(\psi)[[T]].$$

Then

$$L_p(f, \alpha_1, \psi, T) = G_\psi^+(T) + G_\psi^-(T) \cdot \alpha_1.$$

As before, we have

$$L_p(f, \alpha_1, \psi, \zeta_n - 1) = \frac{c_n}{{\alpha_1}^{n+1}} \qquad \text{and} \qquad L_p(f, \alpha_2, \psi, \zeta_n - 1) = \frac{c_n}{{\alpha_2}^{n+1}}$$

for some constant c_n independent of the α_i. (If $p = 2$, the exponents on the α_i should be $n+2$.) Since $a_p = 0$, we have $\alpha_1 = -\alpha_2$. Hence

$$L_p(f, \alpha_1, \psi, \zeta_n - 1) = L_p(f, \alpha_2, \psi, \zeta_n - 1)$$

for n odd and

$$L_p(f, \alpha_1, \psi, \zeta_n - 1) = -L_p(f, \alpha_2, \psi, \zeta_n - 1)$$

for n even. This forces $G_\psi^+(\zeta_{2n} - 1) = 0$ and $G_\psi^-(\zeta_{2n-1} - 1) = 0$ for all $n > 0$. (If $p = 2$, then the parities are reversed.)

Assume now that both $L_p(f, \alpha_1, \psi, T)$ and $L_p(f, \alpha_2, \psi, T)$ have finitely many zeros. Then Lemma 3.2 guarantees that both have bounded coefficients. Hence both G_ψ^+ and G_ψ^- also have bounded coefficients. But G_ψ^+ and G_ψ^- have infinitely many zeros, which is a contradiction.

Therefore one of $L_p(f, \alpha_1, \psi, T)$ and $L_p(f, \alpha_2, \psi, T)$ has infinitely many zeros. If $\alpha_1 \notin K(\psi)$, the two power series are conjugate and hence both have infinitely many zeros. □

COROLLARY 3.6

Suppose that p is a supersingular prime for an elliptic curve E over $\mathbf{Q}$. Then at least one of $L_p(E, \alpha_1, \psi, T)$ and $L_p(E, \alpha_2, \psi, T)$ has infinitely many zeros in the open unit disc. If $\alpha_1 \notin \mathbf{Q}_p(\psi)$, then both functions have infinitely many zeros.

Proof

For $p > 3$, we have $a_p = 0$ since $p \mid a_p$ and $a_p < 2\sqrt{p}$. Therefore Theorem 3.5 applies. In the case $p = 2$ or 3 and $a_p \neq 0$, then $a_p = \pm 2$ or ± 3. In these four cases, α_1/α_2 is not -1 but rather is a fourth or sixth root of unity. This still forces G_ψ^+ and G_ψ^- to have infinitely many zeros, which is enough to make the above argument work. □

4. The half-logarithms $\log_p^+$ and $\log_p^-$

In the proof of Theorem 3.5, it was shown that for a modular form f with $a_p = 0$ we can write

$$L_p(f, \alpha, \psi, T) = G_\psi^+(T) + G_\psi^-(T) \cdot \alpha,$$

where G_ψ^+ vanishes at $\zeta_{2n} - 1$ and G_ψ^- vanishes at $\zeta_{2n-1} - 1$ for all $n > 0$. The interpolation data also forces $G_\psi^+(\gamma^j \cdot \zeta_{2n} - 1) = G_\psi^-(\gamma^j \cdot \zeta_{2n-1} - 1) = 0$ for $0 \le j \le k-2$. We will see that G_ψ^+ and G_ψ^- have only finitely more zeros than this fixed set of forced roots.

In fact, there exist two power series $\log_p^+$ and $\log_p^-$ in $\mathscr{A}(\mathbf{Q}_p)$, depending only on k and γ, such that $\log_p^+$ and $\log_p^-$ have simple zeros at $\gamma^j \cdot \zeta_{2n} - 1$ and $\gamma^j \cdot \zeta_{2n-1} - 1$, respectively, for j between zero and $k-2$, $n>0$ and such that

$$\frac{G_\psi^+}{\log_p^+} \qquad \text{and} \qquad \frac{G_\psi^-}{\log_p^-}$$

have bounded coefficients. (Recall that if $p=2$, then there is a parity switch and the roles of $\log_p^+$ and $\log_p^-$ should be interchanged.) The notation $\log_p^\pm$ is chosen to reflect the fact that $p^2 \cdot T \cdot \log_p^+ \cdot \log_p^-$ equals the p-adic logarithm when $k=2$.

In this section we construct $\log_p^+$ and $\log_p^-$ as an infinite product of cyclotomic polynomials. We also study the rate of growth of $\log_p^\pm$, prove a trivial functional equation for these power series, and state an interpolation property that they satisfy.

4.1. Construction of $\log_p^\pm$

We first construct two functions $\log_{p,j}^+$ and $\log_{p,j}^-$ in $\mathscr{A}(\mathbf{Q}_p)$ which vanish at $\gamma^j \cdot \zeta_{2n}-1$ and $\gamma^j \cdot \zeta_{2n-1}-1$, respectively, for a *fixed* integer j and all $n>0$. We then take the product of these functions over j between zero and $k-2$ to form our main functions $\log_p^+$ and $\log_p^-$.

Let $\Phi_n(T)=\sum_{t=0}^{p-1} T^{p^{n-1}\cdot t}$ be the p^nth cyclotomic polynomial.

LEMMA 4.1
For any integer j, the products

$$\log_{p,j}^+(T) := \frac{1}{p} \cdot \prod_{n=1}^{\infty} \left(\frac{\Phi_{2n}(\gamma^{-j}(1+T))}{p} \right),$$
$$\log_{p,j}^-(T) := \frac{1}{p} \cdot \prod_{n=1}^{\infty} \left(\frac{\Phi_{2n-1}(\gamma^{-j}(1+T))}{p} \right)$$

converge and define power series in $\mathbf{Q}_p[[T]]$ which are convergent on the open unit disc. The zeros of $\log_{p,j}^+$ (resp., $\log_{p,j}^-$) are precisely $\gamma^j \cdot \zeta_{2n}-1$ (resp., $\gamma^j \cdot \zeta_{2n-1}-1$) for $n>0$, and these are all simple zeros.

Proof
We prove the convergence for the first product; the proof for the second is similar. To see that the product converges, it suffices to see that

$$\frac{\Phi_{2n}\left(\gamma^{-j}(1+T)\right)}{p} \to 1 \quad \text{as } n \to \infty.$$

Let $f_n(T)=(1/p)\Phi_{2n}(\gamma^{-j}(1+T))-1$; we must show that $f_n \to 0$ as $n \to \infty$.

We have for $k < 2n$,

$$f_n(\gamma^j \cdot \zeta_k - 1) = \frac{\Phi_{2n}(\zeta_k)}{p} - 1 = \frac{1}{p}\Bigl(\sum_{t=0}^{p-1} \zeta_k^{p^{n-1}t}\Bigr) - 1 = \frac{1}{p}(p) - 1 = 0.$$

So if $\omega_{n,j} = (\gamma^{-j} \cdot (1+T))^{p^{2n-1}} - 1$, then $\omega_{n,j} \mid f_n$. Since it is clear that $\omega_{n,j} \to 0$ as $n \to \infty$, we get our desired convergence.

As for the zeros of these power series, by construction, $\log_{p,j}^{+}$ (resp., $\log_{p,j}^{-}$) vanishes at $\gamma^j \cdot \zeta_{2n} - 1$ (resp., $\gamma^j \cdot \zeta_{2n-1} - 1$). To see that these are the only zeros, note that

$$\begin{aligned}\log_p\bigl(\gamma^{-j}(1+T)\bigr) &= \lim_{n\to\infty} \frac{(\gamma^{-j}(1+T))^{p^n} - 1}{p^n} \\ &= \bigl(\gamma^{-j} \cdot (1+T) - 1\bigr) \cdot \lim_{n\to\infty} \prod_{k=1}^{n} \frac{\Phi_k(\gamma^{-j} \cdot (1+T))}{p},\end{aligned}$$

and hence

$$p^2 \cdot \log_{p,j}^{+}(T) \cdot \log_{p,j}^{-}(T) = \frac{\log_p(\gamma^{-j}(1+T))}{\gamma^{-j} \cdot (1+T) - 1}.$$

Since $\log_p(\gamma^{-j}(1+T))$ has simple zeros at $\gamma^j \cdot \zeta_n - 1$ for $n \geq 0$ and no other zeros, the zeros of $\log_{p,j}^{-}$ and $\log_{p,j}^{+}$ are exactly as specified in the lemma and all of these zeros are simple. □

COROLLARY 4.2

The power series

$$\log_p^{+}(T) := \prod_{j=0}^{k-2} \log_{p,j}^{+}(T),$$

$$\log_p^{-}(T) := \prod_{j=0}^{k-2} \log_{p,j}^{-}(T)$$

in $\mathbf{Q}_p[[T]]$ *(depending only on* k *and our chosen generator* γ*) are convergent on the open unit disc, and the only zeros of* $\log_p^{+}$ *(resp.,* $\log_p^{-}$*) are simple zeros at* $\gamma^j \cdot \zeta_{2n} - 1$ *(resp.,* $\gamma^j \cdot \zeta_{2n-1} - 1$*) for* $0 \leq j \leq k-2$ *and for* $n > 0$.

Proof

This all follows from Lemma 4.1. □

COROLLARY 4.3

We have

$$\log_p^+(T) \cdot \log_p^-(T) = \prod_{j=0}^{k-2} \frac{\log_p(\gamma^{-j} \cdot (1+T))}{p^2 \cdot (\gamma^{-j} \cdot (1+T) - 1)}.$$

Proof

This formula follows from the proof of Lemma 4.1. □

4.2. The rate of growth of $\log_p^\pm$

Definition 4.4

For F and G locally analytic functions on the open unit disk of $\mathbf{C}_p$, we say that $F \sim G$ if F is $\mathrm{O}(G)$ and G is $\mathrm{O}(F)$.

LEMMA 4.5

We have $\log_p^+(T) \sim \log_p^-(T) \sim \log_p(1+T)^{(k-1)/2}$.

Proof

By Corollary 4.3, it suffices to show that $\log_p^+ \sim \log_p^-$. We have

$$\sup_{|z|_p<r} \left|\Phi_n\big(\gamma^{-j} \cdot (1+z)\big)\right|_p = \frac{r}{p^{n-1}(p-1)}.$$

Comparing our infinite products term by term, we see that $\log_p^+$ is $\mathrm{O}(\log_p^-)$ and $\log_p^-$ is $\mathrm{O}(T \cdot \log_p^+)$. But T is bounded, and hence $\log_p^+ \sim \log_p^-$. □

4.3. Functional equations for $\log_p^\pm$

The natural change of variables in the T-variable for a functional equation is $T \mapsto 1/(1+T) - 1$. The next lemma shows that $\log_p^+$ and $\log_p^-$ are invariant under this change of variable when $k = 2$.

LEMMA 4.6

For $k = 2$ *we have*

$$\log_p^+\left(\frac{1}{1+T} - 1\right) = \log_p^+(T),$$
$$\log_p^-\left(\frac{1}{1+T} - 1\right) = \log_p^-(T).$$

Proof

We prove the functional equation for $\log_p^+$; the argument for $\log_p^-$ is the same. By definition,

$$\begin{aligned}\log_p^+\left(\frac{1}{1+T}-1\right) &= \frac{1}{p}\prod_{k=1}^{\infty}\frac{\Phi_{2k}(1/(1+T))}{p}\\ &= \frac{1}{p}\prod_{k=1}^{\infty}\frac{\Phi_{2k}(1+T)\cdot(1+T)^{p^{2k-1}(p-1)}}{p}\end{aligned}$$

(since the roots of Φ_{2k} are invariant under $z \mapsto z^{-1}$)

$$= \frac{1}{p}\prod_{k=1}^{\infty}\frac{\Phi_{2k}(1+T)}{p} = \log_p^+(T)$$

since $\prod_{k=1}^{\infty}(1+T)^{p^{2k-1}(p-1)} = 1$. □

4.4. Interpolation property of $\log_p^{\pm}$

In the case where $k=2$, both $\log_p^+(T)$ and $\log_p^-(T)$ are $o(\log_p(1+T))$, and hence they are uniquely determined by their values at $\zeta_n - 1$ for all n. The following lemma describes these values.

LEMMA 4.7

For $k=2$*,*

$$\log_p^+(\zeta_n-1) = \begin{cases} 0, & 2 \mid n,\\ p^{-(n+1)/2}\cdot\prod_{j=1}^{(n-1)/2}\Phi_{2j}(\zeta_n), & 2 \nmid n,\end{cases}$$

$$\log_p^-(\zeta_n-1) = \begin{cases} p^{-n/2-1}\cdot\prod_{j=1}^{n/2}\Phi_{2j-1}(\zeta_n), & 2 \mid n,\\ 0, & 2 \nmid n.\end{cases}$$

Proof

For $m > n$,

$$\Phi_m(\zeta_n) = 1 + (\zeta_n)^{p^{m-1}} + \cdots + (\zeta_n)^{p^{m-1}(p-1)} = p.$$

Hence the terms in the tail-end of the products describing $\log_p^{\pm}(\zeta_n - 1)$ are all 1, and the beginning part of the product is what appears in the above formulas. □

The following lemma computes the valuations of these special values and is useful in Section 6.3.

LEMMA 4.8
For $k = 2$,

$$\operatorname{ord}_p\left(\log_p^+(\zeta_n - 1)\right) = \frac{p^{n-1} - p^{n-2} + \cdots + p^2 - p}{p^{n-1}(p-1)} - \frac{n+1}{2} \quad \text{for } n \text{ odd},$$
$$\operatorname{ord}_p\left(\log_p^-(\zeta_n - 1)\right) = \frac{p^{n-1} - p^{n-2} + \cdots + p - 1}{p^{n-1}(p-1)} - \frac{n+2}{2} \quad \text{for } n \text{ even}.$$

Proof
For $m < n$,

$$\Phi_m(\zeta_n) = \frac{(\zeta_n)^{p^m} - 1}{(\zeta_n)^{p^{m-1}} - 1} = \frac{\zeta_{n-m} - 1}{\zeta_{n-m+1} - 1}.$$

Hence

$$\operatorname{ord}_p\left(\Phi_m(\zeta_n)\right) = \frac{p^m - p^{m-1}}{p^{n-1}(p-1)}$$

and the lemma follows. □

5. Description of p-adic L-functions in terms of $\log_p^+$ and $\log_p^-$

5.1. Main result

Recall that f is a modular form of weight k, level N, and character ε which is an eigenform for all T_n. We have that $K(f)$ is the number field generated by the eigenvalues of f and the value of ε. Let p be a prime number, and let K be the completion of $K(f)$ at our chosen prime over p. Let ψ be a Dirichlet character of conductor M. Here both M and N are assumed to be prime to p. Let K_ψ be the field generated by the values of ψ over K, and let $\mathscr{O}_\psi$ be its ring of integers. Finally, let $\Lambda_\psi = \mathscr{O}_\psi[[T]]$ be the Iwasawa algebra.

THEOREM 5.1
If p is odd and $a_p = 0$, then

$$L_p(f, \alpha, \psi, T) = L_p^+(f, \psi, T) \cdot \log_p^+(T) + L_p^-(f, \psi, T) \cdot \log_p^-(T) \cdot \alpha,$$

where $L_p^\pm(f, \psi, T) \in \Lambda_\psi \otimes K_\psi$. If $p = 2$ and $a_2 = 0$, then

$$L_2(f, \alpha, \psi, T) = L_2^+(f, \psi, T) \cdot \log_2^-(T) + L_2^-(f, \psi, T) \cdot \log_2^+(T) \cdot \alpha,$$

where $L_2^\pm(f, \psi, T) \in \Lambda_\psi \otimes K_\psi$.

Proof
We argue in the case where p is odd. Write

$$L_p(f, \alpha, \psi, T) = G_\psi^+(T) + G_\psi^-(T) \cdot \alpha,$$

as in the proof of Theorem 3.5. The interpolation property from Proposition 2.11 forces

$$G_\psi^+(\gamma^j \cdot \zeta_{2n} - 1) = 0 \qquad \text{and} \qquad G_\psi^-(\gamma^j \cdot \zeta_{2n-1} - 1) = 0$$

for $0 \le j \le k-2$ and all $n > 0$. Since all the zeros of $\log_p^+$ (resp., $\log_p^-$) are also zeros of G_ψ^+ (resp., G_ψ^-), [12, (4.8)] tells us that

$$\log_p^+ \mid G_\psi^+ \qquad \text{and} \qquad \log_p^- \mid G_\psi^-$$

in $K_\psi[[T]]$ (even in $\mathscr{A}(K_\psi)$). Let

$$L_p^+(f, \psi, T) = \frac{G_\psi^+}{\log_p^+} \qquad \text{and} \qquad L_p^-(f, \psi, T) = \frac{G_\psi^-}{\log_p^-}.$$

By Theorem 2.6, $G_\psi^+(T)$ and $G_\psi^-(T)$ are $\mathrm{O}(\log_p(1+T)^{(k-1)/2})$, and by Lemma 4.5, $\log_p^+(T) \sim \log_p^-(T) \sim \log_p(1+T)^{(k-1)/2}$. Hence both $L_p^+(f, \psi, T)$ and $L_p^-(f, \psi, T)$ are $\mathrm{O}(1)$ (i.e., bounded). From the following lemma, we can conclude that $L_p^+(f, \psi, T)$ and $L_p^-(f, \psi, T)$ have bounded coefficients and thus lie in $\Lambda_\psi \otimes K_\psi$. □

LEMMA 5.2
If $G \in \mathscr{A}(K)$ is a bounded analytic function, then G has bounded coefficients.

Proof
Let $G(T) = \sum_i a_i T^i$, and let $N = \sup_{|z|_p<1} G(z)$. Then this maximum value is given by $N = \sup_{i,z} |a_i z^i|_p$, and taking $|z|_p$ close to 1, we conclude that $|a_i|_p \le N$. □

5.2. The case of elliptic curves

5.2.1. Definition of p-adic L-functions

Let E be an elliptic curve over $\mathbf{Q}$. Since E is modular (see [29], [4]), we define the p-adic L-function of E to be the p-adic L-function of the corresponding modular form. More precisely, let $\pi : X_0(N) \to E$ be a modular parametrization, so that $\pi^*(\omega_E) = c \cdot f_E \cdot dq/q$ with c the Manin constant for π and f_E a normalized newform of weight 2 and level N. Here, ω_E is the Néron differential of E.

To define the p-adic L-function of f_E, we need to make a choice of periods (as in Theorem 2.7). We now pin down these two periods up to sign. Let $\delta^\pm$ generate $H_1(E, \mathbf{Z})^\pm$. Define

$$\Omega_E^\pm := \begin{cases} \int_{\delta^\pm} \omega_E & \text{if } E(\mathbf{R}) \text{ is connected,} \\ 2 \cdot \int_{\delta^\pm} \omega_E & \text{otherwise,} \end{cases}$$

which is uniquely determined up to sign. We then define the p-adic L-function of E by $L_p(E,\alpha,\cdot) = L_p(f_E,\alpha,\cdot)$, where the p-adic L-function of f_E is defined using $\Omega_E^{\pm}$.

Remark 5.3

In Section 2.2, modular symbols were notated by $\lambda^{\pm}(f, P; a, m)$, where P is an integral polynomial of degree less than or equal to $k-2$. Since $k=2$ for elliptic curves, the P term becomes irrelevant. Furthermore, when P is trivial, $\lambda^{\pm}(f, P; a, m)$ depends only on the rational number a/m. In the case of elliptic curves, we adopt the (standard) notation

$$\left[\frac{a}{m}\right]^{\pm} := \lambda^{\pm}(f_E, 1; a, m).$$

Remark 5.4

The periods $\Omega_E^{\pm}$ do not necessarily satisfy the requirements of Theorem 2.7. For example, take $E = X_0(11)$ and $p=5$. Then

$$[0]^+ = \frac{\left(\int_{i\infty}^{0} f_E\right)}{\Omega_E^+} = \frac{1}{5}.$$

However, for a fixed curve E, the denominators of the modular symbols are bounded. In fact, at a prime of good reduction with $a_p \not\equiv 1 \pmod{p}$, then $2[a/p^n]^{\pm} \in c^{-1}\mathbf{Z}$, where c is the Manin constant for E (see [14, Theorem 3.3]).

Remark 5.5

For p a prime of good supersingular reduction, the Manin constant c is prime to p. This fact follows from the fact that $E[p]$ is irreducible and from [17, Corollary 4.1] when p is odd and [1] when $p=2$. In particular, $2[a/p^n]^{\pm} \in \mathbf{Z}_p$ for such p.

5.2.2. *Main result for elliptic curves*

When $a_p \equiv 0 \pmod{p}$, we are in the supersingular case, and then certainly $L_p(E,\alpha,T) \notin \mathbf{Z}_p[[T]]$. In fact, by Theorem 3.5, $L_p(E,\alpha,T) \notin \mathbf{Z}_p[[T]] \otimes \mathbf{Q}_p$. We know from Theorem 5.1 that $L_p^+(E,T)$ and $L_p^-(E,T)$ have bounded coefficients. In the case of elliptic curves, we can strengthen this to say that they are actually integral power series.

THEOREM 5.6

Let $E/\mathbf{Q}$ be an elliptic curve with $a_p = 0$. If p is odd, we have

$$L_p(E,\alpha,T) = L_p^+(E,T)\cdot \log_p^+(T) + L_p^-(E,T)\cdot \log_p^-(T)\cdot \alpha$$

with $L_p^+(E,T), L_p^-(E,T) \in \mathbf{Z}_p[[T]]$*, and if* $p = 2$*, we have*

$$L_2(E,\alpha,T) = L_2^+(E,T)\cdot \log_2^-(T) + L_2^-(E,T)\cdot \frac{1}{2}\log_2^+(T)\cdot\alpha$$

with $L_2^+(E,T), L_2^-(E,T) \in \mathbf{Z}_2[[T]]$.

Remark 5.7
The extra factor of $1/2$ appearing when $p = 2$ is necessary to ensure that $L_2^-(E,T)$ lies in $\mathbf{Z}_2[[T]]$.

Remark 5.8
To ease notation, at times we refer to $L_p^{\pm}(E,T)$ as $L_p^{\pm}$.

Since the weight of f_E is 2, $L_p(E,\alpha,T)$ is defined by a limit of standard Riemann sums that lend themselves to explicit computation. Approximating by Riemann sums, we have $L_p(E,\alpha,T) = \lim_{n\to\infty} L_n$, where

$$L_n = \sum_{a\in(\mathbf{Z}/p^n)^\times} \mu_{f,\alpha}^{\pm}(a + p^n\mathbf{Z}_p)\cdot(1+T)^{\log_p(a)/\log_p(\gamma)}. \tag{2}$$

If $L_n = G_n^+ + G_n^-\cdot\alpha$, then $G_n^+ \to G^+$ and $G_n^- \to G^-$. The following lemma gives precise formulas for G_n^+ and G_n^-. The proof of Theorem 5.6 then follows from simply counting the number of p's in the denominator of $L_p^{\pm}(E,T)$ and seeing that there are none.

LEMMA 5.9
For p odd,

$$G_n^+ = \begin{cases} (-p)^{-(n/2)} \displaystyle\sum_{a\in(\mathbf{Z}/p^n)^\times} \left[\frac{a}{p^n}\right]^+ (1+T)^{\log_p(a)/\log_p(\gamma)}, & 2 \mid n, \\ (-p)^{-((n+1)/2)} \displaystyle\sum_{a\in(\mathbf{Z}/p^n)^\times} \left[\frac{a}{p^{n-1}}\right]^+ (1+T)^{\log_p(a)/\log_p(\gamma)}, & 2 \nmid n \end{cases}$$

and

$$G_n^- = \begin{cases} (-p)^{-(n/2+1)} \displaystyle\sum_{a\in(\mathbf{Z}/p^n)^\times} \left[\frac{a}{p^{n-1}}\right]^+ (1+T)^{\log_p(a)/\log_p(\gamma)}, & 2 \mid n, \\ (-p)^{-((n+1)/2)} \displaystyle\sum_{a\in(\mathbf{Z}/p^n)^\times} \left[\frac{a}{p^n}\right]^+ (1+T)^{\log_p(a)/\log_p(\gamma)}, & 2 \nmid n. \end{cases}$$

Proof
Writing the expression for L_n in (2) in terms of 1 and α yields the above formulas for G_n^+ and G_n^- (see also [3, page 230]). □

Proof of Theorem 5.6
We prove this for p odd and for L_p^+; the other cases follow similarly. Note that for $1 \leq k \leq n-1$, $L_n(\zeta_k - 1) = L_p(E, \alpha, \zeta_k - 1)$ since the Riemann sum perfectly approximates the integral. We know that $G^+(\zeta_{2k} - 1) = 0$, and hence we have $G_n^+(\zeta_{2k} - 1) = 0$ for $1 \leq k \leq [(n-1)/2]$.

Therefore we can write

$$G_n^+ = \Big(\frac{1}{p} \prod_{k=1}^{[(n-1)/2]} \frac{\Phi_{2k}(1+T)}{p}\Big) \cdot L_{p,n}^+ \quad \text{with } L_{p,n}^+ \in \mathbf{Q}_p[T].$$

But from Lemma 5.9 and Remark 5.5, we see that $p^{[(n+1)/2]} \cdot G_n^+ \in \mathbf{Z}_p[T]$. Since each $\Phi_{2k}(1+T)$ divides $p^{[(n+1)/2]} \cdot G_n^+$ in $\mathbf{Z}_p[T]$, we conclude that $L_{p,n}^+$ has integral coefficients.

Taking limits yields

$$G^+ = \log_p^+ \cdot L_p^+ \quad \text{with } L_p^+ \in \mathbf{Z}_p[[T]].$$

The case is similar for L_p^- and for $p = 2$. (Note that for $p = 2$, one must exploit a symmetry in the Riemann sum defining $L_p(E, \alpha, T)$ to remove the extra factor of 2 appearing in Remark 5.5.) □

The following theorem of Rohrlich guarantees that the p-adic L-function and $L_p^\pm$ are not identically zero.

THEOREM 5.10
Let $E/\mathbf{Q}$ be an elliptic curve, and let p be a prime number. Then there are only a finite number of characters χ of p-power order and conductor such that $L(E, \chi, 1) = 0$.

Proof
See [24]. □

COROLLARY 5.11
We have that $L_p(E, \alpha, T)$, $L_p^+(E, T)$, and $L_p^-(E, T)$ are all nonzero functions.

Proof
Theorem 5.10 implies that $L_p(E, \alpha, T)$ is a nonzero function since, by Proposition 2.11, it interpolates the values of $L(E, \chi, 1)$. Also, we have

$$L_p(E, \alpha, \zeta_{2n-1} - 1) = L_p^+(E, \zeta_{2n-1} - 1) \cdot \log_p^+(\zeta_{2n-1} - 1),$$
$$L_p(E, \alpha, \zeta_{2n} - 1) = L_p^-(E, \zeta_{2n} - 1) \cdot \log_p^-(\zeta_{2n} - 1) \cdot \alpha.$$

Since $\log_p^+(\zeta_{2n-1}-1)$ and $\log_p^-(\zeta_{2n}-1)$ are both nonzero, it follows that $L_p^+(E,T)$ and $L_p^-(E,T)$ are also nonzero functions. □

COROLLARY 5.12
Let $E/\mathbf{Q}$ be an elliptic curve, and let p be a prime with $a_p=0$. Then $L_p(E,\alpha,T)$ and $L_p(E,\overline{\alpha},T)$ have only finitely many common zeros.

Proof
Any common zero of $L_p(E,\alpha,T)$ and $L_p(E,\overline{\alpha},T)$ is a zero of both G^+ and G^-. By Theorem 5.6, $G^+=\log_p^+\cdot L_p^+$ and $G^-=\log_p^-\cdot L_p^-$ with $L_p^\pm\in\mathbf{Z}_p[[T]]$. Now $\log_p^+$ and $\log_p^-$ have no common zeros, while L_p^+ and L_p^- have only finitely many common zeros (by Corollary 5.11). From this we conclude that G^+ and G^- share only finitely many roots, completing the proof. □

5.2.3. *Functional equations for $L_p^\pm(E,T)$*

The functional equation for $L_p(E,\alpha,\chi_u)$ reads

$$L_p(E,\alpha,\chi_u)=\epsilon_N\cdot u^c\cdot L_p(E,\alpha,\chi_{u^{-1}}),$$

where ϵ_N is the negative of the sign of f_E (i.e., $w_N(f_E)=-\epsilon_N f_E$) and $c\in\mathbf{Z}_p^\times$ is such that $\gamma^{-c}=\langle N\rangle$. Here $\langle\cdot\rangle:\mathbf{Z}_p^\times\twoheadrightarrow 1+p\mathbf{Z}_p$ is the natural projection. In terms of $L_p(E,\alpha,T)$, we have

$$L_p(E,\alpha,T)=\epsilon_N\cdot(1+T)^c\cdot L_p\Big(E,\alpha,\frac{1}{1+T}-1\Big).$$

Both $L_p^+(E,T)$ and $L_p^-(E,T)$ satisfy a functional equation of this type.

THEOREM 5.13
With $L_p^+(E,T)$ and $L_p^-(E,T)$ as in Theorem 5.1,

$$L_p^+(E,T)=\epsilon_N\cdot(1+T)^c\cdot L_p^+\Big(E,\frac{1}{1+T}-1\Big)$$

and

$$L_p^-(E,T)=\epsilon_N\cdot(1+T)^c\cdot L_p^-\Big(E,\frac{1}{1+T}-1\Big).$$

Proof
From Lemma 4.6, we know that

$$\log_p^+\Big(\frac{1}{1+T}\Big)=\log_p^+(T)\qquad\text{and}\qquad\log_p^-\Big(\frac{1}{1+T}\Big)=\log_p^-(T).$$

So expressing the functional equation for $L_p(E,\alpha,T)$ in terms of $L_p^+(E,T)$ and $L_p^-(E,T)$ yields

$$\begin{aligned}\log_p^+(T)\cdot\Bigl(L_p^+(E,T)-\epsilon_N(1+T)^c L_p^+\Bigl(E,\frac{1}{1+T}-1\Bigr)\Bigr)\\ =\log_p^-(T)\cdot\Bigl(L_p^-(E,T)-\epsilon_N(1+T)^c L_p^-\Bigl(E,\frac{1}{1+T}-1\Bigr)\Bigr)\cdot\alpha.\end{aligned}$$

But the nonzero coefficients of the left-hand side have valuations in $\mathbf{Z}$, while on the right-hand side each has valuation $n/2$ with n an odd integer. This forces both sides to be identically zero, and the functional equations for $L_p^+(E,T)$ and $L_p^-(E,T)$ follow. □

5.3. *Algebraic p-adic L-functions*

In [22], Perrin-Riou constructed algebraic p-adic L-functions attached to elliptic curves at odd supersingular primes. The natural setting of these algebraic p-adic L-functions is a ring of power series with growth tensored by the Dieudonné module associated to the elliptic curve.

Translating into our more naive language of p-adic power series, for each root α of $x^2-a_px+p=0$ there exists an algebraic p-adic L-function (determined up to a unit power series). This L-function (denoted by $L_p^{\mathrm{alg}}(E,\alpha,T)$) is in $\mathscr{A}(\mathbf{Q}_p(\alpha))$ and is $\mathrm{O}(\log_p(1+T)^{1/2})$.

Remark 5.14

When context demands, we refer to $L_p(E,\alpha,T)$ defined in Section 2.3 and $L_p^\pm(E,T)$ constructed in Section 5.2.2 as $L_p^{\mathrm{an}}(E,\alpha,T)$ and $L_p^{\mathrm{an},\pm}(E,T)$, respectively, to emphasize that they are analytic p-adic L-functions.

The following is the main conjecture for elliptic curves in the supersingular case (see [22, page 985] and [23, Conjecture 3.1.1]).

CONJECTURE 5.15 (Main conjecture)

Let E be an elliptic curve over $\mathbf{Q}$ with p a supersingular prime. Then

$$L_p^{\mathrm{an}}(E,\alpha,T)=u(T)\cdot L_p^{\mathrm{alg}}(E,\alpha,T),$$

where $u(T)$ is a unit in $\mathbf{Z}_p[[T]]$.

As in the ordinary case, much progress has been made towards this result using Kato's construction of an Euler system for the Tate module of E.

THEOREM 5.16 (Kato)
Let p be an odd prime, and let $E/\mathbf{Q}$ be an elliptic curve. Then

$$L_p^{\mathrm{an}}(E,\alpha,T) = h(T)\cdot L_p^{\mathrm{alg}}(E,\alpha,T),$$

where $h(T)\in \mathbf{Z}_p[[T]]\otimes\mathbf{Q}_p$. Furthermore, if the Galois representation on the p-torsion of E is surjective, then $h(T)$ can be taken to be in $\mathbf{Z}_p[[T]]$.

Proof
See [9, Theorem 12.5] and [23, Théorème 3.1.3]. □

The results of Section 5.1 also apply to $L_p^{\mathrm{alg}}(E,\alpha,T)$ in the case $a_p=0$.

THEOREM 5.17
Let $E/\mathbf{Q}$ be an elliptic curve, and let p be an odd prime with $a_p=0$. Then

$$L_p^{\mathrm{alg}}(E,\alpha,T) = L_p^{\mathrm{alg},+}(E,T)\cdot\log_p^+(T) + L_p^{\mathrm{alg},-}(E,T)\cdot\log_p^-(T)\cdot\alpha$$

with $L_p^{\mathrm{alg},+}(E,T), L_p^{\mathrm{alg},-}(E,T)\in\mathbf{Z}_p[[T]]\otimes\mathbf{Q}_p$.

Proof
We have that $L_p^{\mathrm{alg}}(E,\alpha,T)\pm L_p^{\mathrm{alg}}(E,\overline{\alpha},T)$ vanishes at $\zeta_{2n}-1$ (resp., $\zeta_{2n-1}-1$) for $n\geq 1$ (see [22, Proposition 2.1.4]). Furthermore, these algebraic L-functions are $\mathrm{O}(\log_p(1+T)^{1/2})$ (see [9, Theorem 16.4(ii)]). The theorem then follows from these two facts as in the proof of Theorem 5.1. □

COROLLARY 5.18
If p is odd and $a_p=0$, then $L_p^{\mathrm{alg},\pm}(E,T)\mid L_p^{\mathrm{an},\pm}(E,T)$ in $\mathbf{Z}_p[[T]]\otimes\mathbf{Q}_p$.

Proof
This result is immediate from Theorem 5.16. □

6. Consequences for elliptic curves in the cyclotomic direction

Let $\mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$-extension with subfields $\mathbf{Q}_n$ of degree p^n over $\mathbf{Q}$. The arithmetic of an elliptic curve E along this extension is conjecturally controlled by the special values of $L_p^{\mathrm{an}}(E,\alpha,T)$. In this section we explore the conjectural consequences of Theorem 5.6 in this setting.

6.1. Iwasawa invariants of p-adic L-functions

For $f(T)\in\mathbf{Z}_p[[T]]\otimes\mathbf{Q}_p$, we can write

$$f(T) = p^{\mu(f)}\cdot P(T)\cdot U(T)$$

with $P(T)$ a distinguished polynomial of degree $\lambda(f)$ and $U(T)$ a unit power series. The values $\mu(f)$ and $\lambda(f)$ are the Iwasawa invariants of $f(T)$.

Such invariants can be attached to the p-adic L-function of an elliptic curve at an ordinary prime p. However, for a supersingular prime, the L-functions have growth and do not have a single λ- or μ-invariant. Instead, we can define two λ-invariants and two μ-invariants for each L-function based upon Theorem 5.6 and Theorem 5.17.

Definition 6.1
Let $E/\mathbf{Q}$ be an elliptic curve with $a_p = 0$. Then define

$$\lambda_{\text{an}}^{\pm} = \lambda(L_p^{\text{an},\pm}), \qquad \lambda_{\text{alg}}^{\pm} = \lambda(L_p^{\text{alg},\pm}),$$
$$\mu_{\text{an}}^{\pm} = \mu(L_p^{\text{an},\pm}), \qquad \text{and} \qquad \mu_{\text{alg}}^{\pm} = \mu(L_p^{\text{alg},\pm}).$$

Remark 6.2
These λ- and μ-invariants were also defined by Perrin-Riou in [23]. Her method differs from the one presented here in that she constructs these invariants without needing to build the underlying Iwasawa functions $L_p^{\text{an},\pm}(E,T)$ or $L_p^{\text{alg},\pm}(E,T)$. Her construction also allows these invariants to be defined even in the case where $a_p \neq 0$ (but is still divisible by p).

In the ordinary case, R. Greenberg has conjectured that the μ-invariant vanishes when $E[p]$ is irreducible (see [7, Conjecture 1.11]). When p is supersingular, $E[p]$ is always irreducible. This observation together with a large amount of numerical data leads us to extend his conjecture to the supersingular case.

CONJECTURE 6.3
Let $E/\mathbf{Q}$ be an elliptic curve, and let p be a prime such that $a_p = 0$. Then $\mu_{\text{an}}^{\pm} = \mu_{\text{alg}}^{\pm} = 0$.

Both λ-invariants can be further refined. Let P be a distinguished polynomial. Decompose P as a product $P_{MW} \cdot P_{Ш}$, where P_{MW} vanishes (with correct multiplicity) at all of the p-cyclotomic zeros of P (i.e., the zeros of the form $\zeta_n - 1$). Let λ_{MW} be the degree of P_{MW}, and let $\lambda_{Ш}$ be the degree of $P_{Ш}$, so that $\lambda = \lambda_{MW} + \lambda_{Ш}$.

In the following sections we give bounds for the analytic rank of $E(\mathbf{Q}_\infty)$ and asymptotic formulas for the analytic size of $Ш(E/\mathbf{Q}_n)_{p^\infty}$ in terms of these μ- and λ-invariants.

6.2. Growth of the Mordell-Weil group in the cyclotomic direction
Let E be an elliptic curve over $\mathbf{Q}$, and let p be any prime number (not necessarily supersingular for E).

Definition 6.4

The *(p-adic) analytic rank* of $E(\mathbf{Q}_n)$ is defined by

$$r^{\mathrm{an}}\big(E(\mathbf{Q}_n)\big) = \sum_{\zeta} \operatorname{ord}_{\zeta-1}\big(L_p^{\mathrm{an}}(E,\alpha,T)\big),$$

where the sum is taken over all p^nth roots of unity and $\operatorname{ord}_{\zeta-1}(\cdot)$ represents the order of vanishing at $\zeta - 1$.

Remark 6.5

The p-adic analytic rank should conjecturally agree with the (complex) analytic rank of $E(\mathbf{Q}_n)$ defined by the order of vanishing of the complex L-series $L(E/\mathbf{Q}_n, s)$ at 1 so long as E has good reduction at p.

The following lemma says that in the supersingular case the above definition is independent of α.

LEMMA 6.6

Let $E/\mathbf{Q}$ be an elliptic curve, and let p be a supersingular prime for E with $a_p = 0$. Then

$$\sum_{\zeta} \operatorname{ord}_{\zeta-1}\big(L_p^{\mathrm{an}}(E,\alpha,T)\big) = \sum_{\zeta} \operatorname{ord}_{\zeta-1}\big(L_p^{\mathrm{an}}(E,\overline{\alpha},T)\big).$$

Proof

Let $f^{(n)}$ represent the nth derivative of f. Then $L_p^{(n)}(E,\alpha,T)$ and $L_p^{(n)}(E,\overline{\alpha},T)$ are conjugate power series related by some $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. Note that σ is independent of n. Hence

$$\operatorname{ord}_{\zeta-1}\big(L_p^{\mathrm{an}}(E,\alpha,T)\big) = \operatorname{ord}_{\zeta^{\sigma}-1}\big(L_p^{\mathrm{an}}(E,\overline{\alpha},T)\big),$$

from which the lemma follows. □

The stronger result that these sums should match up term by term is preferable and expected from Birch and Swinnerton-Dyer–type considerations. We now prove this when $p \equiv 3 \pmod 4$.

LEMMA 6.7

Let $E/\mathbf{Q}$ be an elliptic curve, and let $p \equiv 3 \pmod 4$ be a supersingular prime for E. If ζ is a p^nth root of unity, then

$$\operatorname{ord}_{\zeta-1} L_p^{\mathrm{an}}(E,\alpha,T) = \operatorname{ord}_{\zeta-1} L_p^{\mathrm{an}}(E,\overline{\alpha},T).$$

Proof

Let ζ be a p^nth root of unity, and choose $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ such that $\zeta^\sigma = \zeta^{-1}$. Since $p \equiv 3 \pmod 4$ and α is a square root of $-p$, we have $\alpha^\sigma = -\alpha$. (Consider the representation of α a Gauss sum.) Therefore $L_p^{(n)}(E,\alpha,T)$ and $L_p^{(n)}(E,\overline{\alpha},T)$ are conjugate power series by σ. We conclude that

$$\mathrm{ord}_{\zeta^{-1}-1}\, L_p^{\mathrm{an}}(E,\alpha,T) = \mathrm{ord}_{\zeta-1}\, L_p^{\mathrm{an}}(E,\overline{\alpha},T).$$

Finally, from the functional equation for $L_p(E,\alpha,T)$, we have

$$\mathrm{ord}_{\zeta-1}\, L_p^{\mathrm{an}}(E,\alpha,T) = \mathrm{ord}_{\zeta^{-1}-1}\, L_p^{\mathrm{an}}(E,\alpha,T),$$

which yields the result. □

By a theorem of D. Rohrlich (Theorem 5.10), it is known that $E(\mathbf{Q}_\infty)$ has finite analytic rank. (This is now known algebraically via Kato's Euler system even in the supersingular case; see [25].)

In the ordinary case, it is clear that $r^{\mathrm{an}}(E(\mathbf{Q}_\infty))$ is bounded by the λ-invariant of the p-adic L-function. (In fact, it is equal to λ_{MW}.) In the supersingular case, we give bounds for this analytic rank in terms of the λ-invariants of $L_p^{\mathrm{an},+}(E,T)$ and $L_p^{\mathrm{an},-}(E,T)$.

COROLLARY 6.8

For p a supersingular prime of E such that $p \equiv 3 \pmod 4$ and $a_p = 0$,

$$r^{\mathrm{an}}\big(E(\mathbf{Q}_\infty)\big) \le \lambda_{MW}^{\mathrm{an},+} + \lambda_{MW}^{\mathrm{an},-}.$$

Proof

It suffices to prove the following claim:

$$\mathrm{ord}_{\zeta_n-1}\, L_p^{\mathrm{an}}(E,\alpha,T) \le \begin{cases} \mathrm{ord}_{\zeta_n-1}\, L_p^{\mathrm{an},-}(E,T), & 2 \mid n, \\ \mathrm{ord}_{\zeta_n-1}\, L_p^{\mathrm{an},+}(E,T), & 2 \nmid n, \end{cases}$$

for any p^nth root of unity ζ_n. We consider the case where n is odd; the case of n even is similar.

Applying Lemma 6.7, we have $\mathrm{ord}_{\zeta_n-1}\, L_p^{\mathrm{an}}(E,\alpha,T) = \mathrm{ord}_{\zeta_n-1}\, L_p^{\mathrm{an}}(E,\overline{\alpha},T)$; we call this common value m. Then $G^+(T) = (L_p^{\mathrm{an}}(E,\alpha,T) + L_p^{\mathrm{an}}(E,\overline{\alpha},T))/2$ vanishes at least to order m at $\zeta_n - 1$. Since $G^+ = L_p^{\mathrm{an},+} \cdot \log_p^+$ and $\log_p^+$ is nonzero at $\zeta_n - 1$, we have that $L_p^{\mathrm{an},+}$ also vanishes at least to order m at $\zeta_n - 1$. □

6.3. Valuations of special values of L-series

The description of the p-adic L-function given in Theorem 5.6 allows one to compute the valuations of special values of L-series twisted by finite-order characters of $1+q\mathbf{Z}_p$. Compare the following proposition to [11, Proposition 2.1] and to [23, Proposition 4.1.2].

PROPOSITION 6.9
Let $E/\mathbf{Q}$ be an elliptic curve, and let p be a prime such that $a_p = 0$. Let χ be a character of $\mathbf{Z}_p^\times$ with order p^n. Denote by $\tau(\chi)$ the corresponding Gauss sum. Then for p odd and n large enough,

$$\operatorname{ord}_p\left(\tau(\chi)\frac{L(E,\chi^{-1},1)}{\Omega_E}\right) = \begin{cases} \dfrac{p^{n-1}-p^{n-2}+\cdots+p-1+\lambda_{\mathrm{an}}^-}{p^{n-1}(p-1)} + \mu_{\mathrm{an}}^-, & 2 \mid n, \\ \dfrac{p^{n-1}-p^{n-2}+\cdots+p^2-p+\lambda_{\mathrm{an}}^+}{p^{n-1}(p-1)} + \mu_{\mathrm{an}}^+, & 2 \nmid n. \end{cases}$$

For $p=2$, the Iwasawa invariants of $L_p^{\mathrm{an},+}(E,T)$ and $L_p^{\mathrm{an},-}(E,T)$ are interchanged.

Proof
We give the argument for p and n odd; the other cases are similar. From the interpolation property (Proposition 2.11), we have

$$L_p^{\mathrm{an}}(E,\alpha,\zeta_n-1) = \frac{1}{\alpha^{n+1}} \cdot \frac{p^{n+1}}{\tau(\chi^{-1})} \cdot \frac{L(E,\chi^{-1},1)}{\Omega_E},$$

where $\chi(\gamma)=\zeta_n$. Hence

$$\tau(\chi)\cdot\frac{L(E,\chi^{-1},1)}{\Omega_E} = \pm\alpha^{n+1}\cdot L_p^{\mathrm{an}}(E,\alpha,\zeta_n-1)$$

since $\tau(\chi)\cdot\tau(\chi^{-1}) = \pm p^{n+1}$. To compute the valuation of the right-hand side, we use Theorem 5.1. We have

$$L_p^{\mathrm{an}}(E,\alpha,\zeta_n-1) = \log_p^+(\zeta_n-1)\cdot L_p^{\mathrm{an},+}(E,\zeta_n-1).$$

As usual, write $L_p^{\mathrm{an},+}(E,T) = p^{\mu_{\mathrm{an}}^+}\cdot P^+\cdot U^+$. Since P^+ is a distinguished polynomial, if n is large enough, then the leading term of P^+ dominates and

$$\operatorname{ord}_p\left(L_p^{\mathrm{an},+}(\zeta_n-1)\right) = \mu_{\mathrm{an}}^+ + \frac{\lambda_{\mathrm{an}}^+}{p^{n-1}(p-1)}.$$

Lemma 4.7 computes the valuation of $\log_p^+(\zeta_n-1)$. Putting this all together yields the result. □

6.4. Growth of the Tate-Shafarevich group in the cyclotomic direction

In this section we derive asymptotic formulas for the growth of the p-part of the analytic size of $Ш(E/\mathbf{Q}_n)$ (that is, the size of $Ш(E/\mathbf{Q}_n)_{p^\infty}$ as predicted by the Birch and Swinnerton-Dyer conjecture).

Define the analytic size of the Tate-Shafarevich group by

$$\#\text{Ш}^{\text{an}}(E/\mathbf{Q}_n) := \frac{L^{(r_n)}(E/\mathbf{Q}_n,1)\cdot \#E^{\text{tor}}(\mathbf{Q}_n)^2\cdot\sqrt{D(\mathbf{Q}_n)}}{\Omega_{E/\mathbf{Q}_n}\cdot R(E/\mathbf{Q}_n)\cdot \operatorname{Tam}(E/\mathbf{Q}_n)},$$

where $D(\mathbf{Q}_n)$ is the discriminant, $R(E/\mathbf{Q}_n)$ is the regulator, $\operatorname{Tam}(E/\mathbf{Q}_n)$ is the product of the Tamagawa numbers, $\Omega_{E/\mathbf{Q}_n}$ is the real period, and r_n is the rank of $E(\mathbf{Q}_n)$ (see [13, p. 57] for a precise statement of the Birch and Swinnerton-Dyer conjecture in this level of generality). Furthermore, let r be the rank of $E(\mathbf{Q}_\infty)$.

PROPOSITION 6.10
Let

$$f_n^{\text{an}} = \operatorname{ord}_p\left(\frac{\#\text{Ш}^{\text{an}}(E/\mathbf{Q}_n)}{\#\text{Ш}^{\text{an}}(E/\mathbf{Q}_{n-1})}\right).$$

Then for n large enough and p odd,

$$f_n^{\text{an}} = \begin{cases} p^{n-1}-p^{n-2}+\cdots+p-1+(\lambda_{\text{an}}^- - r)+p^{n-1}(p-1)\cdot\mu_{\text{an}}^-, & 2\mid n,\\ p^{n-1}-p^{n-2}+\cdots+p^2-p+(\lambda_{\text{an}}^+ - r)+p^{n-1}(p-1)\cdot\mu_{\text{an}}^+, & 2\nmid n.\end{cases}$$

(For $p=2$, the roles of $L_p^{\text{an},+}(E,T)$ and $L_p^{\text{an},-}(E,T)$ are reversed.) Moreover, if $\operatorname{ord}_p(L(E,1)/\Omega_E)=0$, *then $f_0^{\text{an}}=f_1^{\text{an}}=0$ and the above formulas are valid for* $n\ge 2$.

Proof
Pick n so large that $E(\mathbf{Q}_n)=E(\mathbf{Q}_{n-1})$, $\operatorname{Tam}(E/\mathbf{Q}_n)=\operatorname{Tam}(E/\mathbf{Q}_{n-1})$, and $L(E,\chi,1)\neq 0$ for χ of order p^n.

We then have

$$\frac{\#\text{Ш}^{\text{an}}(E/\mathbf{Q}_n)}{\#\text{Ш}^{\text{an}}(E/\mathbf{Q}_{n-1})} = \left(\prod_\chi \frac{L(E/\mathbf{Q},\chi,1)}{\Omega_{E/\mathbf{Q}}}\right)\cdot c_n, \tag{3}$$

where the product is taken over all χ corresponding to $\mathbf{Q}_n$ but not to $\mathbf{Q}_{n-1}$ and with

$$\operatorname{ord}_p(c_n) = p^{n-1}(p-1)\cdot\frac{n+1}{2} - r.$$

One determines the valuation of c_n by computing the discriminant of $\mathbf{Q}_n$ and noting that $R(E/\mathbf{Q}_n)=p^{r_n}\cdot R(E/\mathbf{Q}_{n-1})$ and $\Omega_{E/\mathbf{Q}_n}=\left(\Omega_{E/\mathbf{Q}}\right)^{p^n}$.

The result then follows from Proposition 6.9, (3), and the fact that

$$\operatorname{ord}_p\left(\prod_\chi \tau(\chi)\right) = p^{n-1}(p-1)\cdot\frac{n+1}{2},$$

where the product is taken over characters of $\mathbf{Q}_n$ not corresponding to $\mathbf{Q}_{n-1}$. □

Remark 6.11

In the case where $\mathrm{ord}_p(L(E,1)/\Omega_E) = 0$, p is odd, and the Galois representation on $E[p]$ is surjective, Kurihara has proven that $Ш(E/\mathbf{Q}_n)_{p^\infty}$ is finite, and its size is indeed given by the above formulas predicted by Birch and Swinnerton-Dyer (see [11]). Note that in this special case, $\lambda^{\pm}_{\mathrm{an}} = \mu^{\pm}_{\mathrm{an}} = 0$.

Remark 6.12

More generally, Perrin-Riou has proven algebraic formulas for the size of the p-part of $Ш(E/\mathbf{Q}_n)$ (assuming its finiteness) in terms of $\lambda^{\pm}_{\mathrm{alg}}$ and $\mu^{\pm}_{\mathrm{alg}}$ by using the theory of algebraic p-adic L-functions (see [23]). Her formulas agree with the ones above assuming that $\lambda^{\pm}_{\mathrm{an}} = \lambda^{\pm}_{\mathrm{alg}}$ and $\mu^{\pm}_{\mathrm{an}} = \mu^{\pm}_{\mathrm{alg}}$ (i.e., assuming that the main conjecture is true).

Remark 6.13

When p is ordinary,

$$f_n^{\mathrm{an}} = (\lambda_{\mathrm{an}} - r) + p^{n-1}(p-1) \cdot \mu^{\mathrm{an}}.$$

Remark 6.14

Kurihara's and Perrin-Riou's results imply that the size of the Tate-Shafarevich group necessarily grows without bound in the cyclotomic direction. Comparing the formulas of Proposition 6.10 to the formula of Remark 6.13 in the ordinary case, one sees that the analytic explanation for this growth is the presence of the functions $\log_p^{\pm}$ in the p-adic L-function.

6.5. *The Structure of* $Ш(E/\mathbf{Q}_n)_{p^\infty}$

In [11], when $\mathrm{ord}_p(L(E,1)/\Omega_E) = 0$, Kurihara not only determined formulas for the size of $Ш(E/\mathbf{Q}_n)_{p^\infty}$, but he also determined its structure as a Galois module. Its structure is described in terms of the modular elements of Mazur and J. Tate.

Definition 6.15

Let

$$\theta_n(T) := \sum_{\overline{a} \in (\mathbf{Z}/p^{n+1})^\times} \left[\frac{a}{p^{n+1}}\right] \cdot (1+T)^{\log_p(a)/\log_p(\gamma)} \in \mathbf{Q}[T]$$

be the modular element of Mazur and Tate.

Remark 6.16

The θ_n live more naturally in the group algebra $\mathbf{Q}[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$, where they have no dependence on a choice of γ. However, we define the θ_n in this less canonical way to make their relation to $L_p^{\mathrm{an},\pm}$ more apparent in what follows.

We have $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]] \cong \mathbf{Z}_p[[T]]$ with the isomorphism determined by our choice of γ. The following theorem describes the structure of $Ш(E/\mathbf{Q}_n)_{p^\infty}$ as a Λ-module.

THEOREM 6.17 (Kurihara)
Let E be an elliptic curve over $\mathbf{Q}$, and let p be an odd prime such that $\mathrm{ord}_p(L(E,1)/\Omega_E) = 0$, $p \nmid \mathrm{Tam}(E/\mathbf{Q})$, and such that the Galois representation on $E[p]$ is surjective. Then

$$Ш(E/\mathbf{Q}_n)_{p^\infty} \cong \Lambda/(\omega_n, \theta_n, \xi_n\theta_{n-1}),$$

where $\omega_n = (1+T)^{p^n} - 1$ and $\xi_n = \Phi_n(1+T)$.

We wish to interpret the above isomorphism in terms of $L_p^{\mathrm{an},\pm}$, and hence we make the assumption that $a_p = 0$. Let

$$\omega_n^+ = \prod_{1\le 2k\le n} \Phi_{2k}(1+T) \qquad \text{and} \qquad \omega_n^- = \prod_{1\le 2k-1\le n} \Phi_{2k-1}(1+T).$$

Note that $T\omega_n^+\omega_n^- = \omega_n$.

PROPOSITION 6.18
For $E/\mathbf{Q}$ an elliptic curve and p an odd prime with $a_p = 0$, we have

$$\theta_n \equiv \begin{cases} \omega_n^- \cdot L_p^{\mathrm{an},-} \pmod{\omega_n}, & 2 \mid n, \\ \omega_n^+ \cdot L_p^{\mathrm{an},+} \pmod{\omega_n}, & 2 \nmid n. \end{cases}$$

Proof
We argue for n odd; the other case is similar. We have

$$\theta_n = p^{(n+1)/2} G_{n+1}^+ = \omega_n^+ L_{p,n+1}^+,$$

where G_{n+1}^+ and $L_{p,n+1}^+$ are defined as in Lemma 5.9. So we need to verify that $L_p^{\mathrm{an},+} \equiv L_{p,n+1}^+ \pmod{T\omega_n^-}$. This amounts to checking that $L_p^{\mathrm{an},+}$ and $L_{p,n+1}^+$ agree at zero and at $\zeta_k - 1$ for odd $k \le n$. The two functions agree at zero since their constant terms are both the total measure of $\mathbf{Z}_p^\times$. Now for an odd $k \le n$, $G^+(\zeta_k - 1) = G_{n+1}^+(\zeta_k - 1)$ since the Riemann sum perfectly approximates the integral. Also, $\log_p^+(\zeta_k - 1) = p^{-(n+1)/2}\omega_n^+(\zeta_k - 1)$ from Lemma 4.7. Hence

$$L_p^{\mathrm{an},+}(E, \zeta_k - 1) = \frac{G^+(\zeta_k - 1)}{\log_p^+(\zeta_k - 1)} = p^{(n+1)/2}\frac{G_{n+1}^+(\zeta_k - 1)}{\omega_n^+(\zeta_k - 1)} = L_{p,n+1}^+(E, \zeta_k - 1),$$

which completes the proof. □

From this proposition we have

$$(\omega_n, \theta_n, \xi_n\theta_{n-1}) = (\omega_n, \omega_n^+ \cdot L_p^{\mathrm{an},+}, \omega_n^- \cdot L_p^{\mathrm{an},-}),$$

which in the case of Kurihara is simply the ideal (ω_n^+, ω_n^-) since $L_p^{\mathrm{an},+}$ and $L_p^{\mathrm{an},-}$ are units. Hence

$$Ш(E/\mathbf{Q}_n)_{p^\infty} \cong \Lambda/(\omega_n^+, \omega_n^-),$$

which is completely independent of the curve and depends only upon the fact that a_p is zero! Kurihara explains this phenomenon quite well in his proof of Theorem 6.17 by relating the Tate-Shafarevich group to the formal group of the elliptic curve which depends only upon the value of a_p.

We now conclude by stating a conjecture of Kurihara on the general structure of $\mathrm{Sel}(E/\mathbf{Q}_n)_{p^\infty}$ rewritten in terms of $L_p^{\mathrm{an},\pm}(E,T)$ via Proposition 6.18.

CONJECTURE 6.19 (Kurihara)
Let $E/\mathbf{Q}$ be an elliptic curve with p an odd prime such that $a_p = 0$ and $p \nmid \mathrm{Tam}(E/\mathbf{Q}_n)$. Then if $\Lambda_n = \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$, we have

$$\mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(E/\mathbf{Q}_n)^\wedge_{p^\infty}\right) = (\omega_n^+ \cdot L_p^{\mathrm{an},+}, \omega_n^- \cdot L_p^{\mathrm{an},-}),$$

where $X^\wedge = Hom(X, \mathbf{Q}_p/\mathbf{Z}_p)$ and $\mathrm{Fitt}_{\Lambda_n}(\cdot)$ is the Fitting ideal as a Λ_n-module.

7. Some data

In practice, the λ- and μ-invariants of $L_p^{\mathrm{an},\pm}$ are quite easy to compute for twists of curves with small conductor. We conclude with a table of the analytic invariants $\mu^\pm$, $\lambda_Ш^\pm$, and $\lambda_{MW}^\pm$ for $X_0(32)$ twisted by various quadratic characters with $p = 3$ (see Table 1). Specifically, we twist by characters with discriminant prime to 6 and of absolute value less than 200. These computations were done on W. Stein's modular cluster using the programming language MAGMA.

If the Iwasawa invariants of a twist are all zero, they are not included in the table. If the only nonzero data of a twist is $\lambda_{MW}^\pm = 1$, then this data is also not included in the table.

In the column labeled “roots” the general entry $(r : s)$ represents r roots of slope s. A small dot next to such an entry signifies that these are p-cyclotomic roots (i.e., of the form $\zeta_n - 1$). A root at zero that is forced by the functional equation is not included in the table.

Note that the conjectural arithmetic significance of these zeros (and their slopes) is given by the work of Kobayashi in [10].

Table 1. Twists of $32A$ with $p = 3$

D	r	$\lambda^{+}_{\text{Ш}}$	λ^{+}_{MW}	*roots*	$\lambda^{-}_{\text{Ш}}$	λ^{-}_{MW}	*roots*
13	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
37	1	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
41	2	2	2	$(2{:}\infty)^{\cdot}$ $(1{:}2)$ $(1{:}1)$	0	2	$(2{:}\infty)^{\cdot}$
53	1	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
61	1	1	1	-	2	1	$(2{:}\frac{1}{2})$
65	2	0	2	$(2{:}\infty)^{\cdot}$	0	2	$(2{:}\infty)^{\cdot}$
77	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
85	1	0	1	-	2	1	$(2{:}1)$
101	1	2	1	$(2{:}\frac{3}{2})$	0	1	-
133	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
137	2	0	2	$(2{:}\infty)^{\cdot}$	2	2	$(2{:}\infty)^{\cdot}$ $(2{:}\frac{1}{2})$
145	2	0	2	$(2{:}\infty)^{\cdot}$	0	2	$(2{:}\infty)^{\cdot}$
149	1	2	1	$(2{:}\frac{1}{2})$	12	1	$(12{:}\frac{1}{12})$
161	2	0	2	$(2{:}\infty)^{\cdot}$	0	2	$(2{:}\infty)^{\cdot}$
181	1	0	1	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
197	1	0	1	$(2{:}\frac{1}{2})^{\cdot}$	2	1	$(2{:}\frac{1}{2})$
-23	1	1	0	-	2	1	$(2{:}1)$
-43	0	8	0	$(2{:}\frac{1}{2})$ $(6{:}\frac{1}{6})$	2	0	$(2{:}1)$
-47	1	2	1	$(2{:}1)$	2	1	$(2{:}\frac{3}{2})$
-71	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
-103	1	0	1	-	6	1	$(6{:}\frac{1}{6})$
-107	0	2	0	$(2{:}1)$	6	0	$(2{:}\frac{1}{2})$ $(4{:}\frac{1}{4})$
-127	1	2	3	$(2{:}\frac{1}{2})^{\cdot}$ $(2{:}\frac{1}{2})$	4	1	$(4{:}\frac{1}{2})$
-131	0	2	0	$(2{:}1)$	2	0	$(2{:}1)$
-143	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
-163	0	2	0	$(2{:}1)$	2	0	$(2{:}1)$
-167	1	4	1	$(4{:}\frac{1}{4})$	2	1	$(2{:}\frac{1}{2})$
-191	1	2	1	$(2{:}1)$	0	1	-
-199	1	0	1	-	6	1	$(6{:}\frac{1}{6})$

Acknowledgments. We would like to thank Barry Mazur for suggesting the study of the zeros of p-adic L-functions in the supersingular case and for many stimulating conversations on the subject; Keith Conrad for a valuable suggestion that went into the construction of $\log_p^{\pm}(T)$; and Tom Weston and the anonymous referee for several corrections and improvements to an earlier draft of this paper.

References

[1] A. ABBES and E. ULLMO, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. **103** (1996), 269–286. MR 97f:11038 542

[2] Y. AMICE and J. VÉLU, "Distributions p-adiques associées aux séries de Hecke" in *Journées arithmétiques de Bordeaux (Bordeaux, 1974)*, Astérisque **24**–**25**, Soc. Math. France, Montrouge, 1975, 119–131. MR 51:12709 524, 527, 529

[3] D. BERNARDI and B. PERRIN-RIOU, *Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier)*, C. R. Acad. Sci. Paris Sér. I Math. **317** (1993), 227–232. MR 94k:11071 543

[4] C. BREUIL, B. CONRAD, F. DIAMOND, and R. TAYLOR, *On the modularity of elliptic curves over* **Q***: Wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939. MR 2002d:11058 541

[5] P. COLMEZ, *Théorie d'Iwasawa des représentations de de Rham d'un corps local*, Ann. of Math. (2) **148** (1998), 485–571. MR 2000f:11077 529

[6] J. E. CREMONA, *Algorithms for Modular Elliptic Curves*, 2d ed., Cambridge Univ. Press, Cambridge, 1997. MR 99e:11068

[7] R. GREENBERG, "Iwasawa theory for elliptic curves" in *Arithmetic Theory of Elliptic Curves (Cetraro, Italy, 1997)*, Lecture Notes in Math. **1716**, Springer, Berlin, 1999, 51–144. MR 2002a:11056 548

[8] R. GREENBERG and G. STEVENS, "On the conjecture of Mazur, Tate, and Teitelbaum" in *p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture (Boston, 1991)*, Contemp. Math. **165**, Amer. Math. Soc., Providence, 1994, 183–211. MR 95j:11057 529

[9] K. KATO, *p-adic Hodge theory and values of zeta functions of modular forms*, preprint, 2000. 547

[10] S. KOBAYASHI, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), 1–36. 526, 555

[11] M. KURIHARA, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction, I*, Invent. Math. **149** (2002), 195–224. CMP 1 914 621 523, 526, 551, 553

[12] M. LAZARD, *Les zéros des fonctions analytiques d'une variable sur un corps valué complet*, Inst. Hautes Études Sci. Publ. Math. **14** (1962), 47–75. MR 27:2497 533, 541

[13] JU. I. MANIN, *Cyclotomic fields and modular curves* (in Russian), Uspekhi Mat. Nauk **26**, no. 6 (1971), 7–71. MR 53:5480 552

[14] ———, *Parabolic points and zeta functions of modular curves* (in Russian), Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19 – 66. MR 47:3396 542

[15] ———, *Periods of cusp forms, and p-adic Hecke series* (in Russian), Mat. Sb. (N.S.) **92** (**134**) (1973), 378 – 401, 503. MR 49:10638

[16] B. MAZUR, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183 – 266. MR 56:3020

[17] ———, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129 – 162. MR 80h:14022 542

[18] B. MAZUR and P. SWINNERTON-DYER, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1 – 61. MR 50:7152 524

[19] 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. MR 87e:11076 524, 527, 530, 532

[20] A. G. NASYBULLIN, *p-adic L-series of supersingular elliptic curves* (in Russian), Funkcional. Anal. i Priložen. **8**, no. 1 (1974), 82 – 83. MR 52:411 526

[21] B. PERRIN-RIOU, *Théorie d'Iwasawa p-adique locale et globale*, Invent. Math. **99** (1990), 247 – 292. MR 91b:11116 525

[22] ———, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble) **43** (1993), 945 – 995. MR 95d:11081 526, 546, 547

[23] ———, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, preprint, 2001, http://math.uiuc.edu/Algebraic-Number-Theory/0306 523, 546, 547, 548, 551, 553

[24] D. E. ROHRLICH, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), 409 – 423. MR 86g:11038b 544

[25] K. RUBIN, "Euler systems and modular elliptic curves" in *Galois Representations in Arithmetic Algebraic Geometry (Durham, England, 1996)*, London Math. Soc. Lecture Note Ser. **254**, Cambridge Univ. Press, Cambridge, 1998, 351 – 367. MR 2001a:11106 550

[26] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. **106**, Springer, New York, 1992. MR 95m:11054

[27] M. M. VIŠIK, *Nonarchimedean measures associated with Dirichlet series* (in Russian), Mat. Sb. (N.S.) **99** (**141**), no. 2 (1976), 248 – 260, 296. MR 54:243 524, 527, 528, 529, 530

[28] M. M. VIŠIK and JU. I. MANIN, *p-adic Hecke series of imaginary quadratic fields* (in Russian), Mat. Sb. (N.S.) **95** (**137**) (1974), 357 – 383, 471. MR 51:8078

[29] A. WILES, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), 443 – 551. MR 96d:11071 541

Department of Mathematics, University of Chicago, 5734 South University Avenue, Chicago, Illinois 60637, USA; pollack@math.uchicago.edu