Algebra & Number Theory

Volume 11

2017

No. 4

On pairs of p-adic L-functions for weight-two modular forms

Florian Sprung

msp

ALGEBRA AND NUMBER THEORY 11:4 (2017)
dx.doi.org/10.2140/ant.2017.11.885

On pairs of p-adic L-functions for weight-two modular forms

Florian Sprung

Dedicated to Barry, Joe, and Rob

The point of this paper is to give an explicit p-adic analytic construction of two Iwasawa functions, $L_p^\sharp(f,T)$ and $L_p^\flat(f,T)$, for a weight-two modular form $\sum a_n q^n$ and a good prime p. This generalizes work of Pollack who worked in the supersingular case and also assumed $a_p = 0$. These Iwasawa functions work in tandem to shed some light on the Birch and Swinnerton-Dyer conjectures in the cyclotomic direction: we bound the rank and estimate the growth of the Šafarevič–Tate group in the cyclotomic direction analytically, encountering a new phenomenon for small slopes.

1. Introduction

Let $f = \sum a_n q^n$ be a weight-two modular form. The idea of attaching a p-adic L-function to f goes back to at least Mazur and Swinnerton-Dyer in the case where the associated abelian variety A_f is an elliptic curve. They analytically constructed a power series $L_\alpha(f,T)$, whose behavior at special values $\zeta_{p^n} - 1$, corresponding to finite layers $\mathbb{Q}_n$ of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$, should mirror that of the rational points $A_f(\mathbb{Q}_n)$ and the Šafarevič–Tate group $Ш(A_f/\mathbb{Q}_n)$ in view of the Birch and Swinnerton-Dyer conjectures. Identifying algebraic numbers with p-adic numbers via a fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$, we may give a_p a valuation v. Their crucial assumption was that p be good and $v = 0$ (p is *ordinary*), so that $L_\alpha(f,T)$ is an Iwasawa function, i.e., analytic on the closed unit disc. Since $L_\alpha(f,T)$ is nonzero by work of Rohrlich [1984], we can extract Iwasawa invariants, responsible for that behavior of $L_\alpha(f,T)$ which under the main conjecture corresponds to a

This material is based upon work supported by the National Science Foundation under agreement No. DMS-1128155. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

MSC2010: primary 11G40; secondary 11F67, 11R23.

Keywords: Birch and Swinnerton-Dyer, p-adic L-function, elliptic curve, modular form, Šafarevič–Tate group, Iwasawa Theory.

bound for $\operatorname{rank}(A_f(\mathbb{Q}_\infty))$ and a description of the size of $Ш(A_f/\mathbb{Q}_n)[p^\infty]$. Skinner and Urban [2014] settled the main conjecture in many cases.

The construction of $L_\alpha(f, T)$ has been generalized to the supersingular (i.e., $v > 0$) case as well [Amice and Vélu 1975; Višik 1976], in which there are two power series $L_\alpha(f, T)$ and $L_\beta(f, T)$. They are not Iwasawa functions, and thus not amenable for estimates for $\operatorname{rank}(A_f(\mathbb{Q}_\infty))$ or $Ш(A_f/\mathbb{Q}_n)$ directly. Nevertheless, the results of Rohrlich show that $L_\alpha(f, T)$ and $L_\beta(f, T)$ vanish at finitely many special values $\zeta_{p^n} - 1$, so that the analytic rank of $A_f(\mathbb{Q}_\infty)$ is bounded. His results are effective.[1]

The main theorem (Theorem 2.14) of Part I in this paper obtains a *pair* of appropriate Iwasawa functions in the general good reduction case so that p can be ordinary or supersingular. This pair is unique when p is supersingular, and generalize the results of Pollack in the $a_p = 0$ case. Note that the hypothesis $a_p = 0$ is very restrictive since the vast majority of supersingular modular abelian varieties have modular forms failing this condition. The philosophy of using *pairs* of objects has its origins in the work of Perrin-Riou [1990; 1993] in the supersingular case in which the pair consisting of $L_\alpha(f, T)$ and $L_\beta(f, T)$ is considered as one object as a power series with coefficients in the Dieudonné module. Our main theorem generalizes the construction of a pair of functions in the case of elliptic curves and supersingular primes [Sprung 2012] via Kato's zeta element. As pointed out in [Lei et al. 2010, Remark 5.26], the methods in [Sprung 2012] extend to the case $v \geqslant \frac{1}{2}$ as well. In this paper, we have completely isolated the analytic aspects of the theory and are thus able to treat the much harder case $v < \frac{1}{2}$. In the supersingular case, we prove a functional equation for this pair, which corrects a corresponding statement in [Pollack 2003] when reduced to the $a_p = 0$ case. Also, we give a quick proof that $L_\alpha(f, T)$ and $L_\beta(f, T)$ have finitely many common zeros, as conjectured by Greenberg.

Part 2 is dedicated to the estimates connected to the Birch and Swinnerton-Dyer conjectures. We bound the p-adic analytic rank of $A_f(\mathbb{Q}_\infty)$, which is the number of zeros of $L_\alpha(f^\sigma, T)$ at cyclotomic points $T = \zeta_{p^n} - 1$ summed over all Galois conjugates f^σ of f. This analytic rank does not depend on the choice of α in the supersingular case, as shown in Proposition 7.1. When p is ordinary, α is chosen to be a p-adic unit. This is hard even when f is ordinary, since f^σ may not be ordinary, i.e., we may have $v = 0$ but $v^\sigma > 0$, where v^σ is the valuation for a_p^σ for $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We overcome this difficulty by giving an upper bound in terms of the Iwasawa invariants of our pair of Iwasawa functions in the supersingular case. Apart from our Iwasawa-theoretic arguments, the key ingredient for this upper bound is to find any nonjump in the analytic rank in the cyclotomic tower, i.e.,

[1] In the elliptic curve case, $L_\alpha(\zeta_{p^n} - 1) \neq 0$ for $p^n > \max(10^{1000}N^{170}, 10^{120p}p^{7p}, 10^{6000}p^{420})$, where N is the conductor of $E = A_f$ [Rohrlich 1984, p. 416].

any n such that $L_\alpha(f, \zeta_{p^n} - 1) \neq 0$. Note that this is a much weaker corollary to Rohrlich's theorem (stating that almost all n give rise to nonjumps). This manifests itself in the fact that the first such n is typically very small. We also give another upper bound that assumes $a_p = 0$ (so that all f^σ are supersingular), and is due to Pollack under the further assumption $p \equiv 3 \pmod 4$, which our new proof removes. This upper bound is in most cases not as sharp as the more general one. Note that the upper bounds are also upper bounds for the corresponding algebraic objects (i.e., that rank of $A_f(\mathbb{Q}_\infty)$) in view of classical work of Perrin-Riou [1990, Lemme 6.10].

We then give growth formulas for the analytic size of $Ш(A_f/\mathbb{Q}_n)[p^\infty]$, unifying results of Mazur (who assumed $v^\sigma = 0$ for all σ) and Pollack (who assumed $v^\sigma = \infty$ for all σ, i.e., $a_p = 0$), and finishing this problem in most of the good reduction cases.[2] For example, we finish this problem when A_f is an elliptic curve, where there are infinitely many remaining cases all for which $p = 2$ or $p = 3$ in view of the Hasse bound. In Mazur's case, this formula was governed by $L_\alpha(f^\sigma, T)$, while in the $a_p = 0$ case, Pollack's Iwasawa functions alternated responsibility for the growth at even n and odd n. The reason we can cover the remaining cases is that our estimates result from both of our Iwasawa functions working *in tandem*, giving rise to several growth formula scenarios in these remaining cases, illustrating their difficulty even when A_f is an elliptic curve. In the ordinary case (and some special subcases of the supersingular case), one of the Iwasawa functions dominates, and only the invariants of that function are visible in the estimates. When $0 < v^\sigma < \frac{1}{2}$, we encounter a mysterious phenomenon: the estimates depend further on which one of (up to infinitely many) progressively smaller intervals v^σ lies in, and the roles of the Iwasawa functions generally alternate in adjacent intervals. We suspect the answer to the following question is very deep: *Where does this phenomenon come from and why does it occur?*

We now state our results more precisely. We work in the context of weight-two modular forms and a good (coprime to the level) prime p. The functions $L_\alpha(f, T)$ and $L_\beta(f, T)$ are named after the roots α and β of the Hecke polynomial $X^2 - a_p X + \epsilon(p)p$, ordered such that $\mathrm{ord}_p(\alpha) \leqslant \mathrm{ord}_p(\beta)$. In the supersingular case (i.e., when $v := \mathrm{ord}_p(a_p) > 0$), we can now trace the p-adic L-functions back to a pair of Iwasawa functions when $v = \infty$ (i.e., $a_p = 0$) thanks to the methods of Pollack [2003].

In Part I, we prove the following theorem.

Theorem 1.1. *Let $f = \sum a_n q^n$ be a modular form of weight two and p be a good prime. We let $\Lambda = \mathcal{O}[\![T]\!]$, where $\mathcal{O}$ is the ring of integers of the completion at a prime above p of $\mathbb{Q}((a_n)_{n\in\mathbb{N}}, \epsilon(\mathbb{Z}))$.*

[2] The remaining cases we term the *sporadic cases*, which shouldn't occur in nature: For $v^\sigma > 0$, we are in the sporadic case when the μ-invariants differ in a specific way and $v^\sigma = \frac{1}{2}p^{-k}$ for $k \in \mathbb{N}$ and the valuation of $\sigma(a_p)^2 - \epsilon(p)\Phi_p(\zeta_{p^{k+2}})$ is exactly $2v^\sigma(1 + p^{-1} - p^{-2})$ for n with a fixed parity with respect to k; see Definition 8.3.

(1) *When p is a supersingular prime*, *we have*

$$\big(L_\alpha(f,T),L_\beta(f,T)\big)=\big(L_p^\sharp(f,T),L_p^\flat(f,T)\big)\mathcal{L}og_{\alpha,\beta}(1+T),$$

for two power series $L_p^\sharp(f,T)$ and $L_p^\flat(f,T)$ which are elements of Λ, *and $\mathcal{L}og_{\alpha,\beta}(1+T)$ is an explicit 2×2 matrix of functions converging on the open unit disc.*

(2) *When p is ordinary*, *we can write*

$$L_\alpha(f,T)=L_p^\sharp(f,T)\log_\alpha^\sharp(1+T)+L_p^\flat(f,T)\log_\alpha^\flat(1+T),$$

for some nonunique Iwasawa functions $L_p^\sharp(f,T)$ and $L_p^\flat(f,T)$, *where $\log_\alpha^\sharp(T)$ and $\log_\alpha^\flat(T)$ are the entries in the first column of $\mathcal{L}og_{\alpha,\beta}(1+T)$. They are functions converging on the closed unit disc.*

In the supersingular case, our vector $(L_p^\sharp(f,T),L_p^\flat(f,T))$ is related to the vector $(L_\alpha(f,T),L_\beta(f,T))$ much like the completed Riemann zeta function is related to the original zeta function: since $L_\alpha(f,T)$ and $L_\beta(f,T)$ are not Iwasawa functions, they have infinitely many zeros in the open unit disk. The analogue of the Gamma factor is the matrix $\mathcal{L}og_{\alpha,\beta}(1+T)$. It removes zeros of linear combinations of $L_\alpha(f,T)$ and $L_\beta(f,T)$, producing the vector of Iwasawa functions with finitely many zeros. Its definition for odd p is

$$\mathcal{L}og_{\alpha,\beta}(1+T):=\lim_{n\to\infty}\mathcal{C}_1\cdots\mathcal{C}_nC^{-(n+2)}\begin{pmatrix}-1&-1\\ \beta&\alpha\end{pmatrix},$$

where

$$\mathcal{C}_i:=\begin{bmatrix}a_p&1\\ -\epsilon(p)\Phi_{p^i}(1+T)&0\end{bmatrix},\quad C:=\begin{bmatrix}a_p&1\\ -\epsilon(p)p&0\end{bmatrix},$$

and $\Phi_n(X)$ is the n-th cyclotomic polynomial.

As one immediate corollary of Theorem 1.1, we obtain that $L_\alpha(f,T)$ and $L_\beta(f,T)$ have finitely many common zeros, as conjectured by Greenberg [2001].

When $p=2$ and $a_2=0$, our construction of $\mathcal{L}og_{\alpha,\beta}(1+T)$ explains a seemingly artificial extra factor of $\frac{1}{2}$ in Pollack's [2003] corresponding half-logarithm. The theorem also shows that for $p=2$, the functions $L_2^\sharp(T)$ and $L_2^\flat(T)$ of [Sprung 2012] in $\Lambda\otimes\mathbb{Q}$ are in fact elements of Λ in the strong Weil case.

Our proof of Theorem 1.1 is completely p-adic analytic, generalizing the arguments of Pollack [2003] when $v=\infty$ (i.e., $a_p=0$). Recall that the methods in [Sprung 2012] extend to the case $v\geqslant\frac{1}{2}$ ([Lei et al. 2010, Remark 5.26]). However, the situation for the *remaining* (and more difficult) valuations when $v<\frac{1}{2}$ is more involved. This part forms the technical heart of the first half of the paper, in which one major new tool is Lemma 4.17, which gives an explicit expansion of the terms of $\mathcal{L}og_{\alpha,\beta}(1+T)$. We use *valuation matrices*, an idea introduced in [Sprung 2013], to scrutinize the growth properties of the functions in its columns: They grow like $L_\alpha(f, T)$ and $L_\beta(f, T)$ for $v \geqslant \frac{1}{2}$, and at most as fast as these functions when $v < \frac{1}{2}$, proving, e.g., that the entries in the first column are Iwasawa functions when $v = 0$.

We also construct a completed version $\widehat{\mathcal{L}og}_{\alpha,\beta}$ of $\mathcal{L}og_{\alpha,\beta}$, and similarly $\widehat{L}_p^\sharp$ and $\widehat{L}_p^\flat$, and then prove functional equations for these completed objects.

Theorem 1.2. *Let p be supersingular. Then under the change of variables*

$$(1+T) \mapsto (1+T)^{-1},$$

$\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ is invariant, and the vector $(\widehat{L}_p^\sharp(T), \widehat{L}_p^\flat(T))$ is invariant up to a root number of the form $-\epsilon(-1)(1+T)^{-\log_\gamma(N)}$. A similar statement holds for $p = 2$.

For a precise definition of the root number, we refer to Section 2.

We derive functional equations for $L_p^\sharp$ and $L_p^\flat$ in some cases as well, which correct a corresponding statement in [Pollack 2003] (where $a_p = 0$), which is off by a unit factor. The algebraic version of the functional equation by Kim [2008] when $a_p = 0$ is still correct, since it is given up to units.

Part II is concerned with applications involving the invariants of the Birch and Swinnerton-Dyer (BSD) conjectures in the cyclotomic direction:

- Choose a subset $\mathcal{G}_f$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\{f^\sigma\}_{\sigma\in\mathcal{G}_f}$ contains each Galois conjugate of f once. Each zero of $L_\alpha(f^\sigma, T)$ or $L_\beta(f^\sigma, T)$ at $T = \zeta_{p^n} - 1$ (counted with multiplicity) with $\sigma \in \mathcal{G}_f$ should, in view of BSD for number fields, contribute toward the jump in the ranks, $\mathrm{rank}(A_f(\mathbb{Q}_n)) - \mathrm{rank}(A_f(\mathbb{Q}_{n-1}))$, where $\mathbb{Q}_n$ is the n-th layer in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q} = \mathbb{Q}_0$. More specifically, the number of zeroes r_∞^{an} at all $T = \zeta_{p^n} - 1$ of all $L_\alpha(f^\sigma, T)$ is an analytic upper bound for $r_\infty = \lim_{n\to\infty} \mathrm{rank}\, A_f(\mathbb{Q}_n)$. Denote by $r_\infty^{\mathrm{an}}(f^\sigma)$ the σ-part of r_∞^{an}, i.e., the number of such zeros of $L_\alpha(f^\sigma, T)$, so that $r_\infty^{\mathrm{an}} = \sum_{\sigma\in\mathcal{G}_f} r_\infty^{\mathrm{an}}(f^\sigma)$. When f^σ is ordinary, $r_\infty^{\mathrm{an}}(f^\sigma)$ is bounded by the λ-invariant λ^σ of $L_\alpha(f^\sigma, T)$.

For the case in which f^σ is supersingular, $L_\alpha(f^\sigma, T)$ and $L_\beta(f^\sigma, T)$ are known to have finitely many zeroes of the form $\zeta_{p^n} - 1$, by a theorem of Rohrlich. By only assuming the much weaker corollary that $L_\alpha(f^\sigma, T)$ does not vanish at some $\zeta_{p^n} - 1$, we give an explicit upper bound:

Theorem 1.3. *Let $\lambda_\sharp$ and $\lambda_\flat$ be the λ-invariants of $L_p^\sharp(f^\sigma, T)$ and $L_p^\flat(f^\sigma, T)$. Put*

$$q_n^\sharp := \left\lfloor \frac{p^n}{p+1} \right\rfloor \text{ if } n \text{ is odd}, \quad \text{and} \quad q_n^\sharp := q_{n+1}^\sharp \text{ for even } n,$$

$$q_n^\flat := \left\lfloor \frac{p^n}{p+1} \right\rfloor \text{ if } n \text{ is even}, \quad \text{and} \quad q_n^\flat := q_{n+1}^\flat \text{ for odd } n,$$

$$\nu_\sharp := \text{largest odd integer } n \geqslant 1 \text{ such that } \lambda_\sharp \geqslant p^n - p^{n-1} - q_n^\sharp,$$

$$\nu_\flat := \text{largest even integer } n \geqslant 2 \text{ such that } \lambda_\flat \geqslant p^n - p^{n-1} - q_n^\flat,$$

$$\nu := \max(\nu_\sharp, \nu_\flat).$$

(1) *Assume $\mu_\sharp = \mu_\flat$. Then the σ-part $r_\infty^{\text{an}}(f^\sigma)$ of the cyclotomic analytic rank r_∞ for* $\lim_{n\to\infty} \operatorname{rank} A_f(\mathbb{Q}_n)$ *is bounded above by*

$$\min(q_\nu^\sharp + \lambda_\sharp, q_\nu^\flat + \lambda_\flat).$$

(2) *For the case $\mu_\sharp \neq \mu_\flat$, there is a similar bound of the form $q_\nu^* + \lambda_*$, where $* \in \{\sharp, \flat\}$. We refer the reader to Theorem 7.8 for a precise formulation.*

(3) *When $a_p = 0$, another analytic upper bound is given by $\lambda_\sharp + \lambda_\flat$.*

Let $\mathcal{G}_f^{\text{ord}} = \{\sigma \in \mathcal{G}_f : f^\sigma$ is ordinary$\}$ and $\mathcal{G}_f^{\text{ss}} = \{\sigma \in \mathcal{G}_f : f^\sigma$ is supersingular$\}$. When $\sigma \in \mathcal{G}_f^{\text{ss}}$, denote by $\lambda_\natural^\sigma$ the minimum of the bounds from Theorem 1.3.

Corollary 1.4. *For a prime of good reduction, r_∞^{an} is bounded above as follows:*

$$r_\infty^{\text{an}} \leqslant \sum_{\sigma\in\mathcal{G}_f^{\text{ord}}} \lambda^\sigma + \sum_{\sigma\in\mathcal{G}_f^{\text{ss}}} \lambda_\natural^\sigma.$$

The *Kurihara terms* $q_n^{\sharp/\flat}$ in Theorem 1.3 are p-power sums, e.g., when $\nu > 1$ and ν is odd, we have

$$q_\nu^\sharp = p^{\nu-1} - p^{\nu-2} + p^{\nu-3} - p^{\nu-4} + \cdots + p^2 - p.$$

The $\nu \in \mathbb{N}$ is chosen according to an explicit algorithm that measures the contribution of $\mathcal{L}og_{\alpha,\beta}(1+T)$ to the cyclotomic zeroes. For example, when $\mu_\sharp = \mu_\flat$ and $\lambda_\sharp < p-1$ and $\lambda_\flat < (p-1)^2$, we have $\nu = 0$, in which case $q_0^\sharp = q_0^\flat = 0$ and the bound is simply $\min(\lambda_\sharp, \lambda_\flat)$, which is very much in the spirit of the bound in the ordinary case.

The bound for the case $a_p = 0$, $\lambda_\sharp + \lambda_\flat$, is a generalization of work of Pollack [2003]. When p is odd, this bound is in most (computationally known) cases weaker than the above one, but there are cases in which it is stronger. It is interesting to ask for an *optimal bound*.

- For the leading term part, we know from the discussion above that $L_\alpha(f, T)$ and $L_\beta(f, T)$ don't vanish at $T = \zeta_{p^n} - 1$ for $n \gg 0$, so that these values should encode $\#(\text{Ш}(A_f/\mathbb{Q}_n)[p^\infty])/\#(\text{Ш}(A_f/\mathbb{Q}_{n-1})[p^\infty])$, i.e., the jumps in the p-primary parts of Ш at the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension.

In the ordinary case, a classical result of Mazur gives an estimate for

$$\#\text{Ш}^{\text{an}}(A_f/\mathbb{Q}_n) := \frac{L^{(r_n^{\text{an}'})}(A_f/\mathbb{Q}_n, 1)\#A_f^{\text{tor}}(\mathbb{Q}_n)\#\widehat{A}_f^{\text{tor}}(\mathbb{Q}_n)\sqrt{D(\mathbb{Q}_n)}}{(r_n^{\text{an}'})!\Omega_{A_f/\mathbb{Q}_n} R(A_f/\mathbb{Q}_n)\operatorname{Tam}(A_f/\mathbb{Q}_n)}.$$

His analytic estimate for $e_n := \operatorname{ord}_p(\#\text{Ш}^{\text{an}}(A_f/\mathbb{Q}_n))$ when f^σ are all ordinary says that for $n \gg 0$,

$$e_n - e_{n-1} = \sum_{\sigma\in\mathcal{G}_f} \mu^\sigma(p^n - p^{n-1}) + \lambda^\sigma - r_\infty^{\text{an}}(f^\sigma),$$

much in the spirit of Iwasawa's famous class number formula. Here, μ^σ and λ^σ are the Iwasawa invariants of $L_\alpha(f^\sigma, T)$. We prove a theorem that estimates e_n in the general good reduction case in terms of the Iwasawa invariants of $L_p^\sharp(f^\sigma, T)$ and $L_p^\flat(f^\sigma, T)$ and $v^\sigma = \operatorname{ord}_p(a_p^\sigma)$:

Given an integer n, we now define two generalized Kurihara terms $q_n^*(v^\sigma)$ for $* \in \{\sharp, \flat\}$ which are *continuous* in $v^\sigma \in [0, \infty]$. They are each a sum of a truncated Kurihara term and a multiple of $p^n - p^{n-1}$. For fixed n, they are piecewise linear in v.

Definition 1.5. For a real number $v > 0$, let $k \in \mathbb{Z}^{\geqslant 1}$ be the smallest positive integer such that $v \geqslant p^{-k}/2$.

$$q_n^\sharp(v) := \begin{cases} (p^n - p^{n-1})kv + \left\lfloor \dfrac{p^{n-k}}{p+1} \right\rfloor & \text{when } n \not\equiv k \bmod (2), \\ (p^n - p^{n-1})((k-1)v) + \left\lfloor \dfrac{p^{n+1-k}}{p+1} \right\rfloor & \text{when } n \equiv k \bmod (2), \end{cases}$$

$$q_n^\flat(v) := \begin{cases} (p^n - p^{n-1})((k-1)v) + p\left\lfloor \dfrac{p^{n-k}}{p+1} \right\rfloor + p - 1 & \text{when } n \not\equiv k \bmod (2), \\ (p^n - p^{n-1})kv + p\left\lfloor \dfrac{p^{n-1-k}}{p+1} \right\rfloor + p - 1 & \text{when } n \equiv k \bmod (2). \end{cases}$$

We also put

$$q_n^*(\infty) := \lim_{v \to \infty} q_n^*(v), \quad \text{and} \quad q_n^*(0) := \lim_{v \to 0} q_n^*(v) = \begin{cases} 0 & \text{when } * = \sharp, \\ p-1 & \text{when } * = \flat. \end{cases}$$

Definition 1.6 (modesty algorithm). Given $v \in [0, \infty]$, an integer n, integers $\lambda_\sharp$ and $\lambda_\flat$, and rational numbers $\mu_\sharp$ and $\mu_\flat$, choose $* \in \{\sharp, \flat\}$ via

$$* = \begin{cases} \sharp & \text{if } (p^n - p^{n-1})\mu_\sharp + \lambda_\sharp + q_n^\sharp(v) < (p^n - p^{n-1})\mu_\flat + \lambda_\flat + q_n^\flat(v), \\ \flat & \text{if } (p^n - p^{n-1})\mu_\flat + \lambda_\flat + q_n^\flat(v) < (p^n - p^{n-1})\mu_\sharp + \lambda_\sharp + q_n^\sharp(v). \end{cases}$$

Theorem 1.7. *Let $e_n := \operatorname{ord}_p(\#\text{Ш}^{\text{an}}(A_f/\mathbb{Q}_n))$. Then for $n \gg 0$, we have*

$$e_n - e_{n-1} = \sum_{\sigma \in \mathcal{G}_f} \big(\mu_*^\sigma (p^n - p^{n-1}) + \lambda_*^\sigma + q_n^*(v^\sigma) \big) - r_\infty^{\text{an}},$$

where:

(1) $* \in \{\sharp, \flat\}$ *is chosen according to the modesty algorithm* (Definition 1.6) *with the choice $v = v^\sigma$ when $v^\sigma \neq p^{-k}/2$. Note that one input of the algorithm is the parity of the integer k such that $v^\sigma \in \left[\frac{1}{2}p^{-k}, \frac{1}{2}p^{-k+1}\right)$.*

(2) *The term $q_n^*(v^\sigma)$ is replaced by a modified Kurihara term $q_n^*(v^\sigma, v_2^\sigma)$, when $v^\sigma = p^{-k}/2$, that depends further on the valuation v_2^σ of $(a_p^\sigma)^2 - \epsilon(p)\Phi_p(\zeta_{p^{k+2}})$ when $\mu_\sharp^\sigma \neq \mu_\flat^\sigma$. Further, $* \in \{\sharp, \flat\}$ is chosen according to a generalized modesty algorithm which also depends on v_2^σ. We refer the reader to* Theorem 8.5 *for a precise formulation.*

	$v=0$			$0<v<\infty$		$v=\infty$	
	$\lambda_\sharp<\lambda'_\flat$	$\lambda_\sharp>\lambda'_\flat$	$\lambda_\sharp=\lambda'_\flat$	n odd	n even	n odd	n even
$\mu_\sharp=\mu_\flat$	$\sharp$	$\flat$	excluded	$\sharp$	$\flat$	$\sharp$	$\flat$
$\mu_\sharp<\mu_\flat$	$\sharp$	$\sharp$	$\sharp$	$\sharp$	$\sharp$	$\sharp$	$\flat$
$\mu_\flat<\mu_\sharp$	$\flat$	$\flat$	$\flat$	$\flat$	$\flat$	$\sharp$	$\flat$

Table 1. Table for Corollary 1.9, with $\lambda'_\flat$ denoting $\lambda_\flat+p-1$.

Remark 1.8. The (generalized) modesty algorithm doesn't work for some excluded ("sporadic") cases. When $v^\sigma=0$, the excluded case is $\mu_\sharp^\sigma=\mu_\flat^\sigma$, and $\lambda_\sharp^\sigma=\lambda_\flat^\sigma+p-1$, which can be remedied by adhering to the ordinary theory; see Theorem 8.5. The other excluded cases occur when $v^\sigma=p^{-k}/2$ and $v_2^\sigma=p^{-k}(1+p^{-1}-p^{-2})$ and an inequality of μ-invariants (or λ-invariants) is satisfied. This case should conjecturally not occur. See Definition 8.3 for details.

In less precise terms, the theorem above states that *our formulas in the supersingular case approach Mazur's formula in the ordinary case as $k\to\infty$*, and that *during this approach, the roles of $\sharp$ and $\flat$ may switch as the parity of k does*. The simplest scenario is when the μ-invariants are equal. Here, a switch in the parity of k *always* causes a switch in the role of $\sharp$ and $\flat$. It is a mystery why these formulas appear in this way, but we invite the reader to ponder this phenomenon by looking at Figure 1.

In the supersingular case, Greenberg, Iovita, and Pollack (in unpublished work around 2005) generalized the approach of Perrin-Riou of extracting invariants $\mu_\pm$ and $\lambda_\pm$ from the classical p-adic L-functions for a modular form f, $L_p(f,\alpha,T)$ and $L_p(f,\beta,T)$, which they used for their estimates (under the assumption $\mu_+=\mu_-$). Our formulas match theirs exactly in those cases, although the techniques are different.

We write out explicitly the elliptic curve case of the above theorem for the convenience of the readers, and since it hints at a unification of the ordinary and supersingular theories:

Corollary 1.9. *Let E be an elliptic curve over $\mathbb{Q}$, p a prime of good reduction, $v=\operatorname{ord}_p(a_p)$ and $e_n:=\operatorname{ord}_p(\#\text{Ш}^{\text{an}}(E/\mathbb{Q}_n))$, and $\mu_{\sharp/\flat}$ and $\lambda_{\sharp/\flat}$ the Iwasawa invariants of $L_p^{\sharp/\flat}(E,T)$. Then for $n\gg 0$,*

$$e_n-e_{n-1}=\mu_*(p^n-p^{n-1})+\lambda_*-r_\infty^{\text{an}}+\min(1,v)q_n^*,$$

where the q_n^* are the Kurihara terms from Theorem 1.3 and $*\in\{\sharp,\flat\}$ is chosen according to Table 1.

In particular, there are *three* different possible formulas for the growth of the Šafarevič–Tate group when $a_p\neq 0$ and p is supersingular, one for each scenario of

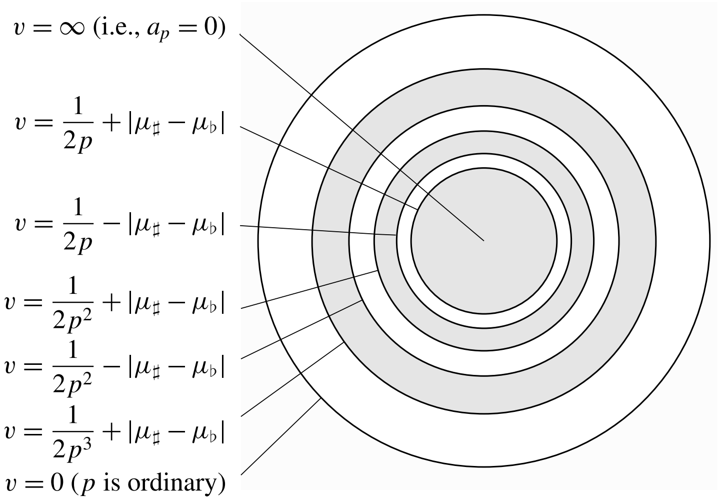
$v = \infty$ (i.e., $a_p = 0$)
$v = \frac{1}{2p} + |\mu_\sharp - \mu_\flat|$
$v = \frac{1}{2p} - |\mu_\sharp - \mu_\flat|$
$v = \frac{1}{2p^2} + |\mu_\sharp - \mu_\flat|$
$v = \frac{1}{2p^2} - |\mu_\sharp - \mu_\flat|$
$v = \frac{1}{2p^3} + |\mu_\sharp - \mu_\flat|$
$v = 0$ (p is ordinary)

Figure 1. The locus inside the p-adic unit disc in which the modesty algorithm chooses $\sharp$ or $\flat$ when $(p-1)/(4p^4) < |\mu_\sharp - \mu_\flat| < (p-1)/(4p^3)$. Here, $v = \operatorname{ord}_p(a_p)$ indicates the possible valuations of a_p inside the unit disc. At the center, we have $a_p = 0$, i.e., $v = \infty$. On the edge, we have $v = 0$, so that p is ordinary. In the central shaded region, the formula involves $\mu_\sharp$, $\lambda_\sharp$ for odd n and $\mu_\flat$, $\lambda_\flat$ for even n, while in the second shaded region, $\mu_\sharp$ and $\lambda_\sharp$ are part of the formula for even n, and $\mu_\flat$ and $\lambda_\flat$ for odd n. In the outermost shaded region, the roles are flipped yet again and the $\sharp$-invariants come into play for odd n, and the $\flat$-invariants for even n. When $\mu_\sharp < \mu_\flat$, the formulas are only controlled by the $\mu_\sharp$ and $\lambda_\sharp$ in the nonshaded regions.

comparing μ-invariants. As visible when $a_p \neq 0$, the Šafarevič–Tate group Ш tries to stay as small as possible (it is "modest") during its ascent along the cyclotomic $\mathbb{Z}_p$-extension by choosing smaller Iwasawa-invariants. The analytic estimates in the case $v = \infty$ (i.e., $a_p = 0$) were given by Pollack [2003], see also the many computations in [Stein and Wuthrich 2013].

Thanks to the work of Kurihara [2002], Perrin-Riou [2003], Kobayashi [2003], and the work in [Sprung 2013], we now understand the algebraic side of the corollary (i.e., the elliptic curve case) quite well in the supersingular case when p is odd.[3] The formulas also match the algebraic ones of Kurihara and Otsuki [2006] when $p = 2$. For the unknown cases (in which $p = 2$), the formulas thus serve as a prediction of how $Ш(E/\mathbb{Q}_n)[p^\infty]$ grows.

[3] These works answer a comment by Coates and Sujatha who wrote in their textbook [2000, p. 56] only 15 years ago that when looking at the p-primary part of $Ш(E/\mathbb{Q}_n)$ as $n \to \infty$, "...nothing seems to be known about the asymptotic behavior of the order ..."

Organization of Paper. This paper consists of two parts. Part I is mainly concerned with the construction of our pair of Iwasawa functions: In Section 2, we introduce *Mazur–Tate symbols*, which inherit special values of L-functions to construct the classical p-adic L-functions of Amice, Vélu, and Višik, and state the main theorem. In Section 3, we give a quick application, answering a question by Greenberg. In Section 4, we scrutinize the logarithm matrix $\mathcal{L}og_{\alpha,\beta}$ and prove its basic properties. In Section 5, we then put this information together to rewrite the p-adic L-functions from Section 2 in terms of the new p-adic L-functions $L_p^\sharp$ and $L_p^\flat$, proving the main theorem. Part II is devoted to the BSD-theoretic aspects as one climbs up the cyclotomic tower: in Section 6, we give the necessary preparation, Section 7 is concerned with the two upper bounds on the Mordell–Weil rank, and Section 8 scrutinizes the size of Ш.

Outlook. Pottharst [2012] constructs an algebraic counterpart (*Selmer modules*) to the pair $L_\alpha(f, T)$, $L_\beta(f, T)$ in the supersingular case, which hints at an algebraic counterpart to $\mathcal{L}og_{\alpha,\beta}(1+T)$ as well, along with algebraic versions of each of our analytic applications; these are equivalent under an Iwasawa main conjecture. A proof of the main conjecture in terms of $L_\alpha(f, T)$ in the ordinary case is due to Skinner and Urban [2014], building on [Kato 2004]. See also [Rubin 1991] for the CM case. The work of Lei, Loeffler, and Zerbes [Lei et al. 2010] constructs pairs of Iwasawa functions (in $\mathbb{Q} \otimes \Lambda$) out of Berger–Li–Zhu's basis [Berger et al. 2004] of *Wach modules*, see also [Loeffler and Zerbes 2013]. They match the Iwasawa functions in this paper when $a_p = 0$ (which shows that the functions in [Lei et al. 2010] actually live in Λ), which hints at an explicit relationship between our methods and theirs. For the higher weight case, there are generalizations of $L_p^\sharp(f, T)$ and $L_p^\flat(f, T)$, which is forthcoming work. Their invariants are already sometimes visible (see, e.g., [Pollack and Weston 2011]). It would be nice to generalize the pairs of p-adic BSD conjectures formulated in [Sprung 2015] to modular abelian varieties as well. For the ordinary case, the generalization of [Mazur et al. 1986] is [Balakrishnan et al. 2016]. Another challenge is formulating p-adic BSD for a bad prime. See [Colmez 2004] for an overview of p-adic BSD, mainly in the good reduction case. Apart from [Mazur et al. 1986], a hint for what to do can be found in Delbourgo's [1998] formulation of Iwasawa theory.

Part I. The pair of Iwasawa functions $L_p^\sharp$ and $L_p^\flat$

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

In this section, we recall the classical p-adic L-functions given in [Amice and Vélu 1975; Mazur et al. 1986; Višik 1976; Mazur and Swinnerton-Dyer 1974], in the case of weight-two modular forms. We give a construction via *queue sequences* which we scrutinize carefully enough to arrive at the decomposition of the classical p-adic L-functions as linear combinations of Iwasawa functions $L_p^\sharp$ and $L_p^\flat$. This is the main theorem of this paper, which will be proved in Sections 4 and 5, and upon which the applications (Sections 3, 6, and 7) depend.

Let f be a weight-two modular form with character ϵ which is an eigenform for the Hecke operators T_n with eigenvalue a_n. We also fix forever a good (i.e., coprime to the level) prime p. Given integers a, m, the *period* of f is

$$\varphi\Big(f, \frac{a}{m}\Big) := 2\pi i \int_{i\infty}^{a/m} f(z)\, dz.$$

The following theorem puts these transcendental periods into the algebraic realm (see also [Greenberg and Stevens 1994, Theorem 3.5.4]).

Theorem 2.1 [Manin 1973, Proposition 9.2c]. *There is a finite extension $K(f)$ of $\mathbb{Q}$ with integer ring $\mathcal{O}(f)$ and nonzero complex numbers $\Omega_f^\pm$ such that the following are in $\mathcal{O}(f)$ for all $a, m \in \mathbb{Z}$:*

$$\left[\frac{a}{m}\right]_f^+ := \frac{\varphi(f, a/m) + \varphi(f, -a/m)}{2\Omega_f^+} \quad \text{and} \quad \left[\frac{a}{m}\right]_f^- := \frac{\varphi(f, a/m) - \varphi(f, -a/m)}{2\Omega_f^-}.$$

Convention 2.2 (for Part II). We choose the convention that $\prod_{f^\sigma} \Omega_{f^\sigma}^\pm = \Omega_{A_f}^\pm$, where the f^σ run over all Galois conjugates of f (see, e.g., [Balakrishnan et al. 2016, (2.4)]), and $\Omega_{A_f}^\pm$ are the Neron periods as in [Manin 1971, §8.10]. We also use the convention that any period Ω with an omitted sign denotes Ω^+.

The $[a/m]_f^\pm$ are called *modular symbols*. For p-adic considerations, we fix an embedding $\overline{\mathbb{Q}} \to \mathbb{C}_p$ of an algebraic closure of $\mathbb{Q}$ inside the completion of an algebraic closure of $\mathbb{Q}_p$. This all allows us to construct p-adic L-functions as follows: Denote by $\mathbb{C}^0(\mathbb{Z}_p^\times)$ the $\mathbb{C}_p$-valued step functions on $\mathbb{Z}_p^\times$. Let a be an integer prime to p, and denote by $\mathbf{1}_U$ the characteristic function of an open set U. We let ord_p be the valuation associated to p so that $\operatorname{ord}_p(p) = 1$. Let α be a root of the Hecke polynomial $X^2 - a_p X + \epsilon(p)p$ of f so that $\operatorname{ord}_p(\alpha) < 1$, and denote the conjugate root by β. Without loss of generality, we assume throughout this paper that $\operatorname{ord}_p(\alpha) \leqslant \operatorname{ord}_p(\beta)$. We define a linear map $\mu_{f,\alpha}^\pm$ from $\mathbb{C}^0(\mathbb{Z}_p^\times)$ to $\mathbb{C}_p$ by setting

$$\mu_{f,\alpha}^\pm(\mathbf{1}_{a+p^n\mathbb{Z}_p}) = \frac{1}{\alpha^{n+1}} \left(\left[\frac{a}{p^n}\right]_f^\pm, \left[\frac{a}{p^{n-1}}\right]_f^\pm \right) \begin{pmatrix} \alpha \\ -\epsilon(p) \end{pmatrix}.$$

Remark 2.3. The maps $\mu_{f,\alpha}^\pm$ are not measures, but $\operatorname{ord}_p(\alpha)$-admissible measures. See, e.g., [Pollack 2003]. For background on measures, see [Washington 1982, Section 12.2].

Theorem 2.4. *We can extend the maps $\mu_{f,\alpha}^\pm$ to all analytic functions on $\mathbb{Z}_p^\times$.*

This can be done by locally approximating analytic functions by *step functions*, since $\mu_{f,\alpha}^{\pm}$ are $\operatorname{ord}_p(\alpha)$-admissible measures. That is, we look at their Taylor series expansions and ignore the higher order terms. For an explicit construction, see [Amice and Vélu 1975] or [Višik 1976]. Since characters χ of $\mathbb{Z}_p^\times$ are locally analytic functions, we thus obtain an element

$$L_p(f,\alpha,\chi) := \mu_{f,\alpha}^{\operatorname{sign}(\chi)}(\chi).$$

Now since $\mathbb{Z}_p^\times \cong (\mathbb{Z}/2p\mathbb{Z})^\times \times (1+2p\mathbb{Z}_p)$, we can write a character χ on $\mathbb{Z}_p^\times$ as a product

$$\chi = \omega^i \chi_u,$$

with $0 \leqslant i < |\Delta|$ for some $u \in \mathbb{C}_p$ with $|u-1|_p < 1$, where χ_u sends the topological generator $\gamma = 1+2p$ of $1+2p\mathbb{Z}_p$ to u, and where $\omega : \Delta \to \mathbb{Z}_p^\times \in \mathbb{C}_p$ is the usual embedding of the $|\Delta|$-th roots of unity in $\mathbb{Z}_p$ so that ω^i is a tame character of $\Delta = (\mathbb{Z}/2p\mathbb{Z})^\times$. Using this product, we can identify the open unit disc of $\mathbb{C}_p$ with characters χ on $\mathbb{Z}_p^\times$ having the same tame character ω^i. Thus if we fix i, we can regard $L_p(f,\alpha,\omega^i\chi_u)$ as a function on the open unit disc. We can go even further:

Theorem 2.5 [Višik 1976; Mazur et al. 1986; Amice and Vélu 1975; Pollack 2003]. *Fix a tame character $\omega^i : \Delta = (\mathbb{Z}/2p\mathbb{Z})^\times \to \mathbb{C}_p$. Then the function $L_p(f,\alpha,\omega^i\chi_u)$ is an analytic function converging on the open unit disc.*

We can thus form its power series expansion about $u = 1$. For convenience, we change variables by setting $T = u-1$ and denote $L_p(f,\alpha,\omega^i\chi_u)$ by $L_p(f,\alpha,\omega^i,T)$.

Denote by $\zeta = \zeta_{p^n}$ a primitive p^n-th root of unity. We can then regard $\omega^i\chi_\zeta$ as a character of $(\mathbb{Z}/p^N\mathbb{Z})^\times$, where $N = n+1$ if p is odd and $N = n+2$ if $p = 2$. Given any character ψ of $(\mathbb{Z}/p^N\mathbb{Z})^\times$, let $\tau(\psi)$ be the Gauß sum $\sum_{a\in(\mathbb{Z}/p^N\mathbb{Z})^\times}\psi(a)\zeta_{p^N}^a$.

Theorem 2.6 [Amice and Vélu 1975; Višik 1976]. *The above $L_p(f,\alpha,\omega^i,T)$ interpolate as follows*:

$$\begin{aligned} L_p(f,\alpha,\omega^i,\zeta-1) &= \frac{p^N}{\alpha^N\tau(\omega^{-i}\chi_{\zeta^{-1}})}\frac{L(f_{\omega^{-i}\chi_{\zeta^{-1}}},1)}{\Omega_f^{\omega^i(-1)}} \quad \textit{if } i \neq 0 \textit{ and } \zeta-1 \neq 0, \\ L_p(f,\alpha,\omega^0,0) &= \left(1-\frac{1}{\alpha}\right)^2\frac{L(f,1)}{\Omega_f^+}. \end{aligned} \tag{1}$$

Queue sequences and Mazur–Tate elements. Denote by μ_{p^n} the group of p^n-th roots of unity, and put $\mathcal{G}_N := \operatorname{Gal}(\mathbb{Q}(\mu_{p^N}))$. We let $\mathbb{Q}_n$ be the unique subextension of $\mathbb{Q}(\mu_{p^N})$ with Galois group isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$ and put $\Gamma_n := \operatorname{Gal}(\mathbb{Q}_n/\mathbb{Q})$. We also let $\Gamma := \operatorname{Gal}\big(\bigcup_n \mathbb{Q}_n/\mathbb{Q}\big)$. We then have an isomorphism

$$\mathcal{G}_N \cong \Delta \times \Gamma_n.$$

We let $K := K(f)_v$ be the completion of $K(f)$ from Theorem 2.1 by the prime v of $K(f)$ over p determined by $\operatorname{ord}_p(\cdot)$ and denote by $\mathcal{O}$ the ring of integers of K. Let $\Lambda_n = \mathcal{O}[\Gamma_n]$ be the finite version of the Iwasawa algebra at level n. We need two maps $\nu = \nu_{n-1/n}$ and $\pi = \pi_{n/n-1}$ to construct queue sequences: π is the natural projection from Λ_n to Λ_{n-1}, and the map $\Lambda_{n-1} \xrightarrow{\nu_{n-1/n}} \Lambda_n$ we define by

$$\nu_{n-1/n}(\sigma) = \sum_{\tau \mapsto \sigma, \tau \in \Gamma_n} \tau.$$

We let $\Lambda = \mathcal{O}[\![\Gamma]\!] = \varprojlim_{\pi_{n/n-1}} \mathcal{O}[\Gamma_n]$ be the Iwasawa algebra. We identify Λ with $\mathcal{O}[\![T]\!]$ by sending our topological generator $\gamma = 1 + 2p$ of $\Gamma \cong \mathbb{Z}_p$ to $1 + T$. This induces an isomorphism between Λ_n and $\mathcal{O}[\![T]\!]/((1+T)^{p^n} - 1)$.

Definition 2.7. A *queue sequence* is a sequence of elements $(\Theta_n)_n \in (\Lambda_n)_n$ such that

$$\pi\Theta_n = a_p\Theta_{n-1} - \epsilon(p)\nu\Theta_{n-2} \quad \text{when } n \geqslant 2.$$

Definition 2.8. For $a \in \mathcal{G}_N$, denote its projection onto Δ by $\bar{a}$, and let $i : \Delta \hookrightarrow \mathcal{G}_N$ be the standard inclusion, so that $a/i(\bar{a}) \in \Gamma_n$. Define $\log_\gamma(a)$ to be the smallest positive integer such that the image of $\gamma^{\log_\gamma(a)}$ under the projection from Γ to Γ_n equals $a/i(\bar{a})$. We then have a natural map $i : \Delta \hookrightarrow \mathcal{G}_\infty$ which allows us to extend this definition to any $a \in \mathcal{G}_\infty = \varprojlim_N \mathcal{G}_N$: let $\log_\gamma(a)$ be the unique element of $\mathbb{Z}_p^\times$ such that $\gamma^{\log_\gamma(a)} = a/i(\bar{a})$.

Example 2.9. We make the identification $\mathcal{G}_N \cong (\mathbb{Z}/p^N\mathbb{Z})^\times$ by identifying σ_a with a, where $\sigma_a(\zeta) = \zeta^a$ for $\zeta \in \mu_{p^N}$. This allows us to construct the *Mazur–Tate element*, which is

$$\vartheta_N^\pm := \sum_{a \in (\mathbb{Z}/p^N)^\times} \left[\frac{a}{p^N}\right]_f^\pm \sigma_a \in \mathcal{O}[\mathcal{G}_N].$$

For each character $\omega^i : \Delta \to \mathbb{C}_p^\times$, put

$$\varepsilon_{\omega^i} = \frac{1}{\#\Delta} \sum_{\tau \in \Delta} \omega^i(\tau)\tau^{-1}.$$

We can take isotypical components $\varepsilon_{\omega^i}\vartheta_N$ of the Mazur–Tate elements, which can be regarded as elements of $\Lambda_n \cong \mathcal{O}[\![T]\!]/((1+T)^{p^n} - 1)$. Denote these *Mazur–Tate elements associated to the tame character* ω^i by

$$\theta_n(\omega^i, T) := \varepsilon_{\omega^i}\vartheta_N^{\operatorname{sign}(\omega^i)}.$$

We extend ω^i to all of $(\mathbb{Z}/p^N\mathbb{Z})^\times$ by precomposing with the natural projection onto Δ, and can thus write these elements explicitly as elements of Λ_n:

$$\theta_n(\omega^i, T) = \sum_{a \in (\mathbb{Z}/p^N\mathbb{Z})^\times} \left[\frac{a}{p^N}\right]_f^{\operatorname{sign}(\omega^i)} \omega^i(a)(1+T)^{\log_\gamma(a)}.$$

When $\omega^i = \mathbf{1}$ is the trivial character, we simply write $\theta_n(T)$ instead of $\theta_n(\mathbf{1}, T)$. For a fixed tame character ω^i, the associated Mazur–Tate elements $\theta_n(\omega^i, T)$ form a queue sequence. For a proof, see [Mazur et al. 1986, (4.2)].

We can now explicitly approximate $L_p(f, \alpha, \omega^i, T)$ by Riemann sums:

Definition 2.10. Put

$$L^{\pm}_{N,\alpha} := \sum_{a\in(\mathbb{Z}/p^N\mathbb{Z})^\times} \mu^{\pm}_{f,\alpha}(\mathbf{1}_{a+p^N\mathbb{Z}_p})\sigma_a \in \mathbb{C}_p[\mathcal{G}_N],$$

so we get the representation

$$\varepsilon_{\omega^i} L^{\mathrm{sign}(\omega^i)}_{N,\alpha}(T) = \sum_{a\in(\mathbb{Z}/p^N\mathbb{Z})^\times} \mu^{\mathrm{sign}(\omega^i)}_{f,\alpha}(\mathbf{1}_{a+p^n\mathbb{Z}_p})\omega^i(a)(1+T)^{\log_\gamma(a)}.$$

Note that the homomorphism $\nu : \Gamma_{n-1} \to \Gamma_n$ extends naturally to a homomorphism from $\mathcal{G}_{N-1}$ to $\mathcal{G}_N$, also denoted by ν.

Lemma 2.11. *Let $n \geqslant 0$, i.e., $N \geqslant 1$ for odd p, and $N \geqslant 2$ for $p = 2$. Then*

$$(L^{\pm}_{N,\alpha}, L^{\pm}_{N,\beta}) = (\vartheta^{\pm}_N, \nu\vartheta^{\pm}_{N-1}) \begin{pmatrix} \alpha^{-N} & \beta^{-N} \\ -\epsilon(p)\alpha^{-(N+1)} & -\epsilon(p)\beta^{-(N+1)} \end{pmatrix}.$$

Proof. This follows from the definitions. □

Proposition 2.12. *As functions converging on the open unit disc, we have*

$$L_p(f, \alpha, \omega^i, T) = \lim_{n\to\infty} \varepsilon_{\omega^i} L^{\mathrm{sign}(\omega^i)}_{N,\alpha}(T).$$

Proof. Approximation by Riemann sums, and decomposition into tame characters. □

Corollary 2.13. *Let p be supersingular. Then both α and β have valuation strictly less than one, so we can reconstruct the p-adic L-functions by the Mazur–Tate elements:*

$$\begin{aligned}&\big(L_p(f, \alpha, \omega^i, T), L_p(f, \beta, \omega^i, T)\big) \\ &\qquad = \lim_{n\to\infty} \big(\theta_n(\omega^i, T), \nu\theta_{n-1}(\omega^i, T)\big) \begin{pmatrix} \alpha^{-N} & \beta^{-N} \\ -\epsilon(p)\alpha^{-(N+1)} & -\epsilon(p)\beta^{-(N+1)} \end{pmatrix}.\end{aligned}$$

In the ordinary case, we have $\mathrm{ord}_p(\alpha) = 0 < 1$, *so*

$$L_p(f, \alpha, \omega^i, T) = \lim_{n\to\infty} \big(\theta_n(\omega^i, T), \nu\theta_{n-1}(\omega^i, T)\big) \begin{pmatrix} \alpha^{-N} \\ -\epsilon(p)\alpha^{-(N+1)} \end{pmatrix}.$$

Proof. This follows from Lemma 2.11. □

In Section 4, we define an explicit 2×2 matrix

$$\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T) = \begin{pmatrix} \widehat{\log}^{\sharp}_{\alpha}(1+T) & \widehat{\log}^{\sharp}_{\beta}(1+T) \\ \widehat{\log}^{\flat}_{\alpha}(1+T) & \widehat{\log}^{\flat}_{\beta}(1+T) \end{pmatrix}$$

that encodes convenient behavior of the Mazur–Tate elements. We prove that the entries are functions convergent on the open unit disc when p is supersingular, and that $\widehat{\log}^{\sharp}_{\alpha}(1+T)$ and $\widehat{\log}^{\flat}_{\alpha}(1+T)$ converge on the closed unit disc in the ordinary case. This assertion is the main lemma (Lemma 4.4). A corollary of the construction, Remark 4.5, says that the determinant of $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ converges and vanishes precisely at $\zeta_{p^n} = 1$ for $n \geqslant 0$. Lemma 4.4 is the key ingredient to proving our main theorem:

Theorem 2.14. *Fix a tame character ω^i.*

(a) *When p is supersingular, there is a unique vector of two Iwasawa functions*

$$\widehat{\overrightarrow{L}}_p(f,\omega^i,T) = \big(\widehat{L}^{\sharp}_p(f,\omega^i,T), \widehat{L}^{\flat}_p(f,\omega^i,T)\big) \in \Lambda^{\oplus 2}$$

such that

$$\big(L_p(f,\alpha,\omega^i,T), L_p(f,\beta,\omega^i,T)\big) = \big(\widehat{L}^{\sharp}_p(f,\omega^i,T), \widehat{L}^{\flat}_p(f,\omega^i,T)\big)\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T).$$

(b) *When p is ordinary, there is vector*

$$\widehat{\overrightarrow{L}}_p(f,\omega^i,T) = \big(\widehat{L}^{\sharp}_p(f,\omega^i,T), \widehat{L}^{\flat}_p(f,\omega^i,T)\big) \in \Lambda^{\oplus 2}$$

such that

$$\widehat{\overrightarrow{L}}_p(f,\omega^i,T)\begin{pmatrix} \widehat{\log}^{\sharp}_{\alpha}(1+T) \\ \widehat{\log}^{\flat}_{\alpha}(1+T) \end{pmatrix} = L_p(f,\alpha,\omega^i,T)$$

and

$$\widehat{\overrightarrow{L}}_p(f,\omega^i,0)\begin{pmatrix} \widehat{\log}^{\sharp}_{\beta}(1) \\ \widehat{\log}^{\flat}_{\beta}(1) \end{pmatrix} \text{ is given by (1) with } \zeta = 1 \text{ and } \alpha \text{ replaced by } \beta.$$

Once $\widehat{\overrightarrow{L}}_p(f,\omega^i,T)$ is fixed, all (other) such vectors are given by

$$\widehat{\overrightarrow{L}}_p(f,\omega^i,T) + g(T)T\big(-\widehat{\log}^{\flat}_{\alpha}(1+T), \widehat{\log}^{\sharp}_{\alpha}(1+T)\big)$$

for $g(T) \in \Lambda$. In particular, the value of $\widehat{\overrightarrow{L}}_p(f,\omega^i,0)$ is uniquely determined.

Statements analogous to parts (a) *and* (b) *also hold for objects without the hats.*

3. A question by Greenberg

To motivate our theorem, we give a quick application. Greenberg [2001] conjectured that $L_p(f,\alpha,\omega^i,T)$ and $L_p(f,\beta,\omega^i,T)$ have finitely many common zeros (in the elliptic curve case) when p is supersingular and $i=0$. In this section, we work in the general supersingular case.

Theorem 3.1 [Rohrlich 1984]. *$L_p(f,\alpha,\omega^i,T)$ and $L_p(f,\beta,\omega^i,T)$ vanish at only finitely many $T=\zeta_{p^n}-1$.*

Proof. Since these functions interpolate well (Theorem 2.6), the result follows from the original theorem of Rohrlich [1984], which guarantees that $L(f,\chi,1)=0$ at finitely many characters of p-power order. □

Theorem 3.2. *$L_p(f,\alpha,\omega^i,T)$ and $L_p(f,\beta,\omega^i,T)$ have finitely many common zeros. In particular, Greenberg's conjecture is true.*

Proof. When a zero is not a p-power root of unity minus 1, it is one of the finitely many zeros of $L_p^\sharp(f,\omega^i,T)$ and $L_p^\flat(f,\omega^i,T)$, since $\det\mathcal{L}og_{\alpha,\beta}(1+T)$ doesn't vanish there. For the other zeros, use Rohrlich's theorem. □

Remark 3.3. Pollack already found a different proof in the case $a_p=0$ ([Pollack 2003, Corollary 5.12]).

4. The logarithm matrix $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$

Definition of the matrix $\mathcal{L}og_{\alpha,\beta}(1+T)$ and convergence of entries. In this section, we construct a matrix $\mathcal{L}og_{\alpha,\beta}(1+T)$ whose entries are functions converging on the open unit disc in the supersingular case. In the ordinary case, its first column converges on the closed unit disc. They directly generalize the four functions $\log_{\alpha/\beta}^{\sharp/\flat}$ from [Sprung 2012] and the three functions $\log_p^+$, $\log_p^-\cdot\alpha$, $\log_p^-\cdot\beta$ from [Pollack 2003], all of which concern the supersingular case. We also construct a completed version $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$.

Definition 4.1. Let $i\geqslant 1$. We *complete* the p^i-th cyclotomic polynomial by putting

$$\widehat{\Phi}_{p^i}(1+T):=\Phi_{p^i}(1+T)/(1+T)^{\frac{1}{2}p^{i-1}(p-1)},$$

except when $p=2$ and $i=1$: to avoid branch cuts (square roots), we set

$$\widehat{\Phi}_2(1+T):=\Phi_2(1+T).$$

Definition 4.2. Define the following matrices:

$$\mathcal{C}_i:=\mathcal{C}_i(1+T):=\begin{pmatrix} a_p & 1\\ -\epsilon(p)\Phi_{p^i}(1+T) & 0\end{pmatrix},\quad \text{and}\quad C:=\mathcal{C}_i(1)=\begin{pmatrix} a_p & 1\\ -\epsilon(p)p & 0\end{pmatrix}.$$

Definition 4.3. Recall that ord_p is the valuation on $\mathbb{C}_p$ normalized by $\mathrm{ord}_p(p) = 1$. Put

$$v = \mathrm{ord}_p(a_p) \quad \text{and} \quad w = \mathrm{ord}_p(\alpha).$$

Lemma 4.4 (main lemma). *Recall that $N = n + 1$ if p is odd, and $N = n + 2$ if $p = 2$. We put*

$$\mathcal{L}og_{\alpha,\beta}(1 + T) := \lim_{n\to\infty} \mathcal{C}_1 \cdots \mathcal{C}_n C^{-(N+1)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}.$$

Then the entries in the left column of $\mathcal{L}og_{\alpha,\beta}(1 + T)$ and $\widehat{\mathcal{L}og}_{\alpha,\beta}(1 + T)$ are well-defined as power series and converge on the open unit disc. When $v > 0$ (the supersingular case) or $T = \zeta_{p^n} - 1$ with $n \geqslant 0$, we can say the same about all entries.

Remark 4.5. We call $\mathcal{L}og_{\alpha,\beta}(1 + T)$ the logarithm matrix. The reason for this name is that for odd p, we have

$$\det \mathcal{L}og_{\alpha,\beta}(1 + T) = \frac{\log_p(1 + T)}{T} \times \frac{\beta - \alpha}{(\epsilon(p)p)^2}.$$

For $p = 2$, the above exponent of 2 has to be replaced by a 3.

Remark 4.6. After this paper was written, Antonio Lei found a more streamlined proof of Lemma 4.4. This can be found in the proof of [Lei 2014, Theorem 1.5], which relies on techniques of Perrin-Riou [1994, §1.2.1]. The methods below uses the technique of valuation matrices developed below instead of those in [Perrin-Riou 1994, §1.2.1].

Convention 4.7. Whenever we encounter an expression $\mathcal{E}$ involving $\Phi_{p^i}(1 + T)$, we let $\widehat{\mathcal{E}}$ be the corresponding expression involving $\widehat{\Phi}_{p^i}(1+T)$. For example, we let $\widehat{\mathcal{C}}_i$ be $\mathcal{C}_i$ with $-\epsilon(p)\widehat{\Phi}_{p^i}(1+T)$ in the lower left entry instead of $-\epsilon(p)\Phi_{p^i}(1+T)$, and

$$\widehat{\mathcal{L}og}_{\alpha,\beta}(1 + T) = \lim_{n\to\infty} \widehat{\mathcal{C}}_1 \cdots \widehat{\mathcal{C}}_n C^{-(N+1)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}.$$

Observation 4.8. For $i > n \geqslant 0$, we have

$$\widehat{\mathcal{C}}_i(T + 1)|_{T=\zeta_{p^n}-1} = \widehat{\mathcal{C}}_i(\zeta_{p^n}) = \mathcal{C}_i(\zeta_{p^n}) = C.$$

Definition 4.9. For a matrix $M = (m_{i,j})_{i,j}$ with entries $m_{i,j}$ in the domain of a valuation val, let the *valuation matrix* $[M]$ *of* M be the matrix consisting of the valuations of the entries:

$$[M] := [\mathrm{val}(m_{i,j})]_{i,j}.$$

Let $N = (n_{j,k})_{j,k}$ be another matrix so that we can form the product MN. Valuation matrices have the following *valuative multiplication* operation:

$$[M][N] := \big[\min_j (m_{i,j} + n_{j,k})\big]_{i,k}.$$

We also define the *valuation* $\operatorname{val}(M)$ *of* M to be the minimum of the entries in the valuation matrix:

$$\operatorname{val}(M) := \min\{\operatorname{val}(m_{i,j})\}.$$

Definition 4.10. Let $0 < r < 1$. Denote by $|\cdot|_p = p^{-\operatorname{ord}_p(\cdot)}$ the p-adic absolute value. For $f(T) \in \mathbb{C}_p[\![T]\!]$ convergent on the open unit disc, we define its *valuation at* r to be

$$v_r(f(T)) := \inf_{|z|_p < r} \operatorname{ord}_p(f(z)).$$

We define the *valuation at* 0 to be

$$v_0(f(T)) := \operatorname{ord}_p(f(0)).$$

Lemma 4.11. *Let* val *be a valuation, and* M *and* N *be matrices as above allowing a matrix product* MN. *Then* $\operatorname{val}(MN) \geqslant \operatorname{val}(M) + \operatorname{val}(N)$.

Proof. Term by term, the valuations of the entries of $[MN]$ are at least as big as those of $[M][N]$. □

Notation 4.12. Let M be a matrix whose coefficients are in $\mathbb{C}_p[\![T]\!]$. With respect to v_r we may then define the *valuation matrix of* M *at* r and denote it by $[M]_r$. We similarly define the *valuation of* M *at* r and denote it by $v_r(M)$. When these terms don't depend on r (e.g., when the entries of M are constants), we drop the subscript r.

Example 4.13.[4] Denote the logarithm with base p by $\log_{(p)}$ to distinguish it from the p-adic logarithm $\log_p$ of Iwasawa.

$$v_r(\Phi_{p^n}(1+T)) = \begin{cases} 1 & \text{when } r \leqslant p^{-(p^{n-1}(p-1))^{-1}}, \\ -\log_{(p)}(r)p^{n-1}(p-1) & \text{when } r \geqslant p^{-(p^{n-1}(p-1))^{-1}}. \end{cases}$$

Example 4.14. $v_r\big((1+T)^{\frac{1}{2}p^{n-1}(p-1)}\big) = \frac{1}{2}p^{n-1}(p-1)v_r(1+T) = 0.$

In what follows, we give the arguments needed for our main lemma (Lemma 4.4) for $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$. From Example 4.14, the proof for $\mathcal{L}og_{\alpha,\beta}(1+T)$ follows by taking the hat off the relevant expressions.

[4] This essentially appears in [Pollack 2003, lemma 4.5]. It seems that he meant to write $p^{-v_r(\Phi_n(1+T))} \sim r^{p^{n-1}(p-1)}$ in the proof.

Definition 4.15. Assume $\beta \neq \alpha$. We put $\rho := \alpha/\beta$ and let

$$\widehat{\Upsilon}_n := \frac{1}{\beta-\alpha}\Big(\beta - \frac{\widehat{\Phi}_{p^n}(1+T)}{\alpha}\Big), \quad H_n := \begin{pmatrix} -1 & -\rho^{n+1} \\ \rho^{-n} & \rho \end{pmatrix},$$

$$\begin{aligned}\widehat{M}_n &:= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + H_n \widehat{\Upsilon}_n \\ &= \begin{pmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{pmatrix} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}^{-1} \widehat{\mathcal{C}}_n \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix} \begin{pmatrix} \alpha^{-n-1} & 0 \\ 0 & \beta^{-n-1} \end{pmatrix},\end{aligned}$$

$$H_{a,n_1,n_2,\dots,n_l} := H_a H_{a+n_1+1} H_{a+n_1+n_2+2} \cdots H_{a+n_1+n_2+\cdots+n_l+l},$$

$$\widehat{\Upsilon}_{a,n_1,n_2,\dots,n_l} := \widehat{\Upsilon}_a \widehat{\Upsilon}_{a+n_1+1} \widehat{\Upsilon}_{a+n_1+n_2+2} \cdots \widehat{\Upsilon}_{a+n_1+n_2+\cdots+n_l+l}.$$

Note that $\mathcal{L}og_{\alpha,\beta}$ differs from $\lim_{n\to\infty} \widehat{M}_1 \widehat{M}_2 \cdots \widehat{M}_n$ by multiplication by $\left(\begin{smallmatrix} -1 & -1 \\ \beta & \alpha \end{smallmatrix}\right)$ on the left and a diagonal matrix on the right.

Lemma 4.16. $H_{a,n_1,n_2,\dots,n_l} =$

$$H_a \begin{pmatrix} (-1)^l(1-\rho^{-n_1})(1-\rho^{-n_2})\cdots(1-\rho^{-n_l}) & 0 \\ 0 & \rho^l(1-\rho^{n_1})(1-\rho^{n_2})\cdots(1-\rho^{n_l}) \end{pmatrix}.$$

Proof. This follows from the fact that

$$H_a H_{a+b+1} = H_a \begin{pmatrix} -(1-\rho^{-b}) & 0 \\ 0 & \rho(1-\rho^b) \end{pmatrix}.$$ □

Lemma 4.17 (expansion lemma).

$$\widehat{M}_1 \cdots \widehat{M}_n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \sum_{a\geqslant 1}^{n} H_a \widehat{\Upsilon}_a + \sum_{l\geqslant 1} \sum_{\substack{a\geqslant 1,\, n_i \geqslant 1 \\ l+a+\sum_{i\geqslant 1}^{l} n_i \leqslant n}} H_{a,n_1,n_2,\dots,n_l} \widehat{\Upsilon}_{a,n_1,n_2,\dots,n_l}.$$

Proof. We prove this by induction. For $n=1$, this is just the definition. Now assume the lemma holds for n. We want to show that it holds for $n+1$. The entries in the very last sum are products of $(l+1)$ matrices $H_m \widehat{\Upsilon}_m$ whose subindices are bounded above by n. In fact, the entries are all such matrix products with the two following conditions on the subindices m:

- The m's are off by at least 2.
- The m's are in ascending order.

Note that the first sum corresponds to the $l=0$ case.

We want to show that

$$(\widehat{M}_1 \cdots \widehat{M}_n)\Big(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + H_{n+1}\widehat{\Upsilon}_{n+1}\Big) = \widehat{M}_1 \cdots \widehat{M}_n + \widehat{M}_1 \cdots \widehat{M}_n H_{n+1} \widehat{\Upsilon}_{n+1}$$

satisfies Lemma 4.17. Each time when multiplying $H_{n+1}\widehat{\Upsilon}_{n+1}$ with the product of $(l+1)$ matrices that satisfy the conditions in the bullet points above, we obtain a product of $(l+2)$ matrices whose subindices are now bounded by $n+1$. The subindices are still in ascending order, and we may assume they are also off by at least 2, since

$$H_a H_{a+1} = \begin{pmatrix} -1 & -\rho^{a+1} \\ \rho^{-a} & \rho \end{pmatrix} \begin{pmatrix} -1 & -\rho^{a+2} \\ \rho^{-a-1} & \rho \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \qquad \square$$

Proof of the main lemma (Lemma 4.4). We want to prove that the sums involved in Lemma 4.17 converge as $n \to \infty$.

When $\beta = \alpha$, $w = \mathrm{ord}_p(\alpha) = \frac{1}{2}$, so that the arguments of [Sprung 2012, Lemma 4.4] work; see [Lei et al. 2010, Remark 5.26]. Thus, suppose $\beta \neq \alpha$. Fix $r < 1$.

For convergence of the first sum, we see the terms in the valuation matrix $[H_a\widehat{\Upsilon}_a]_r$ are bounded below by the terms in

$$\begin{bmatrix} a & 2wa \\ (2-2w)a & a \end{bmatrix}$$

up to a constant independent from a or n. This follows from Example 4.13 and the fact that $\prod_{i\geqslant 1}^{a-1} \Phi_{p^i}(1+T)$ divides $\widehat{\Upsilon}_a$: Indeed, $\widehat{\Upsilon}_a$ vanishes at $T = \zeta_{p^i} - 1$ for $1 \leqslant i \leqslant a-1$, since $\Phi_{p^a}(\zeta_{p^i}) = p$. All terms in this valuation matrix go to ∞ as a does, except for the upper-right term when $w = 0$, or the lower left term when $w = \frac{1}{2}$.

Now we handle the second (double) sum. We want to show that

$$H_{a,n_1,n_2,\dots,n_l}\widehat{\Upsilon}_{a,n_1,n_2,\dots,n_l}$$

is bounded. Note that we have $\mathrm{ord}_p(\rho(1-\rho^m)) \geqslant (2w-1)(1+m)$ so that

$$[\widehat{\Upsilon}_{a+m}\rho(1-\rho^m)]_r \geqslant 2wm + a + C$$

for some constant C independent of a or m. Assume for the moment that we are in the supersingular case. Lemma 4.16 and the easier fact that $[\widehat{\Upsilon}_{a+m}\rho(1-\rho^{-m})]_r \geqslant a+m$ then shows that all entries in the valuation matrix of $H_{a,n_1,n_2,\dots,n_l}\widehat{\Upsilon}_{a,n_1,n_2,\dots,n_l}$, except possibly for the lower-left term, have terms bounded below by the corresponding entries of $H_a\widehat{\Upsilon}_a$.

Thus, three of the terms of $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ converge in the supersingular case. Since $\det \widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ converges as well, all terms of $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ converge. For $\mathcal{L}og_{\alpha,\beta}(1+T)$, we take our hats off.

For the ordinary case, analogous arguments hold for the terms in the left column.

$\square$

The rate of growth.

Definition 4.18. For $f(T), g(T) \in \mathbb{C}_p[\![T]\!]$ converging on the open unit disc, we say $f(T)$ is $O(g(T))$ if

$$p^{-v_r(f(T))} \text{ is } O(p^{-v_r(g(T))}) \quad \text{as } r \to 1^-,$$

i.e., there is an $r_0 < 1$ and a constant C such that

$$v_r(g(T)) < v_r(f(T)) + C \quad \text{when } 1 > r > r_0.$$

If $f(T)$ is $O(g(T))$ and $g(T)$ is $O(f(T))$, we say "$f(T)$ grows like $g(T)$," and write $f(T) \sim g(T)$.

Example 4.19. $1 \sim T \sim \Phi_p(1+T)$. Also, $\det \mathcal{L}og_{\alpha,\beta} \sim \log_p(1+T)$ by Remark 4.5.

Proposition 4.20 (growth lemma). *When $v > \frac{1}{2}$, the entries of $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ and $\mathcal{L}og_{\alpha,\beta}(1+T)$ grow like $\log_p(1+T)^{\frac{1}{2}}$. When $v \leqslant \frac{1}{2}$, the entries in the left column are $O(\log_p(1+T)^v)$, and those in the right $O(\log_p(1+T)^{1-v})$.*

We give the proof for $\mathcal{L}og_{\alpha,\beta}(1+T)$, since it is similar for the case $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$. Before beginning with the proof, let us name the quantities from Example 4.13:

Definition 4.21. $\quad e_{n,r} := v_r(\Phi_{p^n}(1+T)) = \min\bigl(1, -\log_{(p)}(r)(p^n - p^{n-1})\bigr).$

Lemma 4.22. *The entries of $\mathcal{L}og_{\alpha,\beta}(1+T)$ are $O(\log_p(1+T)^{1-w})$.*

Proof. It suffices to prove this for $\lim_{n\to\infty} M_1 \cdots M_n$, where the M_i are as in Definition 4.15. Note that

$$M_n = \Phi_{p^n}(1+T)\begin{pmatrix} 1/\alpha & 1/\beta \\ -1/\alpha & -1/\beta \end{pmatrix} + \begin{pmatrix} -\alpha & -\alpha \\ -\beta & -\beta \end{pmatrix},$$

so that for $r < 1$,

$$[M_n]_r \geqslant e_{n,r} + w - 1 \geqslant (1-w)(e_{n,r} - 1).$$

Hence,

$$[M_1 \cdots M_n]_r \geqslant (1-w)\sum_{i\geqslant 1}^{n}(e_{i,r} - 1) = (1-w)\prod_{i\geqslant 1}^{n}\left[\frac{\Phi_{p^i}(1+T)}{p}\right]_r.$$

Taking limits, the result follows. □

We implicitly used diagonalization in an earlier proof, but write it out for convenience:

Observation 4.23. Let m be an integer. Then

$$\begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}\begin{pmatrix} \alpha^m & 0 \\ 0 & \beta^m \end{pmatrix} = C^m \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}.$$

Proof of the growth lemma (Proposition 4.20). We first treat the case $v=0=\operatorname{ord}_p(\alpha)$. When $n \geqslant 1$,

$$[\mathcal{C}_1\cdots\mathcal{C}_n]_r=[\mathcal{C}_1]_r\cdots[\mathcal{C}_n]_r=\begin{bmatrix}0 & 0\\ e_{1,r} & e_{1,r}\end{bmatrix}.$$

By Observation 4.23, the valuation matrix of the left column of $\mathcal{C}_1\cdots\mathcal{C}_n\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right)$ and of $\mathcal{L}og_{\alpha,\beta}$ is $\left[\begin{smallmatrix}0\\ e_{1,r}\end{smallmatrix}\right]$. Thus, these entries are $O(\Phi_p(1+T))$. Since we have $\Phi_p(1+T)\sim 1$ by Example 4.19, they are indeed $O(1)$.

Next, we assume $0<v\leqslant \frac{1}{2}$. Given r, let i be the largest integer such that $e_{i,r}<2v$. Without loss of generality, assume i is even. We then compute

$$\begin{aligned}[\mathcal{C}_1\cdots\mathcal{C}_i]_r&=[\mathcal{C}_1]_r\cdots[\mathcal{C}_i]_r\\ &=\begin{bmatrix}e_{2,r}+e_{4,r}+\cdots+e_{i,r} & v+e_{2,r}+\cdots+e_{i-2,r}\\ v+e_{1,r}+e_{3,r}+\cdots+e_{i-1,r} & e_{1,r}+\cdots+e_{i-1,r}\end{bmatrix}.\end{aligned}$$

Remembering that $e_{i+1,r}\geqslant 2v$, we see that for $n>i$,

$$\begin{aligned}&[\mathcal{C}_1\cdots\mathcal{C}_n]_r\\ &\quad=\begin{bmatrix}(n-i)v+e_{2,r}+e_{4,r}+\cdots+e_{i,r} & (n-i-1)v+e_{2,r}+\cdots+e_{i,r}\\ \geqslant(n-i-1)v+e_{1,r}+\cdots+e_{i-1,r} & \geqslant(n-i)v+e_{1,r}+\cdots+e_{i-1,r}\end{bmatrix},\end{aligned}$$

where by $\geqslant x$ we have denoted an unspecified entry that is greater than or equal to x. By Observation 4.23, we have that $\left[\mathcal{C}_1\cdots\mathcal{C}_n C^{-(N+1)}\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right)\right]_r$ is

$$\begin{bmatrix}\geqslant(n-N-i)v+e_{2,r}+\cdots+e_{i,r} & \geqslant(n+N-i)v-N+e_{2,r}+\cdots+e_{i,r}\\ \geqslant(n-N-i+1)v+e_{1,r}+\cdots+e_{i-1,r} & \geqslant(n+N-i+1)v-N+e_{1,r}+\cdots+e_{i-1,r}\end{bmatrix}.$$

Now let $m:=i-\lfloor\operatorname{ord}_p(2v)\rfloor$. We then have $e_{m-h,r}\cdot 2v\leqslant e_{i-h,r}$ for any $h<i$, and $e_{M,r}=1$ for any $M>m$. Thus, the top-left entry of $\left[\mathcal{C}_1\cdots\mathcal{C}_n C^{-(N+1)}\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right)\right]_r$ is, up to a constant independent from r, greater than or equal to

$$2v(e_{m-i+2,r}+e_{m-i+4,r}+\cdots+e_{m,r})-iv=2v\cdot v_r\Biggl(\prod_{\substack{k\geqslant m-i+2\\ k\text{ even}}}^{m}\frac{\Phi_{p^k}(1+T)}{p}\Biggr).$$

Now note that

$$\prod_{\text{even }k\geqslant 2}^{\infty}\frac{\Phi_{p^k}(1+T)}{p}\sim\log_p(1+T)^{\frac{1}{2}}.$$

Using similar arguments, one obtains the appropriate bound for the lower left entry.[5] The claim for the case $0\leqslant v\leqslant\frac{1}{2}$ thus follows from Lemma 4.22.

[5] The same arguments show it for the right entries when $v=\frac{1}{2}$, although this already follows from Lemma 4.22.

Lastly, we treat the case $v > \frac{1}{2}$. Without loss of generality, let $n > 1$ be even. Then

$$[\mathcal{C}_1 \cdots \mathcal{C}_n]_r = [\mathcal{C}_1]_r \cdots [\mathcal{C}_n]_r = \begin{bmatrix} e_{2,r} + e_{4,r} + \cdots + e_{n,r} & v + e_{1,r} + \cdots + e_{n-2,r} \\ v + e_{1,r} + \cdots + e_{n-1,r} & e_{1,r} + \cdots + e_{n-1,r} \end{bmatrix}.$$

From Observation 4.23, $\operatorname{ord}_p(\alpha) = \operatorname{ord}_p(\beta) = \frac{1}{2}$, and $e_{n,r} \leqslant 1$, we compute

$$\left[\mathcal{C}_1 \cdots \mathcal{C}_n C^{-(N+1)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}\right]_r \\ = \begin{bmatrix} -N/2 + e_{2,r} + \cdots + e_{n,r} & -N/2 + e_{2,r} + \cdots + e_{n,r} \\ (1-N)/2 + e_{1,r} + \cdots + e_{n-1,r} & (1-N)/2 + e_{1,r} + \cdots + e_{n-1,r} \end{bmatrix}.$$

Up to a constant independent from r, these entries are

$$v_r\Bigg(\prod_{k \geqslant 2,\ k \text{ even}}^{n} \frac{\Phi_{p^k}(1+T)}{p}\Bigg) = e_{2,r} + \cdots + e_{n,r} - \frac{n}{2},$$
$$v_r\Bigg(\prod_{k \geqslant 1,\ k \text{ odd}}^{n} \frac{\Phi_{p^k}(1+T)}{p}\Bigg) = e_{1,r} + \cdots + e_{n-1,r} - \frac{n}{2}.$$

But from [Pollack 2003, Lemma 4.5], we have

$$\prod_{\text{even } k \geqslant 2}^{\infty} \frac{\Phi_{p^k}(1+T)}{p} \sim \prod_{\text{odd } k \geqslant 1}^{\infty} \frac{\Phi_{p^k}(1+T)}{p} \sim \log_p(1+T)^{\frac{1}{2}},$$

from which the assertion follows for the case $v > \frac{1}{2}$. □

Lemma 4.24. *When $v = 0$, the functions $\widehat{\log}_\alpha^\sharp(1+T)$ and $\widehat{\log}_\alpha^\flat(1+T)$ are in Λ.*

Proof. Observation 4.23 and Remark 4.5. □

The functional equation.

Proposition 4.25. *Under the change of variable $(1+T) \mapsto (1+T)^{-1}$, the first column of $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ is invariant. When all four entries of $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ converge, then*

$$\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T) = \widehat{\mathcal{L}og}_{\alpha,\beta}((1+T)^{-1}) \quad \text{if } p \text{ is odd},$$
$$\begin{pmatrix} 1 & 0 \\ 0 & (1+T)^{-1} \end{pmatrix} \widehat{\mathcal{L}og}_{\alpha,\beta}(1+T) = \widehat{\mathcal{L}og}_{\alpha,\beta}((1+T)^{-1}) \quad \text{if } p = 2.$$

Proof. All $\widehat{\mathcal{C}}_i(1+T)$ are invariant under the change of variables $1+T \mapsto 1/(1+T)$, except $\widehat{\mathcal{C}}_1(1+T)$ if $p = 2$, where we have

$$\widehat{\mathcal{C}}_1\Big(\frac{1}{1+T}\Big) = \begin{pmatrix} 1 & 0 \\ 0 & (1+T)^{-1} \end{pmatrix} \widehat{\mathcal{C}}_1(1+T).$$ □

The functional equation in the case $a_p = 0$. The entries of $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$, when $a_p = 0$, are off by units from the corresponding ones in $\mathcal{L}og_{\alpha,\beta}(1+T)$. More precisely, denote by $\log_p^{\pm}(1+T)$ Pollack's [2003] half-logarithms:

$$\log_p^{+}(T) := \frac{1}{p}\prod_{j\geqslant 1}\frac{\Phi_{p^{2j}}(1+T)}{p}, \quad \text{and} \quad \log_p^{-}(T) := \frac{1}{p}\prod_{j\geqslant 1}\frac{\Phi_{p^{2j-1}}(1+T)}{p}.$$

We then have

$$\mathcal{L}og_{\alpha,\beta}(1+T) = \begin{cases} \dfrac{1}{\epsilon(p)}\begin{pmatrix} \log_p^{+}(T) & \log_p^{+}(T) \\ \log_p^{-}(T)\alpha & \log_p^{-}(T)\beta \end{pmatrix} & \text{when } p \text{ is odd,} \\ \dfrac{1}{\epsilon(2)}\begin{pmatrix} \dfrac{-1}{\epsilon(2)2}\log_2^{+}(T)\alpha & \dfrac{-1}{\epsilon(2)2}\log_2^{+}(T)\beta \\ \log_2^{-}(T) & \log_2^{-}(T) \end{pmatrix} & \text{when } p = 2. \end{cases}$$

Setting $U^{\pm}(1+T) := \widehat{\log_p^{\pm}(T)}/\log_p^{\pm}(T)$, we obtain

$$\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T) = \begin{pmatrix} U^{+}(1+T) & 0 \\ 0 & U^{-}(1+T) \end{pmatrix}\mathcal{L}og_{\alpha,\beta}(1+T).$$

Now put

$$W^{+}(1+T) = \frac{U^{+}(1+T)}{U^{+}((1+T)^{-1})} = \prod_{j\geqslant 1}(1+T)^{-p^{2j-1}(p-1)},$$

and

$$W^{-}(1+T) = \begin{cases} \dfrac{U^{-}(1+T)}{U^{-}((1+T)^{-1})} = \prod_{j\geqslant 1}(1+T)^{-p^{2j-2}(p-1)} & \text{for odd } p, \\ \dfrac{U^{-}(1+T)}{(1+T)U^{-}((1+T)^{-1})} = (1+T)^{-1}\prod_{j\geqslant 2}(1+T)^{-p^{2j-2}(p-1)} & \text{when } p = 2. \end{cases}$$

We can finally arrive at the corrected statement of [Pollack 2003, Lemma 4.6]:

Lemma 4.26. *We have*

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

Proof. This follows from what has been said above, or by going through the proof of [Pollack 2003, Lemma 4.6] on noting that the units $U^{\pm}(1+T) \neq 1$. □

5. The two p-adic L-functions $\widehat{L}_p^{\sharp}(f, T)$ and $\widehat{L}_p^{\flat}(f, T)$

In this section, we construct Iwasawa functions $\widehat{L}_p^{\sharp}(f, T)$ and $\widehat{L}_p^{\flat}(f, T)$. We present the arguments with the completions. The corresponding noncompleted arguments can be recovered by taking off the hat above any expression $\widehat{xyz}$ and replacing it by xyz. Instead of working with the matrices $\widehat{\mathcal{C}}_i$ and C, we make our calculations easier via the following definitions:

Definition 5.1. We put

$$\widehat{\mathcal{A}}_i := \begin{pmatrix} a_p & \widehat{\Phi}_{p^i}(1+T) \\ -\epsilon(p) & 0 \end{pmatrix}, \quad A := \begin{pmatrix} a_p & p \\ -\epsilon(p) & 0 \end{pmatrix}, \quad \tilde{A} := \begin{pmatrix} a_p & 1 \\ -\epsilon(p) & 0 \end{pmatrix}.$$

Definition 5.2. For any integer i, put $Y_{2i} := p^{-i} A^{2i}$, and $Y_{2i+1} = Y_{2i}\tilde{A}$.

Proposition 5.3 (tandem lemma). *Fix $n \in \mathbb{N}$. Assume that for any $i \in \mathbb{N}$, we are given functions $Q_i = Q_i(T)$ such that $Q_i \in \Phi_{p^i}(1+T)\mathcal{O}[T]$ whenever $i \leqslant n$, and $(Q_{n+1}, Q_n)Y_{n'-n} = (Q_{n'+1}, Q_{n'})$ for any $n' \in \mathbb{N}$. Then*

$$(Q_{n+1}, Q_n) = (\widetilde{q}_1, q_0)\widehat{\mathcal{A}}_1 \cdots \widehat{\mathcal{A}}_n \quad \text{with } \widetilde{q}_1, q_0 \in \mathcal{O}[T].$$

Proof. We inductively show that $(Q_{n+1}, Q_n) = (\widetilde{q}_{i+1}, q_i)\widehat{\mathcal{A}}_{i+1} \cdots \widehat{\mathcal{A}}_n$ for $\widetilde{q}_{i+1}, q_i \in \mathcal{O}[T]$ with $0 \leqslant i \leqslant n$: Note that at the base step $i = n$, the product of the $\widehat{\mathcal{A}}$'s is empty so that we indeed have $(\widetilde{q}_{n+1}, q_n) = (Q_{n+1}, Q_n)$. For the inductive step, let $i \geqslant 1$. Then we have

$$(Q_{n+1}, Q_n) = (\widetilde{q}_{i+1}, q_i)A^{n-i} \quad \text{by evaluation at } \zeta_{p^i} - 1,$$
$$(Q_{n+1}, Q_n)Y_{i-n} = (Q_{i+1}, Q_i) \qquad \text{by assumption.}$$

We thus have

$$(\widetilde{q}_{i+1}, q_i)A^{n-i}Y_{i-n} = (Q_{i+1}, 0) \quad \text{at } \zeta_{p^i} - 1,$$

whence q_i vanishes at $\zeta_{p^i} - 1$. We hence write $q_i = \widehat{\Phi}_{p^i}(1+T) \cdot \widetilde{q}_i$ for some $\widetilde{q}_i \in \mathcal{O}[T]$. Now put $(\widetilde{q}_i, q_{i-1}) := (\widetilde{q}_{i+1}, \widetilde{q}_i)\tilde{A}^{-1}$. Then $(\widetilde{q}_{i+1}, q_i) = (\widetilde{q}_i, q_{i-1})\widehat{\mathcal{A}}_i$. □

Observation 5.4. Let $(\Theta_n)_n$ be a queue sequence and $\pi : \Lambda_n \to \Lambda_{n-1}$ be the projection. Then for $n \geqslant 2$, we have $\pi(\Theta_n, \nu\Theta_{n-1}) = (\Theta_{n-1}, \nu\Theta_{n-2})A$.

Proof. Definition 2.7. □

Proposition 5.5. *Let $(\Theta_n)_n$ be a queue sequence and $0 \leqslant n' \leqslant n$. When lifting elements of Λ_n to $\mathcal{O}[T]$, the second entry of $(\Theta_n, \nu\Theta_{n-1})Y_{n'-n}$ vanishes at $\zeta_{p^{n'}} - 1$.*

Proof. Denote by $\pi_{n/n'}$ the projection from Λ_n to $\Lambda_{n'}$. By the above observation, the second entry of

$$\pi_{n/n'}(\Theta_n, \nu\Theta_{n-1})Y_{n'-n} = (\Theta_{n'}, \nu\Theta_{n'-1})A^{n-n'}Y_{n'-n}$$

is contained in the ideal $(\Phi_{n'}) \subset \Lambda_{n'}$. Thus, its preimage under $\pi_{n/n'}$ is in the ideal $(\Phi_{n'}) \subset \Lambda_n$. □

Corollary 5.6. *Let $(\Theta_n)_n$ be a queue sequence. Then*

$$(\Theta_n, \nu\Theta_{n-1}) = \widehat{\Upsilon}_n \widehat{\mathcal{C}}_1 \cdots \widehat{\mathcal{C}}_n \tilde{A}^{-1} \quad \textit{for some } \widehat{\Upsilon}_n \in \Lambda_n^{\oplus 2}.$$

Proof. We identify elements of Λ_n by their corresponding representative in $\mathcal{O}[T]$ and use Proposition 5.5. Then, we can apply the tandem lemma (Proposition 5.3), and project back to $\Lambda_n^{\oplus 2}$. □

Corollary 5.7. (We rewrite the Riemann sum approximations of Definition 2.10) *For some $\widehat{\overrightarrow{L}}{}^{\omega^i}_{p,n} \in \mathcal{O}[T]^{\oplus 2}$,*

$$\begin{aligned}\left(\varepsilon_{\omega^i} L_{N,\alpha}^{\operatorname{sign}(\omega^i)}, \varepsilon_{\omega^i} L_{N,\beta}^{\operatorname{sign}(\omega^i)}\right) &= \widehat{\overrightarrow{L}}{}^{\omega^i}_{p,n} \widehat{\mathcal{C}}_1 \cdots \widehat{\mathcal{C}}_n \tilde{A}^{-1} \begin{pmatrix} \alpha^{-N} & \beta^{-N} \\ -\alpha^{-(N+1)} & -\beta^{-(N+1)} \end{pmatrix} \\ &= \widehat{\overrightarrow{L}}{}^{\omega^i}_{p,n} \widehat{\mathcal{C}}_1 \cdots \widehat{\mathcal{C}}_n C^{-(N+1)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha. \end{pmatrix}.\end{aligned}$$

Proof. We know that $(\alpha^{N+1} L_{N,\alpha}, \beta^{N+1} L_{N,\beta}) = (\vartheta_N, \nu\vartheta_{N-1}) \left(\begin{smallmatrix} \alpha & \beta \\ -\epsilon & -\epsilon \end{smallmatrix}\right)$. The isotypical components of ϑ_N form queue sequences. Now apply Corollary 5.6 and lift back to $\mathcal{O}[T]^{\oplus 2}$. □

The above $\widehat{\overrightarrow{L}}{}^{\omega^i}_{p,n}$ are not unique, so we take limits by regarding the polynomials as elements of $\Lambda_n^{\oplus 2}$:

Definition 5.8. We define

$$\widehat{\overrightarrow{L}}{}^{\omega^i}_{p} := \lim_{n \to \infty} \widehat{\overrightarrow{L}}{}^{\omega^i}_{p,n} \in \Lambda^{\oplus 2}/\mathfrak{M},$$

where $\mathfrak{M}$ is given by the next definition.

Definition 5.9. We put $\mathfrak{M} := \varprojlim_n \mathfrak{M}_n$, where

$$\mathfrak{M}_n := \ker\left(\times \widehat{\mathcal{C}}_1 \cdots \widehat{\mathcal{C}}_n C^{-(N+1)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix} \right) \subset \Lambda_n \oplus \Lambda_n.$$

Proposition 5.10. *For supersingular p, $\mathfrak{M}$ is trivial. For ordinary p,*

$$\mathfrak{M} \cong T\Lambda(-\log_\alpha^\flat \oplus \log_\alpha^\sharp) \subset \Lambda \oplus \Lambda.$$

Proof. Since

$$C^{-(N+1)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix} \begin{pmatrix} -\alpha^{-(N+1)} & 0 \\ 0 & \beta^{-(N+1)} \end{pmatrix},$$

we have

$$\mathfrak{M}_n = p^{\operatorname{ord}_p(\alpha)(N+1)} (\alpha^{N+1}\Lambda_n \oplus \beta^{N+1}\Lambda_n) \begin{pmatrix} \alpha & 1 \\ -\beta & -1 \end{pmatrix} \widehat{\mathcal{C}}_n^* \cdots \widehat{\mathcal{C}}_1^* (\beta - \alpha) T,$$

where $\widehat{\mathcal{C}}_i^*$ is the adjugate of $\widehat{\mathcal{C}}_i$ (see also [Sprung 2012, Lemma 5.8]).

Since the matrix product to the right of $(\alpha^{N+1}\Lambda_n \oplus \beta^{N+1}\Lambda_n)$ has Λ_n-integral coefficients, we see that $\mathfrak{M}_n \subset p^{\mathrm{ord}_p(\alpha)(N+1)}\Lambda_n^{\oplus 2}$ so that $\varprojlim_n \mathfrak{M}_n = 0$ when $\mathrm{ord}_p(\alpha) > 0$. In the ordinary case, only the terms involving a power of β go to zero in the limit, whence the result. □

Proof of Theorem 2.14. We give the proof with the hats, since the proof for the expressions without the hats is the same. Part a follows from taking limits of $\widehat{\overrightarrow{L}}{}_{p,n}^{\omega^i}$ together with the main lemma (Lemma 4.4) and the above Proposition 5.10 (triviality of $\mathfrak{M}$). For part b, the proof is the same up to the description of $\mathfrak{M}$ and Proposition 5.10, which gives rise to the term $g(T)T(-\widehat{\log}{}_\alpha^\flat \oplus \widehat{\log}{}_\alpha^\sharp)$. Now use Lemma 4.24. □

Now that we have finally proved Theorem 2.14, we can give the following corollary:

Corollary 5.11. *Pick T such that $\mathcal{L}og_{\alpha,\beta}(1+T)$ and $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ converge in all entries and are invertible. Then*

$$\begin{aligned}&\big(\widehat{L}_p^\sharp(f,\omega^i,T), \widehat{L}_p^\flat(f,\omega^i,T)\big)\\ &\qquad = \big(L_p^\sharp(f,\omega^i,T), L_p^\flat(f,\omega^i,T)\big)\mathcal{L}og_{\alpha,\beta}(1+T)\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)^{-1}.\end{aligned}$$

Remark 5.12. In our setup so far, we have worked with the periods $\Omega_f^\pm$. In the case of an elliptic curve E over $\mathbb{Q}$, one can alternatively use the real and imaginary Néron periods $\Omega_E^\pm$. These real and imaginary Néron periods are defined as follows.

Definition 5.13. Decompose $H_1(E,\mathbb{R}) = H_1(E,\mathbb{R})^+ \oplus H_1(E,\mathbb{R})^-$, where complex conjugation acts as $+1$ on the first summand and as -1 on the second. Put $H_1^\pm(E,\mathbb{Z}) := H_1(E,\mathbb{Z})^\pm \cap H_1(E,\mathbb{R})$. Choose generators $\delta^\pm$ of $H_1(E,\mathbb{Z})^\pm$ such that the following integrals are positive:

$$\Omega_E^\pm := \begin{cases} \int_{\delta^\pm} \omega_E & \text{if } E(\mathbb{R}) \text{ is connected,}\\ 2\cdot\int_{\delta^\pm}\omega_E & \text{if not.}\end{cases}$$

Convention 5.14. When working with these periods, we may define modular symbols and p-adic L-functions analogously, and write E wherever we have written f before.

In view of [Breuil et al. 2001] and [Wiles 1995], we have a modular parametrization $\pi : X_0(N) \to E$, such that $\pi^*(\omega_E) = c \cdot f_E \cdot (dq)/q$ for some normalized weight-two newform f_E of level N. The constant c is called the *Manin constant* for π. It is known to be an integer (see [Edixhoven 1991, Proposition 2]) and conjectured to be 1. See [Manin 1972, § 5].

We note that the analogue of Theorem 2.1 is not necessarily satisfied when one replaces $\Omega_f^\pm$ by $\Omega_E^\pm$, but the following is known (see [Pollack 2003, Remarks 5.4, 5.5]):

	$L_p^\sharp(f,\omega^i,0)$	$L_p^\flat(f,\omega^i,0)$
p odd, $i=0$	$\bigl(-a_p^2+2a_p+p-1\bigr)\dfrac{L(f,1)}{\Omega_f^+}$	$(2-a_p)\dfrac{L(f,1)}{\Omega_f^+}$
p odd, $i\neq 0$	$-pa_p\dfrac{L(f,\omega^{-i},1)}{\tau(\omega^{-i})\Omega_f^{\omega^i(-1)}}$	$-p\dfrac{L(f,\omega^{-i},1)}{\tau(\omega^{-i})\Omega_f^{\omega^i(-1)}}$
$p=2$, $i=0$	$\bigl(-a_p^3+2a_p^2+2pa_p-a_p-2p\bigr)\dfrac{L(f,1)}{\Omega_f^+}$	$\bigl(-a_p^2+2a_p+p-1\bigr)\dfrac{L(f,1)}{\Omega_f^+}$
$p=2$, $i\neq 0$	$-p^2a_p\dfrac{L(f,\omega^{-i},1)}{\tau(\omega^{-i})\Omega_f^{\omega^i(-1)}}$	$-p^2\dfrac{L(f,\omega^{-i},1)}{\tau(\omega^{-i})\Omega_f^{\omega^i(-1)}}$

Table 2. Table of the special values for a good prime p.

Theorem 5.15 (imitation of Theorem 2.1). *Let E be a strong Weil curve over $\mathbb{Q}$, and p be a prime of good reduction. Then*:

(1) [Abbes and Ullmo 1996, théorème A] *p does not divide c.*

(2) [Manin 1972, Theorem 3.3] *If $a_p \not\equiv 1 \bmod p$, we have*

$$2\left[\frac{a}{p^n}\right]_E^\pm \in c^{-1}\mathbb{Z}, \quad \textit{so} \quad 2\left[\frac{a}{p^n}\right]_E^\pm \in \mathbb{Z}_p.$$

Corollary 5.16. *When $a_p \not\equiv 1 \bmod p$, $L_p^\sharp(E,\omega^i,T)$ and $L_p^\flat(E,\omega^i,T)$ and their completions are in Λ. In particular, the 2-adic L-functions $L_2^\sharp(E,\omega^i,T)$ and $L_2^\flat(E,\omega^i,T)$ from* [Sprung 2012, Definition 6.1] *agree with those of this paper and are consequently elements of Λ, rather than $\Lambda\otimes\mathbb{Q}$.*

Proof. This follows from Theorem 2.14 and what has just been said. For $p=2$, we exploit the following symmetry in the isotypical components of the Riemann sums $L_{N,\alpha}^\pm$ and $L_{N,\beta}^\pm$: From $\eta^\pm(a/m)=\pm\eta^\pm(-a/m)$, we can conclude that $\omega^i(a)\eta^\pm(a/m)=\pm\omega^i(-a)\eta^\pm(-a/m)$. □

Corollary 5.17 (analogue of Theorem 2.14). *When $a_p \not\equiv 1 \bmod p$, the statement of Theorem 2.14 with f formally replaced by E is still valid. When $a_p \equiv 1 \bmod p$ or E is not a strong Weil curve, we can say the same with the added caveat that $L_p^\sharp(E,\omega^i,T)$, $L_p^\flat(E,\omega^i,T)$, and their completions are elements of $\mathbb{Q}\otimes\Lambda$.*

From Theorem 2.6, we can give a table of the special values for a good prime p, as shown in Table 2. In view of these special values, it seems reasonable to make the following conjecture:

Conjecture 5.18. *Let f be a modular form as above, and let p be a good supersingular prime. When p is odd, $\widehat{L}_p^\flat(f,\omega^i,T)$ and $L_p^\flat(f,\omega^i,T)$ are not identically zero, and $\widehat{L}_p^\sharp(f,\omega^i,T)$ and $L_p^\sharp(f,\omega^i,T)$ are not identically zero when $a_p\neq 2$. When $p=2$, the power series $\widehat{L}_2^\sharp(f,\omega^i,T)$ and $L_2^\sharp(f,\omega^i,T)$ are not identically zero, and $\widehat{L}_2^\flat(f,\omega^i,T)$ and $L_2^\flat(f,\omega^i,T)$ are not identically zero when $a_2\neq 1$.*

The functional equation in the supersingular case. Let f be a weight-two modular form of level N and nebentype ϵ which is an eigenform for all T_n. Recall also $\log_\gamma(\cdot)$ introduced in Definition 2.8. We denote by $f^*(z) = w_N(f(z)) = \epsilon(-1)f(-1/(Nz))$ the involuted form of f under the Atkin-Lehner / Fricke operator, as in [Mazur et al. 1986, (5.1)], and let $\alpha^* = \alpha/\epsilon(p)$ and $\beta^* = \beta/\epsilon(p)$.

Theorem 5.19. *Let p be a supersingular prime so that $(p, N) = 1$, i.e., $N \in \mathbb{Z}_p^\times \cong \mathcal{G}_\infty$. Then*

$$\begin{aligned}&\big(\widehat{L}_p^\sharp(f, \omega^i, T),\ \widehat{L}_p^\flat(f, \omega^i, T)\big)\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)\\ &= -\epsilon(-1)\omega^{-i}(-N)(1+T)^{-\log_\gamma(N)}\\ &\qquad\times\Big(\widehat{L}_p^\sharp\Big(f^*, \omega^{-i}, \frac{1}{1+T}-1\Big),\ \widehat{L}_p^\flat\Big(f^*, \omega^{-i}, \frac{1}{1+T}-1\Big)\Big)\widehat{\mathcal{L}og}_{\alpha^*,\beta^*}(1+T).\end{aligned}$$

Corollary 5.20. *For an elliptic curve E over $\mathbb{Q}$ and a good supersingular prime p, let c_N be the sign of f, i.e., $f^* := -c_N f$* (see [Mazur et al. 1986, §18]). *We then have*

$$\widehat{L}_p^\sharp(E, \omega^i, T) = -(1+T)^{-\log_\gamma(N)}\omega^i(-N)c_N\widehat{L}_p^\sharp\Big(E, \omega^i, \frac{1}{1+T}-1\Big),$$
$$\widehat{L}_p^\flat(E, \omega^i, T) = -(1+T)^{-\log_\gamma(N)}\omega^i(-N)c_N\widehat{L}_p^\flat\Big(E, \omega^i, \frac{1}{1+T}-1\Big).$$

When $a_p = 0$, we can give an explicit functional equation for the noncompleted p-adic L-functions, which corrects [Pollack 2003, Theorem 5.13] *in the case $i = 0$:*

$$L_p^\sharp(E, \omega^i, T) = -(1+T)^{-\log_\gamma(N)}\omega^i(-N)c_N W^+(1+T)L_p^\sharp\Big(E, \omega^i, \frac{1}{1+T}-1\Big),$$
$$L_p^\flat(E, \omega^i, T) = -(1+T)^{-\log_\gamma(N)}\omega^i(-N)c_N W^-(1+T)L_p^\flat\Big(E, \omega^i, \frac{1}{1+T}-1\Big).$$

Proof of Theorem 5.19. This follows from the functional equations for $\widehat{L}_p(f,\alpha,\omega^i,T)$ and $\widehat{L}_p(f, \beta, \omega^i, T)$, which formally display exactly the same invariance under the substitution $T \mapsto (1+T)^{-1}-1$, see [Mazur et al. 1986, §17, (17.3)]. The rest is invariance of $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ under $T \mapsto (1+T)^{-1}-1$, see Proposition 4.25. □

Part II. Invariants coming from the conjectures of Birch and Swinnerton-Dyer in the cyclotomic direction

6. The conjectures about the rank and leading coefficient

We scrutinize what happens when $T = \zeta_{p^n} - 1$ for $n \geqslant 1$: we estimate BSD-theoretic quantities in the cyclotomic direction, using the pairs of Iwasawa invariants of $L_p^\sharp$ and $L_p^\flat$ (which match those of $\widehat{L}_p^\sharp$ and $\widehat{L}_p^\flat$ when used, see Corollary 8.9).

Choose $\mathcal{G}_f \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\left\{f^\sigma = \sum \sigma(a_n)q^n\right\}_{\sigma\in\mathcal{G}_f}$ contains each Galois conjugate of f once.

Definition 6.1. For $\sigma \in \mathcal{G}_f$, the σ-parts of the (p-adic) analytic ranks of $A_f(\mathbb{Q}_n)$ and of $A_f(\mathbb{Q}_\infty)$ are

$$r_n^{\mathrm{an}}(f^\sigma) = \sum_{\zeta:\ p^n\text{-th roots of unity}} \mathrm{ord}_{\zeta-1}(L_p(f^\sigma, \alpha, T)),$$

$$r_\infty^{\mathrm{an}}(f^\sigma) := \lim_{n\to\infty} r_n^{\mathrm{an}}(f^\sigma) = \sum_{\zeta:\ \textit{all}\ p\text{-power roots of unity}} \mathrm{ord}_{\zeta-1}(L_p(f^\sigma, \alpha, T)).$$

Note that by a theorem of Rohrlich [1984], r_∞^{an} is a finite integer.

We can then estimate the p-adic analytic rank of $A_f(\mathbb{Q}_n)$ and of $A_f(\mathbb{Q}_\infty)$ by setting

$$r_n^{\mathrm{an}} := \sum_{\sigma\in\mathcal{G}_f} r_n^{\mathrm{an}}(f^\sigma) \quad \text{and} \quad r_\infty^{\mathrm{an}} := \sum_{\sigma\in\mathcal{G}_f} r_\infty^{\mathrm{an}}(f^\sigma). \tag{2}$$

Conjecturally, r_∞^{an} should agree with the complex analytic rank of $A_f(\mathbb{Q}_\infty)$ defined by the order of vanishing of the Hasse–Weil series $L(A_f/\mathbb{Q}_\infty, s)$ at $s = 1$.

Definition 6.2. We let d_n be the normalized jump in the ranks of A_f at level $\mathbb{Q}_n$:

$$d_n := \frac{\mathrm{rank}(A_f(\mathbb{Q}_n)) - \mathrm{rank}(A_f(\mathbb{Q}_{n-1}))}{p^n - p^{n-1}}.$$

Denote by $D(\mathbb{Q}_n)$ the discriminant, by $R(A_f/\mathbb{Q}_n)$ the regulator, by $\mathrm{Tam}(A_f/\mathbb{Q}_n)$ the product of the Tamagawa numbers, and let $\Omega_{A_f/\mathbb{Q}_n} = (\Omega_{A_f/\mathbb{Q}})^{p^n}$, where $\Omega_{A_f/\mathbb{Q}}$ is the real period of A_f. We also denote by $\widehat{A}_f$ the dual of A_f.

Conjecture 6.3 (cyclotomic BSD). *Let ζ_{p^n} be a primitive p^n-th root of unity, $d_n^{\mathrm{an}}(f)$ the order of vanishing of $L_p(f, \alpha, T)$ at $T = \zeta_{p^n} - 1$, and $r_n^{\mathrm{an}'}(f)$ the order of vanishing of the complex L-series $L(f/\mathbb{Q}_n, s) := \prod_{\chi\in\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})} L(f, \chi, s)$ at $s = 1$. Then*

$$d_n^{\mathrm{an}}(f) = \frac{r_n^{\mathrm{an}'}(f) - r_{n-1}^{\mathrm{an}'}(f)}{p^n - p^{n-1}} \quad \textit{and} \quad \sum_\sigma d_n^{\mathrm{an}}(f^\sigma) = d_n.$$

In particular, the order of vanishing $r_n^{\mathrm{an}'}$ of $L(A_f/\mathbb{Q}_n, s) := \prod_\sigma L(f^\sigma/\mathbb{Q}_n, s)$ at $s = 1$ is d_n.

In view of this conjecture, we put (see [Manin 1971, Remark 8.5]):

$$\#\text{Ш}^{\mathrm{an}}(A_f/\mathbb{Q}_n) := \frac{L^{(r_n^{\mathrm{an}'})}(A_f/\mathbb{Q}_n, 1)\#A_f^{\mathrm{tor}}(\mathbb{Q}_n)\#\widehat{A}_f^{\mathrm{tor}}(\mathbb{Q}_n)\sqrt{D(\mathbb{Q}_n)}}{(r_n^{\mathrm{an}'})!\Omega_{A_f/\mathbb{Q}_n} R(A_f/\mathbb{Q}_n)\,\mathrm{Tam}(A_f/\mathbb{Q}_n)}.$$

Our notation of $d_n^{\mathrm{an}}(f)$, which is independent of the choice ζ_{p^n}, is justified as follows:

Lemma 6.4.
$$d_n^{\mathrm{an}}(f) = \frac{r_n^{\mathrm{an}}(f) - r_{n-1}^{\mathrm{an}}(f)}{p^n - p^{n-1}}.$$

We postpone the proof until after Lemma 7.4.

Remark 6.5. It is not clear (at least not to the author) how to relate the leading Taylor coefficient of $L_p(f,\alpha,T)$ at $T=\zeta_{p^n}-1$ to the size of the Šafarevič–Tate groups, even when A_f is an elliptic curve. (For a relative version, see [Mazur and Swinnerton-Dyer 1974, §9.5, Conjecture 4].)

7. The Mordell–Weil rank in the cyclotomic direction

We now give an upper bound for $r_\infty^{\mathrm{an}}(f)$. When f is ordinary at p, we have the estimate $\lambda \geqslant r_\infty^{\mathrm{an}}(f)$, where λ is the λ-invariant of $L_p(f,\alpha,T)$. This section is devoted to the more complicated supersingular scenario. We give two different upper bounds. To obtain an upper bound on r_∞^{an}, one then simply sums the bounds on $r_\infty^{\mathrm{an}}(f^\sigma)$. (*Note that f^σ may be ordinary or supersingular at p independently of whether f was!*) Recall that the weight of f is two in this paper, so that trivial zeros of p-adic L-functions are not an issue.

Proposition 7.1. *Let f be a weight-two modular form and p be a good supersingular prime. If ζ is a p^n-th root of unity*, *then we have*

$$\operatorname{ord}_{\zeta-1} L_p(f,\alpha,T) = \operatorname{ord}_{\zeta-1} L_p(f,\beta,T).$$

Proof. For $n=0$, this is [Pollack 2003, Lemma 6.6]. Thus, let $n>0$. Let us first prove that $L_p(f,\alpha,\zeta-1)=0$ if and only if $L_p(f,\beta,\zeta-1)=0$: Observation 4.8 allows us to conclude that

$$\begin{aligned}\big(L_p(f,\alpha,\zeta-1),\, L_p(f,\beta,\zeta-1)\big)&\\ &= \overrightarrow{L_p}(f,\zeta-1)\mathcal{L}og_{\alpha,\beta}(\zeta-1)\\ &= \overrightarrow{L_p}(f,\zeta-1)\begin{pmatrix} * & * \\ * & * \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \Phi_{p^n}(\zeta)\end{pmatrix}\begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}\begin{pmatrix} \alpha^{-N} & 0 \\ 0 & \beta^{-N}\end{pmatrix}\\ &= \overrightarrow{L_p}(f,\zeta-1)\begin{pmatrix} * & * \\ * & * \end{pmatrix}\begin{pmatrix} -1 & -1 \\ \beta\Phi_{p^n}(\zeta) & \alpha\Phi_{p^n}(\zeta)\end{pmatrix}\begin{pmatrix} \alpha^{-N} & 0 \\ 0 & \beta^{-N}\end{pmatrix}\end{aligned}$$

for some 2×2-matrix $\left(\begin{smallmatrix} * & * \\ * & * \end{smallmatrix}\right)$ with entries in $\overline{\mathbb{Q}}$. But $\Phi_{p^n}(\zeta)=0$, so

$$L_p(f,\alpha,\zeta-1)=0 \quad \text{implies} \quad \overrightarrow{L_p}(\zeta-1)\begin{pmatrix} * & * \\ * & * \end{pmatrix} = (0,*).$$

Thus, we can conclude that $L_p(f,\beta,\zeta-1)=0$. A symmetric argument shows $L_p(f,\beta,\zeta-1)=0$ implies $L_p(f,\alpha,\zeta-1)=0$.

The rest is induction: Fixing $k\in\mathbb{N}$ and assuming

$$L_p^{(i)}(f,\alpha,\zeta-1)=L_p^{(i)}(f,\beta,\zeta-1)=0 \quad \text{for } 0\leqslant i<k,$$

we have

$$\big(L_p^{(k)}(f,\alpha,\zeta-1), L_p^{(k)}(f,\beta,\zeta-1)\big) = \overrightarrow{L}_p^{(k)}(f,\zeta-1)\mathcal{L}og_{\alpha,\beta}(\zeta-1)$$

by the product rule. By the above argument, $L_p^{(k)}(f,\alpha,\zeta-1)=0$ if and only if $L_p^{(k)}(f,\beta,\zeta-1)=0$. □

Corollary 7.2. *Let $a_p=0$. Then we have $r_\infty^{\mathrm{an}}(f)\leqslant \lambda_\sharp+\lambda_\flat$.*

This has already been proved by Pollack in the elliptic curve case when $p\equiv 3 \bmod 4$ and $a_p=0$. He derived Proposition 7.1 in this case by a very clever argument involving Gauß sums (for which $p\equiv 3 \mod 4$ is needed) and the functional equation (which is simple enough for elliptic curves).

Proof of Corollary 7.2. The proof of [Pollack 2003, Corollary 6.8] now works in the desired generality, since the only hard ingredient was Proposition 7.1. □

Definition 7.3. For any integer n, let Ξ_n be the matrix such that $\mathcal{L}og_{\alpha,\beta}=\mathcal{C}_1\cdots\mathcal{C}_n\,\Xi_n$.

Lemma 7.4. *Fix an integer n and let $m\leqslant n$. Then*

$$\mathrm{ord}_{\zeta_{p^m}-1}L_p(f,\alpha,T)=j \quad \textit{if and only if} \quad \mathrm{ord}_{\zeta_{p^m}-1}\overrightarrow{L_p}(f,T)\mathcal{C}_1\cdots\mathcal{C}_n=j.$$

Proof. Since $\det \Xi_n(\zeta_{p^m}-1)\neq 0$, we have by induction on i and Proposition 7.1 that

$$L_p^{(i)}(f,\alpha,\zeta_{p^m}-1)=0 \quad \text{for } i\leqslant j-1 \text{ but not for } i=j$$

is equivalent to

$$\overrightarrow{L}_p^{(i)}(f,T)\mathcal{C}_1\cdots\mathcal{C}_n(\zeta_{p^m}-1)=(0,0) \quad \text{for } i\leqslant j-1 \text{ but not for } i=j,$$

which is equivalent to $\mathrm{ord}_{\zeta_{p^m}-1}\overrightarrow{L_p}(f,T)\mathcal{C}_1\cdots\mathcal{C}_n=j$. □

Proof of Lemma 6.4. The entries of the vector $\overrightarrow{L_p}(f,T)\mathcal{C}_1\cdots\mathcal{C}_n$ are up to units polynomials, so for $m\leqslant n$, we have

$$\mathrm{ord}_{\zeta_{p^m}-1}\overrightarrow{L_p}(f,T)\mathcal{C}_1\cdots\mathcal{C}_n=\mathrm{ord}_{\zeta'_{p^m}-1}\overrightarrow{L_p}(f,T)\mathcal{C}_1\cdots\mathcal{C}_n$$

for any two primitive p^m-th roots of unity ζ_{p^m} and ζ'_{p^m}. From Lemma 7.4,

$$\mathrm{ord}_{\zeta_{p^m}-1}L_p(f,\alpha,T)=\mathrm{ord}_{\zeta'_{p^m}-1}L_p(f,\alpha,T). \qquad □$$

Notation 7.5. Given $x\in\mathbb{Q}$, we let $\lfloor x\rfloor$ be the largest integer $\leqslant x$.

Definition 7.6. We define the n-th $\sharp/\flat$-*Kurihara terms* $q_n^{\sharp/\flat}$ and some auxiliary integers $\nu_{\sharp/\flat}$, $\widetilde{\nu}_{\sharp/\flat}$.

$$\begin{aligned}
&q_n^\sharp := \left\lfloor \frac{p^n}{p+1} \right\rfloor \text{ if } n \text{ is odd,} \quad \text{and} \quad q_n^\sharp := q_{n+1}^\sharp \text{ for even } n,\\
&q_n^\flat := \left\lfloor \frac{p^n}{p+1} \right\rfloor \text{ if } n \text{ is even,} \quad \text{and} \quad q_n^\flat := q_{n+1}^\flat \text{ for odd } n,\\
&\nu_\sharp := \text{largest odd integer } n \geqslant 1 \text{ such that } \lambda_\sharp \geqslant p^n - p^{n-1} - q_n^\sharp,\\
&\nu_\flat := \text{largest even integer } n \geqslant 2 \text{ such that } \lambda_\flat \geqslant p^n - p^{n-1} - q_n^\flat,\\
&\widetilde{\nu}_\flat := \text{largest odd integer } n \geqslant 3 \text{ such that } \lambda_\flat \geqslant p^n - p^{n-1} - pq_{n-1}^\flat - (p-1)^2,\\
&\widetilde{\nu}_\sharp := \text{largest even integer } n \geqslant 2 \text{ such that } \lambda_\sharp \geqslant p^n - p^{n-1} - pq_{n-1}^\sharp.
\end{aligned}$$

In case no such integer exists, we put respectively $\nu_\sharp := 0$, $\nu_\flat := 0$, $\widetilde{\nu}_\sharp := 0$, but $\widetilde{\nu}_\flat := 1$.

Note that explicitly, we have

$$\begin{aligned}
q_n^\sharp &= p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \cdots + p^2 - p \quad \text{for odd } n > 1,\\
q_n^\flat &= p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \cdots + p - 1 \quad \text{for even } n > 0.
\end{aligned}$$

Convention 7.7. We define the μ-invariant of the 0-function to be ∞.

Theorem 7.8.

- *When* $|\mu_\sharp - \mu_\flat| \leqslant v = \mathrm{ord}_p(a_p)$ (*e.g., when* $a_p = 0$), *put* $\nu = \max(\nu_\sharp, \nu_\flat)$. *We then have* $r_\infty^{\mathrm{an}}(f) \leqslant \min(q_\nu^\sharp + \lambda_\sharp, q_\nu^\flat + \lambda_\flat)$.
- *When* $\mu_\sharp > \mu_\flat + v$, *put* $\nu = \max(\nu_\flat, \widetilde{\nu}_\flat)$. *We then have*
$$r_\infty^{\mathrm{an}}(f) \leqslant \begin{cases} \min(q_\nu^\flat + \lambda_\flat, q_{\nu-1}^\flat - (p-1)^2 + \lambda_\flat) & \text{when } \nu \neq 1,\\ \min(q_1^\flat + \lambda_\flat, q_1^\sharp + \lambda_\sharp) & \text{when } \nu = 1.\end{cases}$$
- *When* $\mu_\flat > \mu_\sharp + v$, *put* $\nu = \max(\nu_\sharp, \widetilde{\nu}_\sharp)$. *We then have*
$$r_\infty^{\mathrm{an}}(f) \leqslant \min(pq_{\nu-1}^\sharp + \lambda_\sharp, q_\nu^\sharp + \lambda_\sharp).$$

Definition 7.9. For a vector $\overrightarrow{a} = (a_\sharp, a_\flat) \in \Lambda^{\oplus 2}$, we define its λ-invariant as $\lambda(\overrightarrow{a}) := \min(\lambda(a_\sharp), \lambda(a_\flat))$.

Proof of Theorem 7.8. We handle the first case first. Denote $L_p(f, \alpha, T)$ by L_α. In the proof, we justify the two equality signs in the following equation:

$$\sum_{\substack{\text{all } p\text{-power}\\ \text{roots of unity } \zeta}} \mathrm{ord}_{\zeta-1} L_\alpha = \sum_{\substack{\zeta \text{ s.t. } \zeta^{p^n}=1\\ \text{and } n \leqslant \nu}} \mathrm{ord}_{\zeta-1} L_\alpha = \sum_{\substack{\zeta \text{ s.t. } \zeta^{p^n}=1\\ \text{and } n \leqslant \nu}} \mathrm{ord}_{\zeta-1} \overrightarrow{L}_p \mathcal{C}_1 \cdots \mathcal{C}_\nu$$

The result then follows on noting that the last term is bounded by $\lambda(\overrightarrow{L}_p \mathcal{C}_1 \cdots \mathcal{C}_\nu)$.

We justify the first equality sign. By Proposition 7.1, $\mathrm{ord}_{\zeta_{p^n}-1} L_\alpha = \mathrm{ord}_{\zeta_{p^n}-1} L_\beta$. Since we have $\det \Xi_n|_{T=\zeta_{p^n}-1} \neq 0$, we can say that $\mathrm{ord}_{\zeta_{p^n}-1} L_\alpha = 0$ if and only if

$\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_n|_{T=\zeta_{p^n}-1}\neq(0,0)$. Since $\lambda(\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_n)$ is bounded above by $\lambda_\sharp+q_n^\sharp$ and $\lambda_\flat+q_n^\flat$, we have that

$$p^n-p^{n-1}>\min(\lambda_\sharp+q_n^\sharp,\lambda_\flat+q_n^\flat)\quad\text{implies}\quad\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_n|_{\zeta_{p^n}-1}\neq(0,0).$$

Now $\lambda_\flat+q_n^\flat<p^n-p^{n-1}$ for some even n implies $\lambda_\flat+q_m^\flat<p^m-p^{m-1}$ for any even $m\geqslant n$. Similarly, $\lambda_\sharp+q_n^\sharp<p^n-p^{n-1}$ for some odd n implies $\lambda_\sharp+q_m^\sharp<p^m-p^{m-1}$ for any odd $m\geqslant n$. Thus,

$$m>\nu\quad\text{implies}\quad\operatorname{ord}_{\zeta_{p^m}-1}L_\alpha=0.$$

The second equality sign follows from Lemma 7.4 applied to $n=\nu$.

In the other cases, similar arguments hold, with the following caveats: in the second case,

$$\lambda(\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_n)=\begin{cases}\lambda_\flat+q_n^\flat & \text{when } n \text{ is even,}\\ \lambda_\flat+pq_{n-1}^\flat-(p-1)^2 & \text{when } n \text{ is odd and } n\neq1,\\ \lambda_\flat+q_1^\flat & \text{when } n=1,\end{cases}$$

while in the third case,

$$\lambda(\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_n)=\begin{cases}\lambda_\sharp+pq_{n-1}^\sharp & \text{when } n \text{ is even,}\\ \lambda_\sharp+q_n^\sharp & \text{when } n \text{ is odd.}\end{cases}$$

The asymmetry in the second case comes from

$$(L_p^\sharp,L_p^\flat)\mathcal{C}_1\equiv(-\Phi_pL_p^\flat,L_p^\sharp)\mod a_p.\qquad\square$$

Comparing this bound with the sum of λ-invariants bound of Corollary 7.2, we find that it is in most cases sharper. (The exception is when $p=2$, in which case it is *never sharper*. Here, the cases when the bounds match is when there is an odd ν so that $\lambda_\sharp=q_\nu^\sharp$ and $\lambda_\flat\leqslant q_\nu^\flat$ or there is an even ν so that $\lambda_\flat=q_\nu^\flat$ and $\lambda_\sharp\leqslant q_\nu^\sharp$.) When p is odd and f is elliptic modular, this bound is strictly sharper in all known cases (see the tables of Perrin-Riou [2003] and Pollack [2002]), except when:

(1) $\lambda_\flat=0$ and $\lambda_\sharp<p-1$,

(2) $p=3$, and

$(\lambda_\sharp,\lambda_\flat)\in\{(0,6),(1,5),(1,6),(2,4),(2,5),(2,6),(12,2),(13,x)\text{ with }x\leqslant5\}$.

The following corollary gives a bound that is in the spirit of the bound in the ordinary case:

Corollary 7.10. *Assume $\lambda_\sharp<p-1$ and $\lambda_\flat<p^2-p-p+1=(p-1)^2$. Then $r_\infty^{\mathrm{an}}(f)\leqslant\min(\lambda_\sharp,\lambda_\flat)$ for $\mu_\flat\leqslant\mu_\sharp+v$, while $r_\infty^{\mathrm{an}}(f)\leqslant\lambda_\sharp$ when $\mu_\flat>\mu_\sharp+v$.*

Proof. Indeed, we have $\nu_\sharp=\nu_\flat=\widetilde{\nu}_\sharp=\widetilde{\nu}_\flat-1=0$ in this case. $\square$

Example 7.11. When p is odd and $\lambda_\sharp = \lambda_\flat = 1$, we have $r_\infty^{\mathrm{an}} = r_\infty^{\mathrm{an}}(f) \leqslant 1$; see [Perrin-Riou 2003, Proposition 7.17] for the elliptic curve case. This case is very common numerically.

We thank Robert Pollack for pointing out the following example in which the sum of the λ-invariants is not a bound for $r_\infty^{\mathrm{an}}(f)$ as in Corollary 7.2. Our proposition explains the bound:

Example 7.12. Consider E37A. For the prime 3, we have $a_3 = -3$, and at this prime 3, we have $\lambda_\sharp = 1$, while $\lambda_\flat = 5$, and $r_\infty^{\mathrm{an}} = r_\infty^{\mathrm{an}}(f) = 7$. In this case $\nu_\sharp = 0$ and $\nu_\flat = 2$. Thus, the bound for r_∞^{an} is $\min(q_2^\flat + 5, q_2^\sharp + 1) = \min(3-1+5, 3^2-3+1) = 7$. Note that $r_\infty^{\mathrm{an}} = 7 > \lambda_\sharp + \lambda_\flat = 6$.

8. The special value of the L-function of f in the cyclotomic direction

The purpose of this section is to prove a special value formula for modular forms of weight two in the cyclotomic direction that estimates the size of $\text{Ш}^{\mathrm{an}}(A_f/\mathbb{Q}_n)[p^\infty]$. We encounter an unexpected phenomenon when $v = \mathrm{ord}_p(a_p) < \frac{1}{2}$.

Definition 8.1. Put

$$\mathcal{C}_i(a, 1+T) := \begin{pmatrix} a & 1 \\ -\epsilon(p)\Phi_{p^i}(1+T) & 0 \end{pmatrix}.$$

We now put $\mathcal{H}_a^i(1+T) := \mathcal{C}_1(a, 1+T) \cdots \mathcal{C}_i(a, 1+T)$.

Definition 8.2. For an element a in the closed unit disc of $\mathbb{C}_p$, let $v := \mathrm{ord}_p(a) \geqslant 0$. When $v > 0$, let $k \in \mathbb{Z}^{\geqslant 1}$ be the smallest positive integer such that $v \geqslant p^{-k}/2$. We now let $v_m = v_m(a)$ be the upper left entry in the valuation matrix of $\mathcal{H}_a^m(\zeta_{p^{k+2}} - 1)$.

Given further an integer n, we now define two functions $q_n^*(v, v_2)$ for $* \in \{\sharp, \flat\}$.

When $\infty > v \geqslant p^{-k}/2$, we put $\delta := \min(v_2 - 2v, (p-1)p^{-k-2})$. Note that $\delta = 0$ when $v > p^{-k}/2$, since $v_2 = \mathrm{ord}_p(a^2 - \Phi_{p^2}(\zeta_{p^{k+2}}))$. We define

$$q_n^\sharp(v, v_2) := \begin{cases} (p^n - p^{n-1})kv + \left\lfloor \dfrac{p^{n-k}}{p+1} \right\rfloor & \text{if } n \not\equiv k \bmod 2 \\ (p^n - p^{n-1})((k-1)v + \delta) + \left\lfloor \dfrac{p^{n+1-k}}{p+1} \right\rfloor & \text{if } n \equiv k \bmod 2, \end{cases}$$

$$q_n^\flat(v, v_2) := \begin{cases} (p^n - p^{n-1})((k-1)v + \delta) + p\left\lfloor \dfrac{p^{n-k}}{p+1} \right\rfloor + p - 1 & \text{if } n \not\equiv k \bmod 2 \\ (p^n - p^{n-1})kv + p\left\lfloor \dfrac{p^{n-1-k}}{p+1} \right\rfloor + p - 1 & \text{if } n \equiv k \bmod 2. \end{cases}$$

Note that the tail terms

$$\left\lfloor \frac{p^{n-k}}{p+1} \right\rfloor \quad \text{and} \quad \left\lfloor \frac{p^{n+1-k}}{p+1} \right\rfloor$$

appearing in $q_n^\sharp(v,v_2)$ are equal to $q_{n-k}^\sharp$. For $n>k$, those for $q_n^\flat(v,v_2)$, i.e.,

$$p\left\lfloor\frac{p^{n-k}}{p+1}\right\rfloor+p-1 \quad\text{and}\quad p\left\lfloor\frac{p^{n-1-k}}{p+1}\right\rfloor+p-1,$$

are both $q_{n-k}^\flat$. For $v=\infty$, we define

$$q_n^*(\infty,v_2):=\lim_{v\to\infty}q_n^*(v,v_2).$$

Finally, for $v=0$, we similarly put

$$q_n^*(0,v_2):=\lim_{v\to 0}q_n^*(v,v_2)=\begin{cases}0 & \text{when } *=\sharp,\\ p-1 & \text{when } *=\flat.\end{cases}$$

(We use this seemingly strange adherence to the symbol v_2 simply for uniform notation.)

Definition 8.3. The *sporadic case* (for v and v_2) occurs if $v=0$ and $\mu_\sharp=\mu_\flat$ and $\lambda_\sharp=\lambda_\flat+p-1$, or if $v=p^{-k}/2$ and $v_2=2v(1+p^{-1}-p^{-2})$ and

$$n\not\equiv k \bmod 2 \quad\text{and}\quad \begin{cases}\mu_\sharp-\mu_\flat>v-2v/(p^3+p^2) & \text{or,}\\ \mu_\sharp-\mu_\flat=v-2v/(p^3+p^2) & \text{and}\quad \lambda_\sharp>\lambda_\flat,\end{cases}$$

or

$$n\equiv k \bmod 2 \quad\text{and}\quad \begin{cases}\mu_\sharp-\mu_\flat<2v/(p^3+p^2)-v & \text{or,}\\ \mu_\sharp-\mu_\flat=2v/(p^3+p^2)-v & \text{and}\quad \lambda_\sharp\leqslant\lambda_\flat.\end{cases}$$

Definition 8.4 (modesty algorithm). Given a in the closed unit disc, an integer n, integers $\lambda_\sharp$ and $\lambda_\flat$, and rational numbers $\mu_\sharp$ and $\mu_\flat$, choose $*\in\{\sharp,\flat\}$ via

$$*=\begin{cases}\sharp & \text{if } (p^n-p^{n-1})\mu_\sharp+\lambda_\sharp+q_n^\sharp(v,v_2)<(p^n-p^{n-1})\mu_\flat+\lambda_\flat+q_n^\flat(v,v_2),\\ \flat & \text{if } (p^n-p^{n-1})\mu_\flat+\lambda_\flat+q_n^\flat(v,v_2)<(p^n-p^{n-1})\mu_\sharp+\lambda_\sharp+q_n^\sharp(v,v_2).\end{cases}$$

Theorem 8.5. *Let f be a modular form of weight two which is a normalized eigenform for all T_n with eigenvalue a_n and p a good prime. Let $v=v(a_p)$ and $v_2=v_2(a_p)$* (via Definition 8.2). *For a character χ of $\mathbb{Z}_p^\times$ with order p^n, denote by $\tau(\chi)$ the Gauß sum. Let n be large enough that*

$$\operatorname{ord}_p\bigl(L_p^{\sharp/\flat}(f,\zeta_{p^n}-1)\bigr)=\mu_{\sharp/\flat}+\frac{\lambda_{\sharp/\flat}}{p^n-p^{n-1}},$$

and suppose that $n>k$ when $v>0$, and that we are not in the sporadic case. Then

$$\operatorname{ord}_p\left(\tau(\chi)\frac{L(f,\chi^{-1},1)}{\Omega_f}\right)=\mu_*+\frac{1}{p^n-p^{n-1}}\bigl(\lambda_*+q_n^*(v,v_2)\bigr),$$

and $*\in\{\sharp,\flat\}$ is chosen according to the modesty algorithm (Definition 8.4).

See Figure 1 in the introduction for an illustration of this theorem.

Proof. Let p be odd, since the other case is similar. Letting $\chi(\gamma) = \zeta_{p^n}$, the interpolation property implies

$$L_p(f, \alpha, \zeta_{p^n} - 1) = \frac{1}{\alpha^{n+1}} \frac{p^{n+1}}{\tau(\chi^{-1})} \frac{L(f, \chi^{-1}, 1)}{\Omega_f}.$$

Now $\alpha^{n+1} L_p(f, \alpha, \zeta_{p^n} - 1)$ has the desired p-adic valuation by Proposition 8.12 below and Theorem 2.14. □

For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, let $\mu^\sigma_{\sharp/\flat}$ and $\lambda^\sigma_{\sharp/\flat}$ be the μ- and λ-invariants of $L_p^{\sharp/\flat}(f^\sigma, T)$, and let $v^\sigma = v(a_p^\sigma)$ and $v_2^\sigma = v_2(a_p^\sigma)$. For $v^\sigma = 0$, put $q_n^\natural(v^\sigma, v_2^\sigma) = 0$ and let $\mu^\sigma_\natural$ and $\lambda^\sigma_\natural$ be the μ- and λ-invariants of $L_p(f^\sigma, \alpha, T)$.

Corollary 8.6. *Let* $p^{e_n} := Ш^{\mathrm{an}}(A_f/\mathbb{Q}_n)[p^\infty]$. *Suppose we are not in the sporadic case for any pair* v^σ, v_2^σ *with* $v^\sigma > 0$. *Then for* $n \gg 0$,

$$e_n - e_{n-1} = \sum_{\sigma \in \mathcal{G}_f} \mu^\sigma_*(p^n - p^{n-1}) + \lambda^\sigma_* + q_n^*(v^\sigma, v_2^\sigma) - r^{\mathrm{an}}_\infty(f^\sigma),$$

where $* \in \{\sharp, \flat\}$ *is chosen according to the modesty algorithm* (Definition 8.4), *except when* $v^\sigma = 0$ (and we are in the sporadic case), *in which case* $* := \natural$.

Proof. This follows from Theorem 8.5 in the same way that [Pollack 2003, Proposition 6.10] follows from [Pollack 2003, Proposition 6.9(3)]: The idea is to pick n large enough that $\mathrm{ord}_p(\#A_f(\mathbb{Q}_n)) = \mathrm{ord}_p(\#A_f(\mathbb{Q}_{n-1}))$, $L(A_f, \chi, 1) \neq 0$ for χ of order p^n, and $\mathrm{ord}_p(\mathrm{Tam}(A_f/\mathbb{Q}_n)) = \mathrm{ord}_p(\mathrm{Tam}(A_f/\mathbb{Q}_{n-1}))$. Noting that $R(A_f/\mathbb{Q}_n) = p^{r_n} R(A_f/\mathbb{Q}_{n-1})$ and by computing $D(\mathbb{Q}_n)$,

$$\begin{aligned} e_n - e_{n-1} &= \mathrm{ord}_p\Bigg(\prod_{\chi \text{ of order } p^n} \frac{L(A_f/\mathbb{Q}, \chi^{-1}, 1)}{\Omega_{A_f/\mathbb{Q}}}\Bigg) + p^{n-1}(p-1) \cdot \frac{n+1}{2} - r^{\mathrm{an}}_\infty \\ &= \mathrm{ord}_p\Bigg(\prod_{\chi \text{ of order } p^n} \tau(\chi) \frac{L(A_f/\mathbb{Q}, \chi^{-1}, 1)}{\Omega_{A_f/\mathbb{Q}}}\Bigg) - r^{\mathrm{an}}_\infty \\ &= \mathrm{ord}_p\Bigg(\prod_{\chi \text{of order } p^n} \tau(\chi) \prod_{\sigma \in \mathcal{G}_f} \frac{L(f^\sigma, \chi^{-1}, 1)}{\Omega_{f^\sigma}}\Bigg) - \sum_{\sigma \in \mathcal{G}_f} r^{\mathrm{an}}_\infty(f^\sigma). \end{aligned}$$

□

Corollary 8.7. *If* A_f *is an elliptic curve*, $\mathrm{ord}_p(L(A_f, 1)/\Omega_{A_f}) = 0$, $a_p \not\equiv 1 \bmod p$, *p is odd, and* $p \nmid \mathrm{Tam}(A_f/\mathbb{Q}_n)$, *then* $e_0 = e_1 = 0 = \mu_{\sharp/\flat} = \lambda_{\sharp/\flat} = r^{\mathrm{an}}_\infty$ *and the above formulas are valid for* $n \geqslant 2$.

Proof. We can pick $n = 0$ by [Kurihara 2002, Proposition 1.2] and the arguments of its proof, invoking [Greenberg 1999, Proposition 3.8] and Theorem 5.15. □

Definition 8.8 (the invariants $\mu_\pm$ and $\lambda_\pm$). Perrin-Riou, (resp. Greenberg, Iovita, and Pollack) defined invariants $\mu_\pm$ (resp. $\lambda_\pm$) as follows. Let p be a supersingular odd prime.[6] Let $(Q_n)_n \in \Lambda_n$ be a queue sequence. Let π be a generator of the maximal ideal of $\mathcal{O}$ such that $\pi^m = p$. When $Q_n \neq 0$, we define $\mu'(Q_n)$ to be the unique integer such that

$$Q_n \in (\pi)^{\mu'(Q_n)}\Lambda_n - (\pi)^{\mu'(Q_n)+1}\Lambda_n.$$

Further, we let $\lambda(Q_n)$ be the unique integer such that

$$\pi^{-\mu'(Q_n)}Q_n \bmod \pi \in \tilde{I}_n^{\lambda(Q_n)} - \tilde{I}_n^{\lambda(Q_n)+1},$$

where $\tilde{I}_n$ is the augmentation ideal of $\mathcal{O}/\pi\mathcal{O}[\Gamma_n]$. Finally, we put $\mu(Q_n) := m\mu'(Q_n)$. Then for even (resp. odd) n, $\mu(Q_n)$ stabilizes to a minimum constant value μ_+ (resp. μ_-). When $\mu_+ = \mu_-$, put

$$\lambda_+ := \lim_{n\to\infty} \lambda(Q_{2n}) - q_{2n}^{\flat} \quad \text{and} \quad \lambda_- := \lim_{n\to\infty} \lambda(Q_{2n+1}) - q_{2n+1}^{\sharp}.$$

Corollary 8.9. *When $\mu_\sharp$ and $\lambda_\sharp$ (resp. $\mu_\flat$ and $\lambda_\flat$) appear in the estimates of Theorem 8.5, they are the Iwasawa invariants of $\widehat{L}_p^\sharp$ (resp. $\widehat{L}_p^\flat$). When $\mu_\sharp = \mu_\flat$, we define $\mu_\pm$ and $\lambda_\pm$ via the queue sequences that gave rise to $L_p^\sharp$ and $L_p^\flat$, and have*

$$\mu_\sharp = \mu_+, \quad \lambda_\sharp = \lambda_+, \quad \mu_\flat = \mu_-, \quad \textit{and} \quad \lambda_\flat = \lambda_-.$$

Proof. The Kurihara terms $q_n^*(v, v_2)$ come from appropriate valuation matrices of $\mathcal{L}og_{\alpha,\beta}$ and $\widehat{\mathcal{L}og}_{\alpha,\beta}$, which are the same. Thus, the Iwasawa invariants of $\widehat{L}_p^{\sharp/\flat}$ and of $L_p^{\sharp/\flat}$ match. We can calculate the p-primary part of the special value in Theorem 8.5 using the appropriate queue sequences.[7] Since $\mu_+ = \mu_-$, we are a posteriori not in the sporadic case, so that our formulas match. □

Remarks in the elliptic curve case. For the remainder of this subsection, assume $A_f = E$ is an elliptic curve. Then in the supersingular case, Corollary 8.6 generalizes [Pollack 2003, Proposition 6.10], which works under the assumption $a_p = 0$. For an algebraic version of this Corollary 8.6 for supersingular primes, see [Kobayashi 2003, Theorem 10.9] in the case $a_p = 0$ and odd p, and [Sprung 2013, Theorem 3.13] for any odd supersingular prime.

Remark 8.10. These formulas are compatible with Perrin-Riou's [2003] formulas. Note that she assumes that p is odd, and that $\mu_+ = \mu_-$ or $a_p = 0$ in [Perrin-Riou 2003, Theorem 6.1(4)]; see also [Sprung 2013, Theorem 5.1] . Her invariants match ours, by Corollary 8.9. For $p = 2$, our results are compatible with [Kurihara and Otsuki 2006, Theorem 0.1(2)] (which determines the structure of the 2-primary

[6] Perrin-Riou makes the assumption that p is odd. For $p = 2$, one could define the $\mu_\pm$ and $\lambda_\pm$ in the same way but switch the signs so that they agree with the Iwasawa invariants of $L_p^\mp$ in the case $a_p = 0$.

[7] This has been explicitly done in an unpublished preprint of Greenberg, Iovita, and Pollack.

component of $Ш(A_f/\mathbb{Q}_n)$ under the assumption $a_2 = \pm 2$ in the elliptic curve case and other conditions, which force the Iwasawa invariants to vanish).

In the ordinary case, the estimate for $n \gg 0$ is

$$e_n - e_{n-1} = (p^n - p^{n-1})\mu + \lambda - r_\infty^{\mathrm{an}},$$

where μ and λ are the Iwasawa invariants of $L_p(E, \alpha, T)$. Thus, we obtain:

Corollary 8.11. *In the ordinary case, let λ be the λ-invariant of $L_p(E, \alpha, T)$. Then*

$$\lambda = \begin{cases} \lambda_\sharp & \text{when } \mu_\sharp < \mu_\flat \quad \text{or} \quad \mu_\sharp = \mu_\flat \text{ and } \lambda_\sharp < \lambda_\flat + p - 1, \\ \lambda_\flat & \text{when } \mu_\flat < \mu_\sharp \quad \text{or} \quad \mu_\flat = \mu_\sharp \text{ and } \lambda_\flat < \lambda_\sharp + 1 - p. \end{cases}$$

Tools for the proof of Theorem 8.5.

Proposition 8.12. *Suppose we have $(L^\sharp(T), L^\flat(T)) \in \mathcal{O}[\![T]\!]^{\oplus 2}$, where $\mathcal{O}$ is the ring of integers of some finite extension of $\mathbb{Q}_p$. Rewrite $L^\sharp(T) := p^{\mu_\sharp} \times P^\sharp(T) \times U^\sharp(T)$ for a distinguished polynomial $P^\sharp(T)$ with λ-invariant $\lambda_\sharp$ and a unit $U^\sharp(T)$. Note that $\mu_\sharp \in \mathbb{Q}$. Rewrite $L^\flat(T)$ similarly to extract $\mu_\flat$ and $\lambda_\flat$. Suppose we are not in the sporadic case. Let a and k be as in Definition 8.2, and e_n the left entry of the 1×2 valuation matrix of*

$$\big(L^\sharp(\zeta_{p^n} - 1), L^\flat(\zeta_{p^n} - 1)\big)\mathcal{H}_a^{n-1}(\zeta_{p^n} - 1).$$

Then for n large enough so that $n > k$ and $\operatorname{ord}_p(L^{\sharp/\flat}(\zeta_{p^n} - 1)) = \mu_{\sharp/\flat} + \dfrac{\lambda_{\sharp/\flat}}{p^n - p^{n-1}}$, we have

$$e_n = \mu_* + \frac{\lambda_*}{p^n - p^{n-1}} + \frac{q_n^*(v, v_2)}{p^n - p^{n-1}},$$

where $* \in \{\sharp, \flat\}$ is chosen according to the modesty algorithm.

Proof. From Lemma 8.14 and Lemma 8.15 below, it follows that the valuation matrix of the above expression is a product (of valuation matrices) of the form

$$\left[\mu_\sharp + \frac{\lambda_\sharp}{p^n - p^{n-1}}, \mu_\flat + \frac{\lambda_\flat}{p^n - p^{n-1}}\right] \begin{bmatrix} \dfrac{q_n^\sharp(v, v_2)}{p^n - p^{n-1}} & * \\ \dfrac{q_n^\flat(v, v_2)}{p^n - p^{n-1}} & * \end{bmatrix},$$

except when $v = p^{-k}/2$ and $v_2 = p^{-k}(1 + p^{-1} - p^{-2})$, in which case one of the two entries shown in the right valuation matrix is the actual entry, while the other is a lower estimate, see Lemma 8.15. The leading term of $P^{\sharp/\flat}(T)$ dominates by assumption, so the modesty algorithm (Definition 8.4) chooses the correct subindex. □

Lemma 8.13. *When $v > 0$ and $n > k+3$, the valuation matrix $[\mathcal{H}_a^{n-k-2}(\zeta_{p^n}-1)]$ is*

$$\begin{cases} \begin{bmatrix} p^{2-n}+p^{4-n}+p^{6-n}+\cdots+p^{-k-2} & v+p^{2-n}+\cdots+p^{-k-4} \\ v+p^{1-n}+\cdots+p^{-k-3} & p^{1-n}+\cdots+p^{-k-3} \end{bmatrix} & \text{if } n \equiv k \bmod 2, \\ \begin{bmatrix} v+p^{2-n}+\cdots+p^{-k-3} & p^{2-n}+\cdots+p^{-k-3} \\ p^{1-n}+\cdots+p^{-k-2} & v+p^{1-n}+\cdots+p^{-k-4} \end{bmatrix} & \text{if } n \not\equiv k \bmod 2. \end{cases}$$

Proof. Multiplication of valuation matrices and induction. □

Lemma 8.14. *With notation as above, assume $v = 0$. Then*

$$\bigl[\mathcal{H}_a^{n-1}(\zeta_{p^n}-1)\bigr] = \begin{bmatrix} 0 & 0 \\ p^{1-n} & p^{1-n} \end{bmatrix}.$$

Proof. Multiplication of valuation matrices. □

Given a real number x, recall that "$\geqslant x$" denotes an unknown quantity greater than or equal to x.

Lemma 8.15. *When $v > 0$ and $n > k$, we have*

$$(p^n - p^{n-1})[\mathcal{H}_a^{n-1}(\zeta_{p^n}-1)] = \begin{bmatrix} q_n^\sharp(v, v_2) & q_n^\sharp(v, v_2) - v \\ q_n^\flat(v, v_2) & q_n^\flat(v, v_2) - v \end{bmatrix},$$

$$\text{unless } v = \tfrac{1}{2}p^{-k} \quad \text{and} \quad v_2 = 2v(1+p^{-1}-p^{-2}).$$

When $v = \frac{1}{2}p^{-k}$ and $v_2 = 2v(1+p^{-1}-p^{-2})$, we have

$$(p^n - p^{n-1})[\mathcal{H}_a^{n-1}(\zeta_{p^n}-1)] = \begin{cases} \begin{bmatrix} \geqslant q_n^\sharp(v, v_2) & \geqslant q_n^\sharp(v, v_2) - v \\ q_n^\flat(v, v_2) & q_n^\flat(v, v_2) - v \end{bmatrix} & \text{when } n \equiv k \bmod 2, \\ \begin{bmatrix} q_n^\sharp(v, v_2) & q_n^\sharp(v, v_2) - v \\ \geqslant q_n^\flat(v, v_2) & \geqslant q_n^\flat(v, v_2) - v \end{bmatrix} & \text{when } n \not\equiv k \bmod 2. \end{cases}$$

Proof. We give the proof for the case $n \equiv k \bmod 2$ and $n \geqslant k+4$. (The case where $n \not\equiv k \bmod 2$ and $n \geqslant 5$ is similar, and the excluded cases are easier variants of these calculations.[8]) We have

$$\mathcal{H}_a^{n-1}(\zeta_{p^n}-1) = \mathcal{H}_a^{n-k-2}(\zeta_{p^n}-1)\mathcal{H}_a^{k+1}(\zeta_{p^n}^{p^{n-k-2}}-1),$$

[8] For $n = k+1$, we directly verify $[\mathcal{H}_a^k(\zeta_{p^{k+1}}-1)] = \left[\begin{smallmatrix} kv & (k-1)v \\ (k-1)v+p^{-k} & (k-2)+p^{-k} \end{smallmatrix}\right]$.

whose valuation matrix is the product of valuation matrices:

$$\left(\begin{bmatrix} \frac{p^{-k}}{p^2-1} & v+\frac{p^{-k-2}}{p^2-1} \\ v+\frac{p^{-k-1}}{p^2-1} & \frac{p^{-k-1}}{p^2-1} \end{bmatrix} - \begin{bmatrix} \frac{p^{2-n}}{p^2-1} & \frac{p^{2-n}}{p^2-1} \\ \frac{p^{1-n}}{p^2-1} & \frac{p^{1-n}}{p^2-1} \end{bmatrix}\right)\begin{bmatrix} v_{k+1} & v_k \\ kv+p^{-1-k} & (k-1)v+p^{-1-k} \end{bmatrix},$$

by Lemma 8.13, where the lower entries in the last valuation matrix are calculated by induction just as in Lemma 8.13 above. The first column of $[\mathcal{H}_a^{n-1}(\zeta_{p^n}-1)]$ is

$$\begin{bmatrix} \min(v_{k+1},(k+1)v+p^{-1-k}-p^{-k-2})+\frac{p^{-k}-p^{2-n}}{p^2-1} \\ \min(v_{k+1},(k-1)v+p^{-1-k})+v+\frac{p^{-k-1}-p^{1-n}}{p^2-1}, \end{bmatrix}.$$

as long as the two terms involved in $\min(\cdot,\cdot)$ are different.

If $2v>p^{-k}$, we have $v_{k+1}=(k-1)v+p^{-k}$, so the first column of $[\mathcal{H}_a^{n-1}(\zeta_{p^n}-1)]$ is

$$\begin{bmatrix} (k-1)v+p^{-k}+\frac{p^{-k}-p^{2-n}}{p^2-1} \\ kv+p^{-1-k}+\frac{p^{-k-1}-p^{1-n}}{p^2-1} \end{bmatrix}.$$

The difficult part is the case $2v=p^{-k}$. From the lemma below, we find that the expression for the lower term is the same as when $2v>p^{-k}$.

We claim that the upper term is the same as well (i.e., the minimum is v_{k+1}) when $v_2<p^{-k}(1+1/p-1/p^2)$, while the minimum is the other term when $v_2>p^{-k}(1+1/p-1/p^2)$. For $v_2\geqslant p^{1-k}$, this follows at once from the below lemma, since $v_{k+1}\geqslant(k-1)v+p^{1-k}$; so the real difficulty is when $p^{1-k}>v_2\geqslant p^{-k}$: Here, the lemma below tells us that $v_{k+1}=v_2+(k-1)p^{-k}/2$, from which we obtain our claim. Note that when $v_2=p^{-k}(1+1/p-1/p^2)$, we obtain our desired inequality. □

Lemma 8.16. *In the above situation, let $m\geqslant 2$. We then have $v_m=(m-2)v+v_2$ when $v_2<p^{1-k}$ and $v_m\geqslant(m-2)v+p^{1-k}$ if not.*

Proof. Explicit decomposition of the valuation matrix of $\mathcal{H}_a^k(\zeta_{p^n}^{p^{n-k-1}}-1)$. □

Acknowledgments

We are grateful to our advisors, Barry Mazur, Robert Pollack, and Joseph Silverman, for many inspiring conversations and many pieces of advice in the writing of this paper, and for making the author a (better) mathematician. We also thank Christian Wuthrich for a helpful conversation about regulators at the Iwasawa 2012 conference, and Tadashi Ochiai and Daniel Disegni for pointing out inaccuracies in an earlier version of this paper. We thank J. Pottharst for enlightening comments, and Diana

Davis and Maxime Bourque for help with typesetting the picture. We are also grateful to the anonymous referees and the typesetter for improving our paper.

References

[Abbes and Ullmo 1996] A. Abbes and E. Ullmo, "À propos de la conjecture de Manin pour les courbes elliptiques modulaires", *Compositio Math.* **103**:3 (1996), 269–286. MR Zbl

[Amice and Vélu 1975] Y. Amice and J. Vélu, "Distributions p-adiques associées aux séries de Hecke", pp. 119–131 in *Journées arithmétiques de Bordeaux* (Bordeaux, 1974), Astérisque **24-25**, Soc. Math. France, Paris, 1975. MR Zbl

[Balakrishnan et al. 2016] J. S. Balakrishnan, J. S. Müller, and W. A. Stein, "A p-adic analogue of the conjecture of Birch and Swinnerton-Dyer for modular abelian varieties", *Math. Comp.* **85**:298 (2016), 983–1016. MR Zbl

[Berger et al. 2004] L. Berger, H. Li, and H. J. Zhu, "Construction of some families of 2-dimensional crystalline representations", *Math. Ann.* **329**:2 (2004), 365–377. MR Zbl

[Breuil et al. 2001] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises", *J. Amer. Math. Soc.* **14**:4 (2001), 843–939. MR Zbl

[Coates and Sujatha 2000] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research Lectures on Mathematics **88**, Narosa, New Delhi, 2000. MR Zbl

[Colmez 2004] P. Colmez, "La conjecture de Birch et Swinnerton-Dyer p-adique", exposé 919, pp. 251–319 in *Séminaire Bourbaki 2002/2003*, Astérisque **294**, Soc. Math. France, Paris, 2004. MR Zbl

[Delbourgo 1998] D. Delbourgo, "Iwasawa theory for elliptic curves at unstable primes", *Compositio Math.* **113**:2 (1998), 123–153. MR Zbl

[Edixhoven 1991] B. Edixhoven, "On the Manin constants of modular elliptic curves", pp. 25–39 in *Arithmetic algebraic geometry* (Texel, 1989), edited by G. van der Geer et al., Progr. Math. **89**, Birkhäuser, Boston, 1991. MR Zbl

[Greenberg 1999] R. Greenberg, "Iwasawa theory for elliptic curves", pp. 51–144 in *Arithmetic theory of elliptic curves* (Cetraro, Italy, 1997), edited by C. Viola, Lecture Notes in Math. **1716**, Springer, Berlin, 1999. MR Zbl

[Greenberg 2001] R. Greenberg, "Iwasawa theory: past and present", pp. 335–385 in *Class field theory: its centenary and prospect* (Tokyo, 1988), edited by K. Miyake, Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo, 2001. MR Zbl

[Greenberg and Stevens 1994] R. Greenberg and G. Stevens, "On the conjecture of Mazur, Tate, and Teitelbaum", pp. 183–211 in *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture* (Boston, 1991), edited by B. Mazur and G. Stevens, Contemp. Math. **165**, American Mathematical Society, Providence, RI, 1994. MR Zbl

[Kato 2004] K. Kato, "p-adic Hodge theory and values of zeta functions of modular forms", pp. 117–290 in *Cohomologies p-adiques et applications arithmétiques, III*, edited by P. Berthelot et al., Astérisque **295**, Soc. Math. France, Paris, 2004. MR Zbl

[Kim 2008] B. D. Kim, "The algebraic functional equation of an elliptic curve at supersingular primes", *Math. Res. Lett.* **15**:1 (2008), 83–94. MR Zbl

[Kobayashi 2003] S.-i. Kobayashi, "Iwasawa theory for elliptic curves at supersingular primes", *Invent. Math.* **152**:1 (2003), 1–36. MR Zbl

[Kurihara 2002] M. Kurihara, "On the Tate–Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction, I", *Invent. Math.* **149**:1 (2002), 195–224. MR Zbl

[Kurihara and Otsuki 2006] M. Kurihara and R. Otsuki, "On the growth of Selmer groups of an elliptic curve with supersingular reduction in the $\mathbb{Z}_2$-extension of $\mathbb{Q}$", *Pure Appl. Math. Q.* **2**:2, part 2 (2006), 557–568. MR Zbl

[Lei 2014] A. Lei, "Factorisation of two-variable p-adic L-functions", *Canad. Math. Bull.* **57**:4 (2014), 845–852. MR Zbl

[Lei et al. 2010] A. Lei, D. Loeffler, and S. L. Zerbes, "Wach modules and Iwasawa theory for modular forms", *Asian J. Math.* **14**:4 (2010), 475–528. MR Zbl

[Loeffler and Zerbes 2013] D. Loeffler and S. L. Zerbes, "Wach modules and critical slope p-adic L-functions", *J. Reine Angew. Math.* **679** (2013), 181–206. MR Zbl

[Manin 1971] Ju. I. Manin, "Cyclotomic fields and modular curves", *Uspehi Mat. Nauk* **26**:6 (1971), 7–71. In Russian; translated in *Russian Math. Surveys* **26**:6 (1971), 7–78. MR Zbl

[Manin 1972] Ju. I. Manin, "Parabolic points and zeta functions of modular curves", *Izv. Akad. Nauk SSSR Ser. Mat.* **36**:1 (1972), 19–66. In Russian; translated in *Math. USSR-Izv.* **6**:1 (1972), 19–64. MR Zbl

[Manin 1973] Ju. I. Manin, "Periods of parabolic forms and p-adic Hecke series", *Mat. Sb. (N.S.)* **92 (134)**:3 (1973), 378–401. In Russian; translation in *Math. USSR-Sb.* **21**:3 (1973) 371–393. MR Zbl

[Mazur and Swinnerton-Dyer 1974] B. Mazur and P. Swinnerton-Dyer, "Arithmetic of Weil curves", *Invent. Math.* **25** (1974), 1–61. MR Zbl

[Mazur et al. 1986] B. Mazur, J. Tate, and J. Teitelbaum, "On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer", *Invent. Math.* **84**:1 (1986), 1–48. MR Zbl

[Perrin-Riou 1990] B. Perrin-Riou, "Théorie d'Iwasawa p-adique locale et globale", *Invent. Math.* **99**:2 (1990), 247–292. MR Zbl

[Perrin-Riou 1993] B. Perrin-Riou, "Fonctions L p-adiques d'une courbe elliptique et points rationnels", *Ann. Inst. Fourier* (*Grenoble*) **43**:4 (1993), 945–995. MR Zbl

[Perrin-Riou 1994] B. Perrin-Riou, "Théorie d'Iwasawa des représentations p-adiques sur un corps local", *Invent. Math.* **115**:1 (1994), 81–161. MR Zbl

[Perrin-Riou 2003] B. Perrin-Riou, "Arithmétique des courbes elliptiques à réduction supersingulière en p", *Experiment. Math.* **12**:2 (2003), 155–186. MR Zbl

[Pollack 2002] R. Pollack, "Tables of Iwasawa invariants of elliptic curves", 2002, Available at http://math.bu.edu/people/rpollack/Data/data.html.

[Pollack 2003] R. Pollack, "On the p-adic L-function of a modular form at a supersingular prime", *Duke Math. J.* **118**:3 (2003), 523–558. MR Zbl

[Pollack and Weston 2011] R. Pollack and T. Weston, "Mazur–Tate elements of nonordinary modular forms", *Duke Math. J.* **156**:3 (2011), 349–385. MR Zbl

[Pottharst 2012] J. Pottharst, "Cyclotomic Iwasawa theory of motives", submitted, 2012, Available at http://tinyurl.com/cyclotomic.

[Rohrlich 1984] D. E. Rohrlich, "On L-functions of elliptic curves and cyclotomic towers", *Invent. Math.* **75**:3 (1984), 409–423. MR Zbl

[Rubin 1991] K. Rubin, "The "main conjectures" of Iwasawa theory for imaginary quadratic fields", *Invent. Math.* **103**:1 (1991), 25–68. MR

[Skinner and Urban 2014] C. Skinner and E. Urban, "The Iwasawa main conjectures for GL_2", *Invent. Math.* **195**:1 (2014), 1–277. MR Zbl

[Sprung 2012] F. E. I. Sprung, "Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures", *J. Number Theory* **132**:7 (2012), 1483–1506. MR Zbl

[Sprung 2013] F. Sprung, "The Šafarevič–Tate group in cyclotomic $\mathbb{Z}_p$-extensions at supersingular primes", *J. Reine Angew. Math.* **681** (2013), 199–218. MR Zbl

[Sprung 2015] F. Sprung, "A formulation of p-adic versions of the Birch and Swinnerton-Dyer conjectures in the supersingular case", *Res. Number Theory* **1** (2015), Art. 17, 13. MR

[Stein and Wuthrich 2013] W. Stein and C. Wuthrich, "Algorithms for the arithmetic of elliptic curves using Iwasawa theory", *Math. Comp.* **82**:283 (2013), 1757–1792. MR Zbl

[Višik 1976] M. M. Višik, "Nonarchimedean measures associated with Dirichlet series", *Mat. Sb. (N.S.)* **99(141)**:2 (1976), 248–260. In Russian; translated in *Math. USSR-Sb.* **28**:2 (1976), 216–228. MR Zbl

[Washington 1982] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics **83**, Springer, New York, 1982. MR Zbl

[Wiles 1995] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. of Math.* (2) **141**:3 (1995), 443–551. MR Zbl

Communicated by Christopher Skinner
Received 2016-04-10 Revised 2016-12-16 Accepted 2017-01-13

fsprung@princeton.edu

School of Mathematics,
Institute for Advanced Study & Princeton University,
1 Einstein Dr, Princeton, NJ 08540, United States

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2017 is US $325/year for the electronic version, and $520/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 11 No. 4 2017