On the p-adic L-function of a modular form at a supersingular prime

Robert Pollack

September 5, 2001

1 Abstract

In this paper, we study the p-adic L-functions attached to a modular form $f = \sum a_n q^n$ at a supersingular prime and mainly the case when $a_p = 0$. It is known in many cases that these L-functions have infinitely many zeroes (in the "extended disc"). Therefore, the zeroes are not controlled by a single polynomial in the Iwasawa algebra as in the ordinary case. The main result of this paper (Theorem 7.1) describes how the zeroes of these L-functions are controlled by two polynomials and by two "gamma-like" functions each with a fixed infinite set of trivial zeroes. Also, asymptotic formulas for the p-part of the analytic size of the Tate-Shafarevich group of an elliptic curve in the cyclotomic direction are computed using this result. These formulas compare favorably with results established by Kurihara in [9] on the algebraic side.

Contents

2 Introduction

In the early 70's, Mazur and Swinnerton-Dyer constructed a p-adic L-function attached to a modular elliptic curve $E/\mathbf{Q}$ for each prime p of good, ordinary reduction (see [15]). This L-function can be represented as a power series in $\mathbf{Z}_p[[T]] \otimes \mathbf{Q}_p$ that p-adically interpolates the special values of the complex L-series of E twisted by various characters. Since this power series has bounded coefficients, by the p-adic Weierstrass preparation theorem, it has finitely many zeroes. The number of zeroes of the p-adic L-function and the slopes of these zeroes are conjecturally related to certain arithmetic invariants of E via the main conjecture (see Conjecture 3.2).

In [1] and [22] (see also [16]), the construction of p-adic L-functions was generalized to higher weight modular forms, to supersingular primes and to primes of bad reduction. At an ordinary prime for the modular form, the p-adic L-function is an element of $\mathcal{O}_K[[T]] \otimes K$ with K some finite extension of $\mathbf{Q}_p$ and therefore the L-function has finitely many zeroes. At a supersingular prime however the situation is quite different. The L-function can have unbounded coefficients and infinitely many zeroes. For each supersingular prime p, there are two p-adic L-functions corresponding to the two non-unit roots of $x^2 - a_p x + p^{k-1}$ where a_p is the eigenvalue of T_p acting on our modular form. When the slopes of the two roots are different, Mazur has shown that at least one of the two L-functions has infinitely many zeroes (Theorem 5.2). In the equal slope case, it is known that if a_p vanishes then one of the two L-functions has infinitely many zeroes (Theorem 5.4).

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

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

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

As observed by Perrin-Riou in [17], the interpolation property defining these L-functions forces G^+ to vanish at $\zeta_{p^{2n}} - 1$ and G^- to vanish at $\zeta_{p^{2n-1}} - 1$ for all $n \geq 1$ where ζ_m is an m-th root of unity (see Theorem 5.4). (There is a change in parity for $p = 2$.) Hence the power series G^+ and G^- have an infinite set of "trivial" zeroes. Note that these zeroes are even independent of E.

We then go on to construct p-adic power series Φ^+ and Φ^- that vanish precisely at the forced zeroes of G^+ and G^- respectively (see Lemma 6.2). These power series are constructed as an infinite product of cyclotomic polynomials. The next step is to examine the functions $g^+ := G^+/\Phi^+$ and $g^- := G^-/\Phi^-$. The relation of Φ^+ and Φ^- to $L_p(E, \alpha, T)$ can be compared to the relation of the gamma function to the Riemann zeta function. The gamma function forces the zeta function to vanish at all of the negative even integers and the interesting zeroes of the zeta function are discovered only after these zeroes are removed from consideration. In our setting, we divide $G^{\pm}$ by $\Phi^{\pm}$ respectively, hoping to uncover its more interesting zeroes. For this reason, we refer to Φ^{+} and Φ^{-} as gamma-like functions. The properties of these functions are studied in section 6.2.

By studying the rate of growth of $G^{\pm}$ and $\Phi^{\pm}$, one sees that $g^{\pm}$ is bounded and actually has integral coefficients. Hence, $g^{\pm}$ has only finitely many zeroes and $G^{\pm}$ vanishes at only finitely many places apart from its fixed set of forced roots. The integrality of g^{+} and g^{-} is the main result of the paper and is proved in Theorem 7.1.

Hence

$$L_p(E,\alpha,T) = g^{+}(T)\cdot\Phi^{+}(T) + g^{-}(T)\cdot\Phi^{-}(T)\cdot\alpha$$

with $g^{\pm} \in \mathbf{Z}_p[[T]]$. In this way, the infinite set of zeroes of $L_p(E,\alpha,T)$ are controlled by a finite set of arithmetically interesting zeroes together with an infinite set of trivial zeroes. (Note that it is not being claimed that it is clear how to determine the zeroes of $L_p(E,\alpha,T)$ from those of g^{+} and g^{-}. However, for example, from the information of the Newton polygons of g^{+} and g^{-}, one can determine the Newton polygon of $L_p(E,\alpha,T)$ which does give quite a lot of information about the zeroes of the L-function.)

Let $\mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. The above result can be used to study the analytic invariants of an elliptic curve E along this extension. This is done in section 8. Via Kato's Euler system, it is now know that $E(\mathbf{Q}_\infty)$ is a finitely generated group (see [19, Corollary 8.2]). By the Birch and Swinnerton-Dyer conjecture, this should translate into $E(\mathbf{Q}_\infty)$ having finite analytic rank. The above result implies that its analytic rank is bounded by the sum of the λ-invariants of g^{+} and g^{-}. (The number of zeroes of an integral p-adic power series is equal to its λ-invariant.) This bound can be tightened to just the number of p-cyclotomic zeroes of g^{+} and g^{-} (see Corollary 8.5).

Let $\mathbf{Q}_n$ be the unique subextension of $\mathbf{Q}_\infty$ of degree p^n. Using Theorem 7.1 we compute asymptotic formulas for the analytic size of $\text{Ш}(E/\mathbf{Q}_n)_{p^\infty}$ (i.e. the size predicted by the Birch and Swinnerton-Dyer conjecture). This is done in Proposition 8.12. In the ordinary case, these formulas involve the Iwasawa invariants of the p-adic L-function (see section 3.2). In the supersingular case, these invariants do not make any sense. Instead, the formulas in this case are based upon the Iwasawa invariants of g^{+} and g^{-} which do exist since these power series have bounded coefficients.

The case where $p \nmid \frac{L(E,1)}{\Omega_E}$ has been studied deeply by Kurihara in [9]. By using Kato's Euler system, he has managed to produce exact formulas for the algebraic size of $\text{Ш}(E/\mathbf{Q}_n)_{p^\infty}$ along the cyclotomic $\mathbf{Z}_p$ extension of $\mathbf{Q}$. Under this hypothesis, the Iwasawa invariants of g^{+} and g^{-} are all zero and the asymptotic formulas derived below compare favorably with those of Kurihara (see Proposition 8.15).

3 A motivating example

For an ordinary prime p of an elliptic curve over $\mathbf{Q}$, Iwasawa theory yields asymptotic formulas for the growth of the p-part of the Tate-Shafarevich group in the cyclotomic direction. The Birch and Swinnerton-Dyer conjecture also predicts asymptotic formulas for the size of this group in terms of the Iwasawa invariants of the p-adic L-series of this elliptic curve. Fortunately these two formulas take on the same shape and agree perfectly via the main conjecture.

In this section, we derive these asymptotic formulas both on the algebraic side and on the analytic side and show how they compare. This calculation is performed in anticipation of the analytic calculations done in section 8.3 in the supersingular case where the analogous algebraic formulas are not currently known. We begin by reviewing Iwasawa theory in the context of class numbers and then move on to elliptic curves.

3.1 Class numbers

In the late fifties, Iwasawa began an intensive study of how class numbers vary in certain towers of number fields, namely in $\mathbf{Z}_p$-extensions. Precisely, let p be a prime number and let K be a number field. Then a $\mathbf{Z}_p$-extension of K is simply an extension L such that $\mathrm{Gal}(L/K) \simeq \mathbf{Z}_p$. Denote by K_n the unique subfield of L with degree p^n over K. Iwasawa discovered that the p-part of the class numbers of the K_n grow systematically along this tower and gave asymptotic formulas for the p-part of these numbers. If h_n is the class number of K_n then Iwasawa established that for n large enough,

$$\mathrm{ord}_p(h_n) = \mu p^n + \lambda n + \nu$$

for some non-negative constants μ, λ and ν (see [7]).

Iwasawa's approach was to package together the p-part of the class group at each finite level into a module over a certain large ring. The structure theory for modules over this ring is fairly simple – reminiscent of the structure theory of modules over a PID. The final step is then to descend information about this large module to the K_n to be able to make deductions about class numbers.

More precisely, let A_n be the p-Sylow subgroup of the ideal class group of K_n and let $A_\infty := \varprojlim A_n$ where the limit is taken under the norm maps. Since A_n is a finite p-group, it can be considered as a $\mathbf{Z}_p$-module. Then if we denote $\Gamma = \mathrm{Gal}(L/K)$ and $\Gamma_n = \mathrm{Gal}(L/K_n)$, we can view A_n as a $\mathbf{Z}_p[\Gamma/\Gamma_n]$-module. Hence, A_∞ is a module over $\mathbf{Z}_p[[\Gamma]] \simeq \varprojlim_n \mathbf{Z}_p[\Gamma/\Gamma_n]$ the completed group algebra of Γ which we will denote by Λ. This is the large ring referred to above and is non-canonically isomorphic to $\mathbf{Z}_p[[T]]$.

Any finitely generated module over Λ is pseudo-isomorphic to the direct sum of a free Λ-module and a torsion Λ-module. Here pseudo-isomorphic means there exists a map having finite kernel and cokernel. Our Λ-module A_∞ is indeed finitely generated and hence we have

$$A_\infty \sim (\oplus_i \, \Lambda/f_i^{n_i}) \oplus \Lambda^r \tag{1}$$

for $f_i \in \Lambda$ where $\sim$ denotes pseudo-isomorphism.

To complete this picture, we must now connect A_∞ to A_n for each n. We will make this connection in the special case where there is only one prime of K sitting over p and where this prime is totally ramified in L. For a Λ-module X, let X_{Γ_n} denote the Γ_n-coinvariants of X (i.e. the maximal quotient on which Γ_n acts trivially). Then the natural map

$$(A_\infty)_{\Gamma_n} \to A_n$$

is an isomorphism for all n. This will allow us to transfer information between A_∞ and the A_n. (Without any assumptions on the primes sitting over p, the group $(A_\infty)_{\Gamma_n}$ could be infinite and hence the above map would not even be a pseudo-isomorphism.)

Remaining under the same hypotheses on p, let us apply this result to the case where $n = 0$. Then the Γ-coinvariants of A_∞ are isomorphic to A_0 and hence finite. From this we can conclude that A_∞ is Λ-torsion and the r in equation (1) is zero. (The Γ-coinvariants of a free Λ-module are infinite.)

For ease of exposition, let us assume that the f_i are pairwise relatively prime. Then $A_\infty \sim \Lambda/f$ where $f = \prod_i f_i$. Therefore, the size of A_n differs from the size of $(\Lambda/f)_{\Gamma_n}$ by a constant bounded independent of n. We have converted the question of computing class numbers to computing the size of the Γ_n-coinvariants of a certain torsion Λ-module! The later is easy to do and we will provide the details of this calculation in what follows (see [5]).

Pick an isomorphism of Λ with $\mathbf{Z}_p[[T]]$ and write the image of f as $f(T)$. Then by the p-adic Weierstrass preparation theorem, we can write

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

where μ is a non-negative integer, $P(T)$ is a distinguished polynomial of degree λ and $U(T)$ is a unit power series. (A distinguished polynomial $P(T)$ is of the form $x^\lambda + a_{\lambda-1}x^{\lambda-1} + \cdots + a_0$ where $p \mid a_i$.)

Let $\omega_n = (1+T)^{p^n} - 1$. Then Λ/ω_n is a free $\mathbf{Z}_p$-module and we can view $(\Lambda/f)_{\Gamma_n}$ as the cokernel of multiplication by f on Λ/ω_n. The size of $(\Lambda/f)_{\Gamma_n}$ is then the p-part of the determinant of this map. Since multiplication by T has eigenvalues $\zeta - 1$ for ζ a p^n-th root of unity, the eigenvalues of multiplication by f are just $f(\zeta - 1)$ where again $\zeta^{p^n} = 1$. Hence,

$$\#\,(\Lambda/f)_{\Gamma_n} \quad \text{and} \quad \prod_{\zeta^{p^n}=1} f(\zeta - 1)$$

differ by a p-adic unit. (Note that since $(\Lambda/f)_{\Gamma_n} \simeq \mathbf{Z}_p[[T]]/(f(T), \omega_n)$ is finite, we must have that $f(T)$ and ω_n are relatively prime and hence $f(\zeta - 1) \neq 0$.)

The valuation of this product is easily calculated in terms of the μ and λ-invariants of f (see section 8.3) yielding

$$\operatorname{ord}_p(h_n) = \mu p^n + \lambda n + \nu$$

for n large enough and ν some constant independent of n.

Note that if either μ or λ is non-zero then the class numbers in this tower grow without bound. Also, if $p \nmid h_0$ then $(A_\infty)_{\Gamma_0} \simeq A_0 = 0$. By a compact version of Nakayama's lemma, we can conclude that $A_\infty = 0$ and hence $h_n = 0$ for all n.

3.2 Iwasawa theory of elliptic curves at ordinary primes

In the early seventies, Mazur applied Iwasawa's ideas to the arithmetic of elliptic curves. Instead of studying class numbers, Mazur studied both the growth of the Mordell-Weil group and the p-part of the Tate-Shafarevich group of an elliptic curve along $\mathbf{Z}_p$-extensions.

Let E be an elliptic curve over $\mathbf{Q}$ and let $\mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$ with $\mathbf{Q}_n$ the unique subextension of degree p^n. For K any algebraic extension of $\mathbf{Q}$, denote by $\mathrm{Sel}(K, E_{p^\infty})$ the p-primary Selmer group of E over K. This group fits into the following exact sequence:

$$0 \to E(K) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to \mathrm{Sel}(K, E_{p^\infty}) \to Ш(E/K)_{p^\infty} \to 0.$$

In order to analyze $E(\mathbf{Q}_n)$ and $Ш(E/\mathbf{Q}_n)_{p^\infty}$, Mazur studied the compact Λ-module $\mathrm{Sel}(\mathbf{Q}_\infty, E_{p^\infty})^\vee$. Here $M^\vee = \mathrm{Hom}(M, \mathbf{Q}_p/\mathbf{Z}_p)$ is the Pontrjagin dual. He proved a control theorem relating $\mathrm{Sel}(\mathbf{Q}_\infty, E_{p^\infty})$ to $\mathrm{Sel}(\mathbf{Q}_n, E_{p^\infty})$. Namely, the natural map

$$\mathrm{Sel}(\mathbf{Q}_n, E_{p^\infty}) \to \mathrm{Sel}(\mathbf{Q}_\infty, E_{p^\infty})^{\Gamma_n}$$

has finite kernel and cokernel with sizes bounded independent of n.

From this control theorem one can deduce that $\mathrm{Sel}(\mathbf{Q}_\infty, E_{p^\infty})^\vee$ is finitely generated as a Λ-module. However, we cannot directly conclude that it is Λ-torsion as in the case of ideal class groups. There we relied on the fact that ideal class groups are always finite. If E has positive rank over $\mathbf{Q}$ then $\mathrm{Sel}(\mathbf{Q}, E_{p^\infty})$ is infinite.

In [14], Mazur conjectured that $\mathrm{Sel}(\mathbf{Q}_\infty, E_{p^\infty})^\vee$ is always Λ-torsion when E has good ordinary reduction at p. This remained an open question until Kato's construction of an Euler system for the Tate module of E (see [8]). From this Euler system, one can deduce that $E(\mathbf{Q}_\infty)$ is a finitely generated group and that $\mathrm{Sel}(\mathbf{Q}_\infty, E_{p^\infty})^\vee$ is indeed Λ-torsion. From this very deep result one can prove the following theorem.

Theorem 3.1. *(Kato - Mazur - Rohrlich) Let $E/\mathbf{Q}$ be an elliptic curve with good, ordinary reduction at some prime number p. Then $E(\mathbf{Q}_\infty)$ is a finitely generated group. Furthermore, assume that $Ш(E/\mathbf{Q}_n)_{p^\infty}$ is finite for all n and let $\#Ш(E/\mathbf{Q}_n)_{p^\infty} = p^{e_n}$. Then for n large enough,*

$$e_n = \mu p^n + \lambda n + \nu$$

for some non-negative constants μ, λ and ν.

Once it is known that $\mathrm{Sel}(\mathbf{Q}_\infty, E_{p^\infty})^\vee$ is Λ-torsion, the proof of this theorem follows in the same manner as in the last section with the added complication that the Γ_n-coinvariants of this Λ-module could be infinite. Again, assume that the torsion module $\mathrm{Sel}(\mathbf{Q}_\infty, E_{p^\infty})^\vee$ has the form Λ/f for some $f \in \Lambda$. We then have to worry about the zeroes of f in the form $\zeta - 1$ where ζ is a p-power root of unity. Call such zeroes p-cyclotomic.

As before let

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

where μ is a non-negative integer, $P(T)$ is a distinguished polynomial of degree λ and $U(T)$ is a unit power series. Write P as $P_{MW} \cdot P_{Ш}$ where P_{MW} vanishes precisely at the p-cyclotomic zeroes of P. Let λ_{MW} be the degree of P_{MW} and let $\lambda_{Ш}$ be the degree of $P_{Ш}$. Then for n large enough so that P_{MW} divides $(1+T)^{p^n} - 1$ we have,

$$(\Lambda/f)_{\Gamma_n} \sim (\Lambda/P_{MW})_{\Gamma_n} \oplus (\Lambda/P_{Ш})_{\Gamma_n} \sim (\Lambda/P_{MW}) \oplus (\Lambda/P_{Ш})_{\Gamma_n}.$$

From the assumption that $Ш(E/\mathbf{Q}_n)_{p^\infty}$ is finite and from Mazur's control theorem, we can conclude that

$$\Lambda/P_{MW} \simeq (E(\mathbf{Q}_n) \otimes \mathbf{Q}_p/\mathbf{Z}_p)^\vee$$

and hence the rank of E over $\mathbf{Q}_n$ equals λ_{MW}. Furthermore,

$$(\Lambda/P_{Ш})_{\Gamma_n} \quad \text{and} \quad Ш(E/\mathbf{Q}_n)_{p^\infty}$$

differ in size by a constant that is bounded independent of n. Hence, the rank of $E(\mathbf{Q}_\infty)$ is equal to λ_{MW} and μ and λ in the above theorem are equal to μ and $\lambda_{Ш}$.

3.3 An analytic approach

We will approach the question of the growth of the p-part of the Tate-Shafarevich group using analytic methods to derive a guess at the above formulas without using Iwasawa theory. That is, we will compute the size of $Ш(E/\mathbf{Q}_n)_{p^\infty}$ predicted by the Birch and Swinnerton-Dyer conjecture. In the end, these analytic formulas will compare well with Theorem 3.1. This method will be applied in section 8.3 to derive similar analytic formulas in the supersingular case where algebraic formulas are not yet known.

Again, let E be an elliptic curve over $\mathbf{Q}$ and p some ordinary prime for E. If the complex L-series $L(E/\mathbf{Q}_n, s)$ vanishes to order r^{an} at 1, we define

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

where $D(\cdot)$ is the discriminant, $R(E/\cdot)$ is the regulator, $\mathrm{Tam}(E/\cdot)$ is the product of the Tamagawa numbers, $\Omega_{E/\mathbf{Q}_n}$ is the real period over $\mathbf{Q}_n$ and r_n is the rank of $E(\mathbf{Q}_n)$, We then define,

$$e_n^{\mathrm{an}} := \mathrm{ord}_p(\#Ш^{\mathrm{an}}(E/\mathbf{Q}_n)).$$

A theorem of Rohrlich (see Theorem 7.11) states that $L(E/\mathbf{Q}, \chi, 1) = 0$ for only finitely many Dirichlet characters χ of p-power order. Since,

$$L(E/\mathbf{Q}_n, s) = \prod_\chi L(E/\mathbf{Q}, \chi, s)$$

where the product is taken over all χ corresponding to $\mathbf{Q}_n/\mathbf{Q}$, we must have that the order of vanishing of $L(E/\mathbf{Q}_n, s)$ at $s = 1$ stabilizes for n large. Furthermore, by [20, Theorem 3], $E(\mathbf{Q}_\infty)^{\mathrm{tor}}$ is finite. By BSD, this should imply that $E(\mathbf{Q}_\infty)$ is finitely generated which we will assume for this calculation. Denote by r the stable value of the r_n. Choose n so large that:

1. $\mathrm{ord}_{s=1} L(E/\mathbf{Q}_{n+1}, s) = \mathrm{ord}_{s=1} L(E/\mathbf{Q}_n, s)$
2. $E(\mathbf{Q}_{n+1}) = E(\mathbf{Q}_n)$
3. $\mathrm{Tam}(E/\mathbf{Q}_{n+1}) = \mathrm{Tam}(E/\mathbf{Q}_n)$.

Then,

$$\frac{\#\text{Ш}^{\mathrm{an}}(E/\mathbf{Q}_{n+1})}{\#\text{Ш}^{\mathrm{an}}(E/\mathbf{Q}_n)} = \left(\prod_\chi \frac{L(E/\mathbf{Q}, \chi, 1)}{\Omega_{E/\mathbf{Q}}}\right) \cdot \sqrt{\frac{D(\mathbf{Q}_{n+1})}{D(\mathbf{Q}_n)}} \cdot \frac{R(E/\mathbf{Q}_n)}{R(E/\mathbf{Q}_{n+1})} \tag{2}$$

where the product is taken over all χ corresponding to $\mathbf{Q}_{n+1}/\mathbf{Q}$ but not to $\mathbf{Q}_n/\mathbf{Q}$.

The regulators $R(E/\mathbf{Q}_n)$ do not stabilize even though $E(\mathbf{Q}_n) = E(\mathbf{Q}_{n+1})$ for n large since the regulators are computed by height functions relative to different fields. For any finite extension of number fields L/K, if $E(K) = E(L)$ we have (see [21, pg. 233])

$$\frac{R(E/L)}{R(E/K)} = [L : K]^{\mathrm{rank}(E(K))}$$

and hence the quotient of the regulators in (2) is just p^r.

The second term in (2) is readily calculated using the conductor-discriminant formula. Namely, there are $p^{n-1}(p-1)$ characters each of conductor p^{n+1} corresponding to $\mathbf{Q}_{n+1}$ and not to $\mathbf{Q}_n$. (When $p = 2$ these characters are of conductor 2^{n+2}.) Hence,

$$\mathrm{ord}_p\left(\sqrt{\frac{D(\mathbf{Q}_{n+1})}{D(\mathbf{Q}_n)}}\right) = p^{n-1}(p-1) \cdot \frac{n+1}{2}. \tag{3}$$

Analyzing the first term in (2) is a more difficult problem. We are interested in the p-part of $L(E/\mathbf{Q}, \chi, 1)/\Omega_E$ where χ is a character of both p-power order and conductor. This is the moment where the p-adic L-function of E enters the game. There exists a p-adic power series in $\mathbf{Z}_p[[T]] \otimes \mathbf{Q}_p$ interpolating the p-part of these twisted L-values. More precisely, fix an embedding of $\overline{\mathbf{Q}}$ into $\overline{\mathbf{Q}}_p$ and view χ as a character with values in $\overline{\mathbf{Q}}_p$. Let α be the unit root of

$x^2 - a_p x + p$ where $a_p = p + 1 - \#\widetilde{E}(\mathbf{F}_p)$. Then there exists a unique power series $L_p(E,T) \in \mathbf{Z}_p[[T]] \otimes \mathbf{Q}_p$ (conjecturally in $\mathbf{Z}_p[[T]]$) such that

$$L_p(E, \zeta_{p^n} - 1) = \frac{1}{\alpha^{n+1}} \cdot \frac{p^{n+1}}{\tau(\overline{\chi})} \cdot \frac{L(E/\mathbf{Q}, \chi, 1)}{\Omega_E} \tag{4}$$

where $n \geq 1$, $\tau(\chi)$ is a Gauss sum and $\zeta_{p^n} = \chi(1+p)$. (When $p = 2$ the exponent of α is $n+2$.) The power series $L_p(E,T)$ is the p-adic L-function of E. The proof of its existence (in a much more general setting) is recalled in section 4.

We have now reduced the question of studying the p-part of $L(E/\mathbf{Q}, \chi, 1)/\Omega_E$ over varying χ to analyzing a p-adic power series evaluated at $\zeta_{p^n} - 1$ as n grows. The later is easy to do via the p-adic Weierstrass preparation theorem. (Note the similarities to the calculations in the previous section!) Write,

$$L_p(E,T) = p^{\mu^{\text{an}}} \cdot P^{\text{an}}(T) \cdot U^{\text{an}}(T)$$

where $\mu^{\text{an}} \in \mathbf{Z}$, $P^{\text{an}}(T)$ is a distinguished polynomial of degree λ^{an} and $U^{\text{an}}(T)$ is a unit power series.

Then for n large enough, $\text{ord}_p(P^{\text{an}}(\zeta_{p^n} - 1)) = \mu^{\text{an}} + \frac{\lambda^{\text{an}}}{p^{n-1}(p-1)}$ as the leading term dominates. Hence,

$$\text{ord}_p\left(\prod L_p(E, \zeta_{p^n} - 1)\right) = \mu^{\text{an}} \cdot p^{n-1}(p-1) + \lambda^{\text{an}}$$

where the product is taken over all primitive p^n-th roots of unity. Also, since $\tau(\chi) \cdot \tau(\overline{\chi}) = \pm p^{n+1}$, we have

$$\text{ord}_p\left(\prod_{\chi} \frac{L(E/\mathbf{Q}, \chi, 1)}{\Omega_{E/\mathbf{Q}}}\right) = \mu^{\text{an}} \cdot p^{n-1}(p-1) + \lambda^{\text{an}} - p^{n-1}(p-1) \cdot \frac{n+1}{2}. \tag{5}$$

Substituting these quantities back into equation (2) yields,

$$e_{n+1}^{\text{an}} - e_n^{\text{an}} = \mu^{\text{an}} \cdot p^{n-1}(p-1) + \lambda^{\text{an}} - r$$

(even for $p = 2$) and hence for n large,

$$e_n^{\text{an}} = \mu^{\text{an}} \cdot p^n + (\lambda^{\text{an}} - r) \cdot n + \nu.$$

These analytic equations parallel those in Theorem 3.1 with $\mu = \mu^{\text{an}}$ and $\lambda = \lambda^{\text{an}} - r$. Let us make a more precise comparison.

Write $P^{\text{an}} = P^{\text{an}}_{MW} \cdot P^{\text{an}}_{\text{Ш}}$ where P^{an}_{MW} vanishes precisely at the p-cyclotomic zeroes of P. Let λ^{an}_{MW} be the degree of P^{an}_{MW} and $\lambda^{\text{an}}_{\text{Ш}}$ be the degree of $P^{\text{an}}_{\text{Ш}}$. From the interpolation property defining the p-adic L-series, each p-cyclotomic zero forces $L(E, \chi, 1) = 0$ for some χ. By BSD this should relate to some Mordell-Weil group being infinite. In fact, a p-adic BSD would imply that $r = \lambda^{\text{an}}_{MW}$. Under such an assumption, we would then have

$$e_n^{\text{an}} = \mu^{\text{an}} \cdot p^n + \lambda^{\text{an}}_{\text{Ш}} \cdot n + \nu$$

for n large.

But now, conjecturally, these constants μ^{an} and $\lambda_{Ш}^{\text{an}}$ should be the same as μ and $\lambda_{Ш}$ appearing in Theorem 3.1! The following conjecture gives a theoretical framework that explains this connection plus a great deal more. Note that if X is a torsion Λ-module pseudo-isomorphic to $\oplus_i \Lambda/f_i$, then $f := \prod_i f_i$ is called its characteristic power series.

Conjecture 3.2. (The Main Conjecture) Let E be an elliptic curve over $\mathbf{Q}$ and let p be an ordinary prime for E. Then the characteristic power series of $\text{Sel}(\mathbf{Q}_\infty, E_{p^\infty})^\vee$ equals the p-adic L-function of E up to an element of $\Lambda^\times$.

This conjecture would then imply that $\mu = \mu^{\text{an}}$, $\lambda_{MW} = \lambda_{MW}^{\text{an}}$ and $\lambda_{Ш} = \lambda_{Ш}^{\text{an}}$. One can think of the characteristic power series of $\text{Sel}(\mathbf{Q}_\infty, E_{p^\infty})^\vee$ as an algebraic p-adic L-series since it is defined using purely algebraic methods. Great progress has been made towards proving this conjecture via Kato's Euler system. It is now known that the algebraic p-adic L-series divides the analytic p-adic L-series up to a power of p. (See [19, Theorem 8.7])

3.4 The supersingular case

When p is supersingular for E the situation on the algebraic side and the analytic side are both less favorable. On the algebraic side, $\text{Sel}(\mathbf{Q}_\infty, E_{p^\infty})^\vee$ is no longer Λ-torsion and Mazur's control theorem fails. On the analytic side, there exist two conjugate p-adic L-functions, but neither are elements of $\mathbf{Z}_p[[T]] \otimes \mathbf{Q}_p$. They both have infinitely many zeroes (see Theorem 5.4) and lack well-defined μ and λ invariants.

On the algebraic side, Kurihara has proved an analogue of Theorem 3.1 for p supersingular in the special case when $p \nmid L(E,1)/\Omega_E$. Kurihara first studies a submodule of $\text{Sel}(\mathbf{Q}_\infty, E_{p^\infty})$ defined by putting a harsher local condition at p. This submodule is in fact Λ-cotorsion and obeys a certain control theorem. (In his special case the submodule is actually zero.) Then Kurihara uses Kato's Euler system to analyze the quotient of the two modules yielding formulas for the size of the p-part of $Ш(E/\mathbf{Q}_n)$.

On the analytic side, the main result of this paper (Theorem 7.1) allows one to make sense of two μ and λ invariants attached to the p-adic L-functions of E. In a calculation analogous to the one done in the last section (see section 8.3), we calculate asymptotic formulas for the p-part of $\#Ш^{\text{an}}(E/\mathbf{Q}_n)$ in terms of these μ and λ invariants. In the case when $p \nmid L(E,1)/\Omega_E$, all of these invariants are zero and the formulas derived agree with Kurihara's.

Still needed to obtain a more complete picture in the supersingular case, would be a general version of Theorem 3.1 (whose formulas depend upon the two μ and λ invariants constructed in this paper).

4 p-adic L-functions of modular forms

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

In this section, we will first construct this distribution out of modular symbols. Then we will describe what it means to integrate against such a distribution. (The distribution may be unbounded and naive Riemann sums will not necessarily converge.) Having integration in hand, we can define the p-adic L-function and discuss its analytic properties including its rate of growth. We will then describe a power series representation of the p-adic L-function (as used in section 3.3). Finally, we will provide a description of the p-adic L-function via a certain interpolation property. For more details see [1],[16] and [22].

4.1 Distributions attached to modular forms

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

Define the periods of f by

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

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

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

and fix the positive and negative parts of η by

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

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

We have the following theorem.

Theorem 4.1. *There exist two non-zero complex numbers Ω_f^+ and Ω_f^- such that*

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

Proof. [6, Theorem 3.5.4] □

Define the modular symbols of f by

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

We will build our distribution out of the data of these modular symbols. First we set some notation. Fix a prime number p and an embedding of $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$. Let $\mathrm{ord}_p(\cdot)$ be the associated valuation at p normalized so that $\mathrm{ord}_p(p) = 1$. Let v be the prime of $K(f)$ over p and let $K := K(f)_v$. Call a root α of $x^2 - a_p x + \varepsilon(p)p^{k-1} = 0$ *allowable* if $\mathrm{ord}_p(\alpha) < k-1$. Finally, let $\mathbf{Z}_{p,M}^\times := \mathbf{Z}_p^\times \times (\mathbf{Z}/M\mathbf{Z})^\times$ for M prime to p. (This $(\mathbf{Z}/M\mathbf{Z})^\times$ factor will allow for twists of the modular form by a character of conductor M.)

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

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

where a is prime to Mp. The following proposition expresses the additivity property of $\mu_{f,\alpha}^{\pm}$.

Proposition 4.2.

$$\mu_{f,\alpha}^{\pm}(P, a + p^n\mathbf{Z}_{p,M}) = \sum_{k=0}^{p-1} \mu_{f,\alpha}^{\pm}(P, a + kp^n + p^{n+1}\mathbf{Z}_{p,M})$$

Proof. This follows from the fact that f is an eigenform for T_p. See [16, Section 10] for more details.

□

In the ordinary case, $\mathrm{ord}_p(a_p) = 0$ and there is a unique allowable α. This α is also a unit and the above distribution is bounded. In the supersingular case, $\mathrm{ord}_p(a_p) > 0$ and hence there can be two allowable choices for α. Since the above distribution contains terms with powers of α in their denominators, $\mu_{f,\alpha}^{\pm}$ need not be bounded.

4.2 Integrating with respect to $\mu_{f,\alpha}^{\pm}$

The fact that $\mu_{f,\alpha}^{\pm}$ is in general only a distribution and not a measure presents a problem with respect to integration. Riemann sums will not necessarily converge. However, the rate at which $\mu_{f,\alpha}^{\pm}$ grows is controllable which will suffice to make sense of integration. The following proposition bounds this growth.

Proposition 4.3. *Let $h' = \mathrm{ord}_p(\alpha)$ be the slope of α. Then for i such that $0 \le i \le [h']$ we have that*

$$\sup_a \left| \mu_{f,\alpha}^{\pm}\left((x-a)^i, a + p^n M\mathbf{Z}_{p,M}\right) \right|$$

is $O(p^{n(h'-i)})$ as a function of n.

Proof. [22, Lemma 3.8]. □

Now let F be a locally analytic function on $\mathbf{Z}_{p,M}^\times$. To approximate F we will use more general Riemann sums that involve the first $[h']+1$ terms of the Taylor series of F.

Let Λ_m be a system of representatives of $\mathbf{Z}_{p,M}^\times$ mod p^n and let $h = [h']+1$. Define,

$$S_m^\pm(F) = \sum_{b\in\Lambda_m} \sum_{i=0}^{h-1} \frac{F^{(i)}(b)}{i!} \cdot \mu_{f,\alpha}^\pm \left((x-b_p)^i, b + p^n M \mathbf{Z}_{p,M}^\times \right)$$

where $x \mapsto x_p$ is the natural projection from $\mathbf{Z}_{p,M}$ to $\mathbf{Z}_p$.

Lemma 4.4. *For F locally analytic,*

$$\lim_{m\to\infty} S_m^\pm(F)$$

converges and is independent of the choice of Λ_m.

Proof. [22, Lemma 1.5,1.6] □

We now define integration by

$$\int_{\mathbf{Z}_{p,M}^\times} F\, d\mu_{f,\alpha}^\pm := \lim_{m\to\infty} S_m^\pm(F).$$

Note that in the ordinary case $h' = 0$ and the above reduces to just standard Riemann sums.

4.3 Analytic properties of the p-adic L-function

The p-adic L-function of a modular form is a function defined by integration on the $\mathbf{C}_p$-valued characters of $\mathbf{Z}_{p,M}^\times$. Precisely,

$$L_p(f,\alpha,\cdot) : \mathrm{Hom}(\mathbf{Z}_{p,M}^\times, \mathbf{C}_p) \to \mathbf{C}_p$$

by the formula

$$L_p(f,\alpha,\chi) := \int_{\mathbf{Z}_{p,M}^\times} \chi\, d\mu_{f,\alpha}^{\mathrm{sgn}\,\chi}.$$

The space $\mathrm{Hom}(\mathbf{Z}_{p,M}^\times, \mathbf{C}_p)$ has a natural analytic structure which we will now describe. Let q equal p for odd primes and 4 for $p = 2$. Fix γ a topological generator of $1 + q\mathbf{Z}_p$. Note that

$$\mathrm{Hom}(\mathbf{Z}_{p,M}^\times, \mathbf{C}_p) \simeq \mathrm{Hom}\left((\mathbf{Z}/Mq\mathbf{Z})^\times, \mathbf{C}_p\right) \times \mathrm{Hom}(1+q\mathbf{Z}_p, \mathbf{C}_p)$$

and

$$\mathrm{Hom}(1+q\mathbf{Z}_p, \mathbf{C}_p) \simeq \{z \in \mathbf{C}_p : |z-1|_p < 1\}$$

via $\psi \mapsto \psi(\gamma)$. So $\mathrm{Hom}(\mathbf{Z}_{p,M}^\times, \mathbf{C}_p)$ is composed of several copies of the open unit disc of $\mathbf{C}_p$. With respect to this analytic structure, $L_p(f,\alpha,\chi)$ is analytic in χ.

We will make this more explicit. Call characters on $\mathbf{Z}_{p,M}^{\times}$ *tame* if they factor thru $(\mathbf{Z}/Mq)^{\times}$ and *wild* if they factor thru $1+q\mathbf{Z}_p$. Define a particular wild character $\chi_u \in \mathrm{Hom}(\mathbf{Z}_{p,M}^{\times}, \mathbf{C}_p)$ by

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

where the first and second maps are the natural projections (the second map sends x to $\frac{x}{\omega(x)}$ with $\omega(x)$ the Teichmüller character). The third map simply sends our chosen generator γ onto u. Fix a tame character ψ on $\mathbf{Z}_{p,M}^{\times}$. Then, under the above identification, $L_p(f,\alpha,\psi\chi_u)$ is analytic as a function of u.

Before proving this fact and discussing the rate of growth of $L_p(f,\alpha,\cdot)$, we will first need to recall the basic theory of the Newton polygon (see [3] for more details).

4.3.1 Newton polygon

Definition 4.5. For $K/\mathbf{Q}_p$, denote by $\mathcal{A}(K)$ the set of rigid analytic functions on the unit disc with coefficients in K. That is,

$$\mathcal{A}(K) = \left\{ F = \sum_{k=0}^{\infty} a_k T^k \;\middle|\; a_k \in K; F \text{ converges on the open unit disc of } \mathbf{C}_p \right\}$$

Definition 4.6. Let $F \in \mathcal{A}(K)$. Define the Newton polygon of F by

$$M_F(t) := \log_p \left(\sup_{|z|_p < p^{-t}} |F(z)|_p \right)$$

for $t \in \mathbf{R}$, $t > 0$. Here $\log_p$ is the usual real valued logarithm having its base equal to p.

Remark 4.7. The above definition is the *only* place in this paper where $\log_p$ will refer to the usual logarithm. In all other places it will refer to the p-adic logarithm.

Proposition 4.8. *For $F \in \mathcal{A}(K)$, we have that*

1. *$M_F(t)$ is a piecewise linear function.*
2. *For z in the unit disc, $F(z) = 0$ if and only if $\mathrm{ord}_p(z)$ is a breakpoint of $M_F(t)$.*
3. *For t a breakpoint of $M_F(t)$, the number of zeroes of F with valuation exactly t is the difference between the slopes of the lines joining at t.*

Example 4.9. We will now analyze $M_F(t)$ where $F = \log_p(1+z)$ — the p-adic logarithm. Since the zeroes of $\log_p(z)$ are exactly the p^n-th roots of unity, the breakpoints of $M_F(t)$ are given by

$$\frac{1}{\phi(p^n)} = \frac{1}{(p^n - p^{n-1})}.$$

Let $t_n = 1/\phi(p^n)$. Note that the slope of $M_F(t)$ between t_{n+1} and t_n is $-\sum_{r=0}^{n} \phi(p^r) = -p^n$. Hence,

$$M_F(t_{n+1}) - M_F(t_n) = p^n \cdot (t_n - t_{n+1}) = 1.$$

Since $M_F(t_1) = -1/(p-1)$, we have

$$M_F(t_n) = n - p/(p-1).$$

Definition 4.10. For F and $G \in \mathcal{A}(K)$, we say that F is $\mathrm{O}(G)$ if

$$\sup_{|z|<r} |F(z)|_p \quad \text{is} \quad \mathrm{O}\left(\sup_{|z|<r} |G(z)|_p\right) \quad \text{as} \quad r \mapsto 1^-.$$

This is equivalent to

$$\lim_{t\to 0^+} M_F(t) - M_G(t) < \infty.$$

We define F being $\mathrm{o}(G)$ similarly and this is equivalent to

$$\lim_{t\to 0^+} M_F(t) - M_G(t) = -\infty.$$

Finally, say $F \sim G$ if F is $\mathrm{O}(G)$ and G^+ is $\mathrm{O}(F)$.

The following lemma is useful in proving convergence of analytic functions.

Lemma 4.11. *Suppose that f_n is a sequence in $\mathcal{A}(K)$ and that t_i is some sequence of positive real numbers tending to 0. Then $f_n \to f$ uniformly on all closed subdiscs of the unit disc iff $\lim_{n\to\infty} M_{f-f_n}(t_i) = -\infty$ for all i.*

Proof. We have that $f_n \to f$ uniformly on the closed disc of radius p^t if and only if $\sup_{|z|_p<p^t} |f(z) - f_n(z)| \to 0$ as $n \to \infty$. This last limit is equivalent to $M_{f-f_n}(t) \to -\infty$ as $n \to \infty$. □

4.3.2 Growth estimates on $L_p(f, \alpha, \cdot)$

Proposition 4.12. *(Visik, Amice-Vélu) The function $L_p(f, \alpha, \chi_u)$ is analytic in u and is $O(\log_p^{h'})$ where $h' = \mathrm{ord}_p(\alpha)$.*

Proof. This proof is taken nearly verbatim from [22, Theorem 2.3] except that there the weaker estimate of $\mathrm{o}(\log_p^h)$ (where $h = [\mathrm{ord}_p(\alpha)] + 1$) is obtained. The bound of $\mathrm{O}(p^{n(h'-i)})$ from Proposition 4.3 yields the big-O estimate on the L-function.

Note that it suffices to see that $u \mapsto \int_{1+p\mathbf{Z}_p} \chi_u \mu_{f,\alpha}^{\pm}$ is analytic and $\mathrm{O}(\log_p^{h'})$. Let $\{\gamma^j\}$ with $0 \le j \le p^{m-1}$ be our set of representatives of $1 + p\mathbf{Z}_p$ mod p^m where γ is our chosen generator. Then

$$S_m^{\pm}(\chi_u) = \sum_{j=0}^{p^{m-1}-1} \sum_{i=0}^{h-1} \frac{\chi_u^{(i)}(\gamma^j)}{i!} \cdot \mu_{f,\alpha}^{\pm}\left((x-\gamma^j)^i, \gamma^j + p^m\mathbf{Z}_p\right)$$

which we will denote simply by $S_m(u)$. The following three facts about S_m are proved in [22].

1. $S_m(u) = R_0^{(m)}(u) + R_1^{(m)}(u) \cdot \log_p(u) + \cdots + R_{h-1}^{(m)}(u) \cdot \log_p^{h-1}(u)$ where the $R_i^{(m)}(u)$ are polynomials in u.
2. $\sup_u |R_i^{(m)}(u)|_p$ is $\mathrm{O}(p^{m(h'-i)})$.
3. $S_{m+1} - S_m \equiv 0 \mod \left(\prod_{i=0}^{h-1}\left(\left(\frac{u}{\gamma^i}\right)^{p^m} - 1\right)\right)$.

Actually, in [22] condition 2 is only stated as $\mathrm{o}(p^{m(h-i)})$, but from proposition 4.3 the stronger bound is clear.

Let $t_n = 1/\phi(p^n)$ and let $M_m = M_{S_{m+1}-S_m}$. Then to see that $L_p(f, \alpha, \chi_u)$ is analytic in u it suffices to see that $\lim_{m\to\infty} M_m(t_n) = -\infty$ for all n. This follows from Lemma 4.11.

First note that condition 3 implies that $S_{m+1} - S_m$ vanishes at $\gamma^j \cdot \zeta_{p^k}$ for $0 \leq j \leq h-1$ and for $k \leq m$. Let F denote $\log_p^h$. Then for $t \geq t_m$, the slope of $M_m(t)$ is greater than or equal to the slope of $M_F(t)$ as F vanishes with multiplicity h at all of the p-power roots of unity.

From example 4.9, we know that $M_F(t_{n+1}) - M_F(t_n) = h$ and hence, we have that

$$M_m(t_m) - M_m(t_n) \geq h(m-n) \quad \text{for} \quad m > n. \tag{6}$$

Now from condition 2, we have that $\lim_{m\to\infty} M_{R_l^{(m)}}(t) - m(h-i) = -\infty$ for any t. (Here we are only using 2 its its weaker form as it appeared in [22].) Also, $M_{\log_p^i}(t_m) = i\,(m - p/(p-1))$. Hence from condition 1,

$$M_m(t_m) = mh + d(m) \tag{7}$$

where $\lim_{m\to\infty} d(m) = -\infty$.

Then from (6) and (7), we have

$$d(m) \geq M_m(t_n) - hn$$

and hence $M_m(t_n) \to -\infty$ as $m \to \infty$. This proves that our L-function is analytic.

Now we move on to prove the growth estimate. Let $L = \lim_{m\to\infty} S_m$. In order to check that L is $\mathrm{O}(\log_p^{h'})$, we need that

$$\lim_{n\to\infty} M_L(t_n) - h'n < \infty.$$

Note that $L = S_1 + \sum_{m=1}^{\infty} S_{m+1} - S_m$ and hence

$$M_G(t_n) \leq \max\left(\sup_{m\leq n} M_m(t_n), \sup_{m>n} M_m(t_n), M_{S_1}(t_n)\right).$$

The last term is easy to control since S_1 is $\mathrm{O}(\log_p^{h-1})$ and hence $\mathrm{O}(\log_p^{h'})$.

For $m \leq n$, we have from conditions 1 and 2,

$$M_m(t_n) \leq \max_{0\leq l\leq h-1} nl - \frac{lp}{p-1} + mh' - ml + d(m)$$

where $\lim_{m\to\infty} d(m) < \infty$. This uses the stronger version of condition 2 as stated in this paper. We then have that

$$\begin{aligned} M_m(t_n) &\leq \max_{0\leq l\leq h-1} nh' + (m-n)(h'-l) - \frac{lp}{p-1} + d(m) \\ &\leq nh' - (n-m)h' + d(m) \\ &\leq nh' + d(m) \end{aligned}$$

as $m \leq n$.

For $m > n$, as in the first part of this proof, we have

$$M_m(t_m) - M_m(t_n) \geq h(m-n) \geq h'(m-n)$$

and

$$M_m(t_m) = mh' + c(m)$$

where $c(m)$ is bounded as $m \to \infty$. (This again uses the stronger estimate in condition 2.) Combining the above two formulas yields,

$$M_m(t_n) \leq nh' + c(m).$$

Finally, combining the two cases of $m \leq n$ and $m > n$ yields,

$$M_m(t_n) \leq nh' + C$$

where C is independent of n establishing the result. □

4.3.3 Power series representation of $L_p(f, \alpha, \cdot)$

Now that we know $L_p(f, \alpha, \psi\chi_u)$ is analytic in u, we can form its power series expansion at 1. Denote this by $L_p(f, \alpha, \psi, T)$ and hence

$$L_p(f, \alpha, \psi, u-1) = L_p(f, \alpha, \psi\chi_u).$$

Note that this expression of the L-function as a power series depends upon our choice of γ generating $1 + q\mathbf{Z}_p$. However, the dependence is not serious and γ will always be suppressed from the notation. Also, if we are in the ordinary case, α is uniquely determined and will be dropped from the notation.

This power series converges on the open unit disc. If the tame part of χ is φ then $\int_{\mathbf{Z}_p^\times} \chi \, d\mu_{f,\alpha}^{\pm} \in K(\alpha, \varphi)$. From this it follows that

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

If ψ is the trivial character then we write $L_p(f, \alpha, T)$ for $L_p(f, \alpha, \psi, T)$.

Remark 4.13. The p-adic L-function of f also depends upon our choice of $\Omega_f^{\pm}$ which are only defined up to an element of $\mathcal{O}_K^\times$. In the case of elliptic curves, we will specify a particular choice of periods and pin down the L-function up to sign.

4.4 Evaluating at finite order characters

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

$$L_p(f, \alpha, \psi, \gamma^j \cdot (\zeta_{p^n} - 1)) \ \text{ for } \ 0 \leq j \leq k-2$$

where ζ_{p^n} is a p^n-th root of unity. In this way, $L_p(f, \alpha, \psi, T)$ can be thought of as a solution to an interpolation problem. In the ordinary case this completely determines $L_p(f, \alpha, \psi, T)$. In the supersingular case this will also completely determine the L-function with the added condition that it be $o(\log_p^h)$ where $h = [\text{ord}_p(\alpha)] + 1$. (Any two functions satisfying the interpolation property will differ by a function that vanishes so often it must grows like $\log_p^h$.)

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

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

Proposition 4.14. *For φ as above,*

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

where $L(f_\varphi, s)$ is the complex L-series attached to f twisted by φ.

Proof. [16, Section 14] □

Remark 4.15. Note that the above formula only depends upon α in the first factor. If $\nu > 0$ the above formula simplifies greatly since $e_p(\alpha, \chi) = \frac{1}{\alpha^\nu}$.

5 Results on the infinitude of zeroes of supersingular L-functions

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

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

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

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

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

We first begin with a lemma that says that if a p-adic power series has finitely many zeroes then its coefficients are bounded.

Lemma 5.1. *(Iovita) Let K be some finite extension of $\mathbf{Q}_p$ and let $\mathcal{A}(K)$ be the subring of $K[[T]]$ consisting of power series convergent on the open unit disc. Then $f(T) \in K[[T]]$ has only finitely many zeroes if and only if $f(T) \in \mathcal{O}_K[[T]] \otimes K$.*

Proof. By the Weierstrass preparation theorem, any element of $\mathcal{O}_K[[T]] \otimes K$ has only finitely many zeroes. Conversely, take $f(T) \in K[[T]]$ with only finitely many zeroes. Then all of its zeroes must be algebraic over K. Let $P(T)$ be a polynomial in $K[T]$ with the same roots (counting multiplicity) as $f(T)$. Then from [10, Lemma 1] there is some $g(T) \in \mathcal{A}(K)$ such that $f(T) = P(T) \cdot g(T)$. Since $g(z)$ is non-zero for all z in the open unit disc, we have that $g(T)$ is a unit in $\mathcal{A}(K)$ [10, Proposition 4.1]. Finally, the units of $\mathcal{A}(K)$ are $K^\times \cdot (1 + T\mathcal{O}_K[[T]])$ [10, (4.8)] which completes the proof. □

Theorem 5.2. *(Mazur) Suppose that $h_1 > 0$ and $h_1 \neq h_2$. Then for a fixed tame character ψ on $\mathbf{Z}_{p,M}^\times$, at least one of $L_p(f, \alpha_1, \psi, \cdot)$ and $L_p(f, \alpha_2, \psi, \cdot)$ has infinitely many zeroes in the open unit disc.*

Proof. From the remark following Proposition 4.14, we have that

$$L_p(f, \alpha_1, \psi, \zeta_{p^{n-1}} - 1) = \frac{c_n}{{\alpha_1}^n}$$

$$L_p(f, \alpha_2, \psi, \zeta_{p^{n-1}} - 1) = \frac{c_n}{{\alpha_2}^n}$$

for some constant c_n independent of the α_i. (Here we are implicitly assuming that $p \neq 2$. For $p = 2$ the exponent on the α_i would be $n+1$ making little difference in the argument below.)

Suppose that both $L_p(f, \alpha_1, \psi, T)$ and $L_p(f, \alpha_2, \psi, T)$ have finitely many zeroes. Then Lemma 5.1 says that they both have bounded coefficients. By the Weierstrass preparation theorem, we can write

$$L_p(f, \alpha_1, \psi, T) = p^{r_1} P_1(T) U_1(T) \quad \text{and} \quad L_p(f, \alpha_2, \psi, T) = p^{r_2} P_2(T) U_2(T),$$

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

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

Taking valuations of the above equation yields

$$h_1 \cdot n + r_1 + d_1 \cdot \mathrm{ord}_p(\zeta_{p^{n-1}} - 1) = h_2 \cdot n + r_2 + d_2 \cdot \mathrm{ord}_p(\zeta_{p^{n-1}} - 1),$$

for large n. Since $\mathrm{ord}_p(\zeta_{p^{n-1}} - 1)$ tends to 0 for large n and $h_1 \neq h_2$, we have a contradiction. Hence, one of the two power series has infinitely many zeroes. □

Remark 5.3. Note that this proof does not indicate which of the two L-functions vanishes infinitely often. It is believed to be true that both of these L-functions have infinitely many zeroes.

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

Theorem 5.4. *(Perrin-Riou; Visik) Suppose that $a_p = 0$ (and hence $h_1 = h_2$). Then for a fixed tame character ψ on $\mathbf{Z}_{p,M}^\times$ one of $L_p(f, \alpha_1, \psi, \cdot)$ and $L_p(f, \alpha_2, \psi, \cdot)$ have infinitely many zeroes in the open unit disc. If $K(\psi, \alpha_1) \neq K(\psi)$ then both L-functions have infinitely many zeroes.*

Proof. Let

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

Then

$$L_{\alpha_1}(T) = G_\psi^+(T) + G_\psi^-(T) \cdot \alpha_1.$$

As before, we have that

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

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

$$L_p(f, \alpha_1, \psi, \zeta_{p^n} - 1) = L_p(f, \alpha_2, \psi, \zeta_{p^n} - 1)$$

for n odd and

$$L_p(f, \alpha_1, \psi, \zeta_{p^n} - 1) = -L_p(f, \alpha_2, \psi, \zeta_{p^n} - 1)$$

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

Assume now that both $L_p(f, \alpha_1, \psi, T)$ and $L_p(f, \alpha_2, \psi, T)$ have finitely many zeroes. Again Lemma 5.1 guarantees that they both have bounded coefficients. Hence, both G_ψ^+ and G_ψ^- also have bounded coefficients. But G_ψ^+ and G_ψ^- have infinitely many zeroes which is a contradiction.

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

Corollary 5.5. *Suppose p is a supersingular prime for an elliptic curve E over $\mathbf{Q}$. Then at least one of $L_p(E, \alpha_1, \psi, T)$ and $L_p(E, \alpha_2, \psi, T)$ have infinitely many zeroes in the open unit disc. If $\mathbf{Q}_p(\psi, \alpha) \neq \mathbf{Q}_p(\alpha)$ then both functions have infinitely many zeroes.*

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

6 The gamma-like functions Φ^+ and Φ^-

In the previous proof it was shown that when $a_p = 0$ we can write

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

where $G_\psi^+(T)$ vanishes at $\zeta_{p^{2n}} - 1$ and $G_\psi^-(T)$ vanishes at $\zeta_{p^{2n-1}} - 1$ for all $n > 0$. The interpolation data also forces $G_\psi^+(T)$ to vanish at $\gamma^j \cdot (\zeta_{p^{2n}} - 1)$ and $G_\psi^-(T)$ to vanish at $\gamma^j \cdot (\zeta_{p^{2n-1}} - 1)$ for $0 \leq j \leq k - 1$. One of the main results of this paper is that G_ψ^+ and G_ψ^- have only finitely more zeroes than this fixed set of forced roots.

In fact, there exists two power series Φ^+ and $\Phi^- \in \mathbf{Q}_p[[T]]$, depending only on k and γ, such that Φ^+ and Φ^- have simple zeroes at $\gamma^j \cdot (\zeta_{p^{2n}} - 1)$ and $\gamma^j \cdot (\zeta_{p^{2n-1}} - 1)$ respectively for $0 \leq j \leq k - 1$, for all $n > 0$ and such that

$$\frac{G_\psi^+(T)}{\Phi^+(T)} \quad \text{and} \quad \frac{G_\psi^-(T)}{\Phi^-(T)}$$

have bounded coefficients. (Recall that if $p = 2$ then there is a parity switch and the roles of Φ^+ and Φ^- should be interchanged.)

In this section we will first construct Φ^+ and Φ^- as an infinite product of cyclotomic polynomials. After this, we will study their rates of growth by computing their Newton polygons. Finally, we will see that they satisfy a trivial functional equation.

6.1 Construction of Φ^+ and Φ^-

For the remainder of the paper, we will abbreviate the notation for a p^n-th root of unity ζ_{p^n} to ζ_n. Let $\Phi_n(T) = \Phi_{p^n}(T) = \sum_{t=0}^{p-1} T^{p^{n-1}\cdot t}$ be the p^n-th cyclotomic polynomial.

We first construct two functions $\Phi_j^+(T)$ and $\Phi_j^-(T)$ that vanish at $\gamma^j\cdot(\zeta_{2n}-1)$ and $\gamma^j\cdot(\zeta_{2n-1}-1)$ respectively for a *fixed* integer j and all $n > 0$. We then take the product of these functions over j between 0 and $k-2$ to form our main functions $\Phi^+(T)$ and $\Phi^-(T)$.

Lemma 6.1. *For any integer j, the products*

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

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

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

Proof. We will prove this for the first product since the argument for the second one is virtually identical. Fix some $R < 1$ and let $\overline{D}(0,R)$ be the closed disc of radius R about zero. To see that the product converges, it suffices to see that

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

We have

$$\left|\frac{\Phi_{2n}\left(\frac{T}{\gamma^j}+1\right)}{p}-1\right| \le \max_{0\le t\le p-1}\left|\left(\frac{\left(\frac{T}{\gamma^j}+1\right)^{p^{2n-1}\cdot t}-1}{p}\right)\right|$$

$$\le \max_{t,s}\left|\frac{\binom{p^{2n-1}\cdot t}{s}}{p}\cdot\left(\frac{T}{\gamma^j}\right)^s\right|.$$

For $1\le s<p^n$, $p^n\Big|\binom{p^{2n-1}\cdot t}{s}$ and so $p^{n-1}\Big|\frac{\binom{p^{2n-1}\cdot t}{s}}{p}\cdot\left(\frac{T}{\gamma^j}\right)^s$ since $\gamma^j\in\mathbf{Z}_p^\times$.
For $p^n\le s\le p^{2n-1}\cdot t$, $T^{p^n}\Big|\frac{\binom{p^{2n-1}\cdot t}{s}}{p}\cdot\left(\frac{T}{\gamma^j}\right)^s$.

Since we are on a closed disc of radius $R<1$, picking n large enough forces all of these terms to tend to 0. This proves convergence of the products. Since the space of convergent power series on the open disc is complete, our power series is automatically convergent on the open unit disc.

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

$$\log_p \left(1 + \frac{T}{\gamma^j}\right) = \lim_{n\to\infty} \frac{\left(\frac{T}{\gamma^j} + 1\right)^{p^n} - 1}{p^n}$$

and hence,

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

Since $\log_p \left(1 + \frac{T}{\gamma^j}\right)$ has simple zeroes at $\gamma^j \cdot (\zeta_n - 1)$ for $n \geq 0$, $\Phi_j^-(T)$ and $\Phi_j^+(T)$ have no extra zeroes and all of their zeroes are simple. □

Lemma 6.2. *The power series*

$$\Phi^+(T) := \prod_{j=0}^{k-2} \Phi_j^+(T)$$
$$\Phi^-(T) := \prod_{j=0}^{k-2} \Phi_j^-(T)$$

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

Proof. This all follows from the previous lemma.

□

6.2 The rate of growth of Φ^+ and Φ^-

Lemma 6.3. $\Phi^+ \sim \Phi^- \sim \log_p^{(k-1)/2}$.

Proof. We will prove this simply by calculating the Newton polygons of both Φ^+ and Φ^-. It may be useful to compare the following to example 4.9.

We begin by computing the Newton polygon of $F = \Phi_j^+(T)$. The breakpoints of $M_F(t)$ are then given by $1/\phi(p^{2n})$. The slope of $M_F(t)$ between t_{2n+2} and t_{2n} is

$$-\sum_{r=1}^{n} \phi(p^{2r}) = -\frac{p \cdot (p^{2n} - 1)}{p + 1}.$$

Hence,

$$M_F(t_{2n+2}) - M_F(t_{2n}) = \frac{p \cdot (p^{2n} - 1)}{p + 1} \cdot (t_{2n} - t_{2n+2}) = 1 - \frac{1}{p^{2n}}.$$

Since $M_F(t_0) = 1$, we have

$$M_F(t_{2n}) = n - \sum_{k=1}^{n} \frac{1}{p^{2k}} + 1.$$

Similarly, for $F = \Phi_j^-(T)$,

$$M_F(t_{2n+1}) = n - \sum_{k=1}^{n} \frac{1}{p^{2k}} + 1.$$

For $F = \Phi^+$ or Φ^- then M_F is given by $k-1$ times the appropriate formula above.

From our computation of the Newton polygon for $\log_p^{(k-1)/2}$ in example 4.9, a simple comparison of all these formulas yields the lemma. □

6.3 Functional equations for Φ^+ and Φ^-

The natural change of variables in the T-variable for a functional equation is $T \mapsto \frac{1}{1+T} - 1$. The next lemma shows that Φ^+ and Φ^- are invariant under this change of variable.

Lemma 6.4. *We have* $\Phi^+\left(\frac{1}{1+T} - 1\right) = \Phi^+(T)$ *and* $\Phi^-\left(\frac{1}{1+T} - 1\right) = \Phi^-(T)$.

Proof.

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

as the root of Φ_{2k} are invariant under $z \mapsto z^{-1}$;

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

as $\prod_{k=1}^{\infty}(1+T)^{\phi(p^{2k})} = 1$. Similarly,

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

□

7 Description of p-adic L-functions in terms of Φ^+ and Φ^-

7.1 Main result

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

Theorem 7.1. *Suppose that $a_p = 0$ and p is odd. Then*

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

where $g_\psi^\pm \in \Lambda_\psi \otimes K_\psi$. If $p = 2$ then

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

where $g_\psi^\pm \in \Lambda_\psi \otimes K_\psi$.

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

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

as in the proof of Theorem 5.4. Then the interpolation property from section 4.4 forces

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

for $0 \leq j \leq k - 2$ and all $n > 0$. Since all the zeroes (counting multiplicity) of Φ^+ (resp. Φ^-) are also zeroes of G_ψ^+ (resp. G_ψ^-), [10, (4.8)] tells us that

$$\Phi^+ \Big| G_\psi^+ \text{ and } \Phi^- \Big| G_\psi^-$$

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

$$g_\psi^+ = \frac{G_\psi^+}{\Phi^+} \text{ and } g_\psi^- = \frac{G_\psi^-}{\Phi^-}.$$

By Lemma 4.12, G_ψ^+ and G_ψ^- are $\mathrm{O}(\log_p^{(k-1)/2})$ and by Lemma 6.3, $\Phi^+ \sim \Phi^- \sim \log_p^{(k-1)/2}$. Hence, both g_ψ^+ and g_ψ^- are O(1) (i.e. bounded). From the following lemma, we can concluded that g_ψ^+ and g_ψ^- have bounded coefficients. □

Lemma 7.2. *If $G(z) = \sum_i a_i z^i$ is a bounded analytic function (i.e. O(1)) then G has bounded coefficients.*

Proof. Assume not and pick i large enough so that $|a_i|_p > 2N$ for an arbitrary integer $N \gg 0$. Note that

$$|a_i|_p \cdot |z|_p^i \leq \sup_{i,z} |a_i z^i|_p = \sup_z |G(z)|_p$$

for all i and z. We can then pick z with $|z|_p$ arbitrarily close to 1. This forces $|G(z)|_p > N$ contradicting the boundedness of G. □

7.2 The case of elliptic curves

7.2.1 Definition of p-adic L-functions

Let E be an elliptic curve over $\mathbf{Q}$. Since E is modular, we will define the p-adic L-function of E to be the p-adic L-function of the corresponding modular form. More precisely, let f_E be the normalized newform corresponding to E of weight 2 and level N. To define the p-adic L-function of f_E we need to make a choice of periods (see Theorem 4.1). We will pin down these two periods up to sign.

Let ω_E be the Néron differential of E and let $\gamma^\pm$ generate $H_1(E,\mathbf{Z})^\pm$. Define $\Omega_E^\pm := \int_{\gamma^\pm} \omega_E$ which is uniquely determined up to sign. We then define the p-adic L-function of E by $L_p(E,\alpha,\cdot) = L_p(f_E,\alpha,\cdot)$ where the p-adic L-function of f_E is defined using $\Omega_E^\pm$. If p is ordinary, we will write this as $L_p(E,\cdot)$ dropping α from the notation.

Remark 7.3. In section 4.1, modular symbols were notated by $\lambda^\pm(f,P;a,m)$ where P is an integral polynomial of degree less than or equal to $k-2$. Since $k=2$ for elliptic curves, the P term becomes irrelevant. Furthermore, when P is trivial, $\lambda^\pm(f,P;a,m)$ depends only on the rational number $\frac{a}{m}$. In the case of elliptic curves, we will adopt the (standard) notation,

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

Remark 7.4. The periods $\Omega_E^\pm$ do not necessarily satisfy the requirements of Theorem 4.1. For example, take $E = X_0(11)$ and $p=5$. Then

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

However, for a fixed E, the denominators of the modular symbols are bounded. This is made more precise in the next lemma.

Lemma 7.5. *Let E be an elliptic curve over $\mathbf{Q}$ of conductor N. Let m be some integer prime to N. Then*

$$2\cdot(p+1-a_p)\cdot\left[\frac{a}{m}\right]^+ \in \mathbf{Z} \quad \textit{and} \quad 2\cdot\left[\frac{a}{m}\right]^- \in \mathbf{Z}$$

for any prime p of good reduction for E.

Proof. First note that if $r, s \in \mathbf{Q}$ are two equivalent cusps of $X_0(N)$ then

$$2\pi i \int_r^s f_E(z)\ dz \in \mathbf{Z}\Omega_E^+ \oplus \mathbf{Z}\Omega_E^-.$$

(Here and in what follows, all integrals will be taken over some path in the upper half plane connecting the two endpoints of integration.) Now

$$2 \cdot \left[\frac{a}{m}\right]^+ \cdot \Omega_E^+ = \int_{i\infty}^{\frac{a}{m}} f_E + \int_{i\infty}^{-\frac{a}{m}} f_E = 2 \cdot \int_{i\infty}^{0} f_E + \int_{0}^{\frac{a}{m}} f_E + \int_{0}^{-\frac{a}{m}} f_E.$$

Since m is relatively prime to N, we have that $0, \frac{a}{m}$ and $-\frac{a}{m}$ are all equivalent cusps in $X_0(N)$. Hence the sum of the last two terms in the above formula yields an integral multiple of Ω_E^+.

As for the first term, see [2, pg. 30] for the following formula:

$$(p + 1 - a_p) \cdot \int_0^{i\infty} f_E = \sum_{a=1}^{p-1} \int_0^{\frac{a}{p}} f_E.$$

Since E has good reduction at p, we have that $p \nmid N$ and hence 0 and $\frac{a}{p}$ are equivalent cusps of $X_0(N)$. Therefore, the right hand side is an integral multiple of Ω_E^+ which proves the first part of the claim.

Since

$$2 \cdot \left[\frac{a}{m}\right]^- \cdot \Omega_E^- = \int_{i\infty}^{\frac{a}{m}} f_E - \int_{i\infty}^{-\frac{a}{m}} f_E = \int_{-\frac{a}{m}}^{\frac{a}{m}} f_E$$

and $\frac{a}{m}$ and $-\frac{a}{m}$ are equivalent cusps, we have $2 \cdot \left[\frac{a}{m}\right]^- \in \mathbf{Z}$.

□

Even though the modular symbols may carry denominators, the p-adic L-function of an elliptic curve is conjectured to be an integral power series in the ordinary case. This is known in many setting. The above lemma handles the following easy case.

Proposition 7.6. *Let E be an elliptic curve over $\mathbf{Q}$ and p a prime of good reduction such that $a_p \not\equiv 0, 1 \pmod{p}$. Then $L_p(E, T)$ is an integral power series.*

Proof. Note that α is dropped from the notation since we are in the ordinary case. For p odd, from Lemma 7.5 we have that $(p + 1 - a_p) \cdot \left[\frac{a}{p^r}\right]^+ \in \mathbf{Z}_p$. Since $a_p \not\equiv 0 \pmod{p}$, we have that $\alpha \in \mathbf{Z}_p^\times$. Since $a_p \not\equiv 1 \pmod{p}$, we have that $\left[\frac{a}{p^r}\right]^+ \in \mathbf{Z}_p$. Therefore, $\mu_{f_E}^+$ takes values in $\mathbf{Z}_p$ from which it is clear that $L_p(E, T) \in \mathbf{Z}_p[[T]]$.

For $p = 2$, $\mu_{f_E}^+$ may take values in $\frac{1}{2}\mathbf{Z}_2$. However, in each Riemann sum both $\mu_{f_E}(a + 2^n\mathbf{Z}_2)$ and $\mu_{f_E}(-a + 2^n\mathbf{Z}_2)$ appear. Since these are equal our needed extra factor of 2 appears. □

Remark 7.7. The complex L-series of an elliptic curve is invariant under isogeny. However, this is not the case for the p-adic L-function. Since f_E is a normalized newform it is invariant under isogeny. However, the periods $\Omega_E^{\pm}$ may change by a rational constant under isogeny which will then change the p-adic L-function by a rational constant. Such a change could at worst affect the μ-invariant of the p-adic L-series.

7.2.2 Main result for elliptic curves

When $a_p \equiv 0 \pmod{p}$, we are in the supersingular case and then certainly $L_p(E, \alpha, T) \notin \mathbf{Z}_p[[T]]$. In fact, by Theorem 5.4, $L_p(E, \alpha, T) \notin \mathbf{Z}_p[[T]] \otimes \mathbf{Q}_p$. We know from Theorem 7.1 that the g^+ and g^- functions corresponding to E have bounded coefficients. In the case of elliptic curves, we can strengthen this to say they are actually integral power series.

Theorem 7.8. *Let $E/\mathbf{Q}$ be an elliptic curve. Let*

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

for $p \neq 2$ and let

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

as in Theorem 7.1. Then $g^+(T), g^-(T) \in \mathbf{Z}_p[[T]]$.

Remark 7.9. The extra factor of $\frac{1}{2}$ appearing when $p = 2$ is necessary to ensure that $g^- \in \mathbf{Z}_2[[T]]$.

This theorem will be proved by an explicit computation. In the proof of Proposition 4.12, a sequence $S_n(T)$ of polynomials in $\mathbf{Q}_p(\alpha)[T]$ was constructed such that $S_n(T) \to L_p(E, \alpha, T)$. Write

$$S_n(T) = G_n^+(T) + G_n^-(T) \cdot \alpha$$

where $G_n^{\pm} \in \mathbf{Q}_p[[T]]$. Since the weight of f_E is 2, $L_p(E, \alpha, T)$ is defined by a limit of standard Riemann sums which lend themselves to explicit computation. The following lemma will give precise formulas for G_n^+ and G_n^-. The proof of the above theorem will then follow from simply counting the number of p's in the denominator and seeing that there are none.

Lemma 7.10. *For p odd,*

$$G_n^+(T) = \begin{cases} (-p)^{-\frac{n}{2}} \displaystyle\sum_{j=0}^{p^{n-1}-1} \left(\sum_{a=0}^{p-1} \left[\frac{\omega(a)\gamma^j}{p^n} \right]^+ \right) (T+1)^j & 2 \mid n \\ (-p)^{-\left(\frac{n+1}{2}\right)} \displaystyle\sum_{j=0}^{p^{n-1}-1} \left(\sum_{a=0}^{p-1} \left[\frac{\omega(a)\gamma^j}{p^{n-1}} \right]^+ \right) (T+1)^j & 2 \nmid n \end{cases}$$

and

$$G_n^-(T) = \begin{cases} (-p)^{-\left(\frac{n}{2}+1\right)} \displaystyle\sum_{j=0}^{p^{n-1}-1} \left(\sum_{a=0}^{p-1} \left[\frac{\omega(a)\gamma^j}{p^{n-1}} \right]^+ \right) (T+1)^j & 2 \mid n \\ (-p)^{-\left(\frac{n+1}{2}\right)} \displaystyle\sum_{j=0}^{p^{n-1}-1} \left(\sum_{a=0}^{p-1} \left[\frac{\omega(a)\gamma^j}{p^n} \right]^+ \right) (T+1)^j & 2 \nmid n. \end{cases}$$

Proof. As in Proposition 4.12, we choose representatives of $\mathbf{Z}_p^\times$ mod p^n, namely $\{\omega(a)\gamma^j\}$ with $1 \leq a \leq p-1$ and $0 \leq j \leq p^{n-1}-1$ where $\omega(a)$ the Teichmüller character. Then we have,

$$S_n(T) = \sum_{j=0}^{p^{n-1}-1} \sum_{a=0}^{p-1} \mu_{f,\alpha}^+(\omega(a)\gamma^j + p^n\mathbf{Z}_p) \cdot (T+1)^j \tag{8}$$

and

$$\mu_{f,\alpha}^+(\omega(a)\gamma^j + p^n\mathbf{Z}_p) = \frac{1}{\alpha^n} \left[\frac{\omega(a)\gamma^j}{p^n} \right]^+ - \frac{1}{\alpha^{n+1}} \left[\frac{\omega(a)\gamma^j}{p^{n-1}} \right]^+ . \tag{9}$$

Combining (8) and (9) and writing everything in terms of 1 and α gives the above formulas for G_n^+ and G_n^- (recalling that $\alpha^2 = -p$). □

Proof of 7.8. Note that for $1 \leq k \leq n-1$, $S_n(\zeta_k - 1) = L_p(E, \alpha, \zeta_k - 1)$ since the Riemann sum perfectly approximates the integral. We know that $G^+(\zeta_{2k} - 1) = 0$ and hence, we have that $G_n^+(\zeta_{2k} - 1) = 0$ for $1 \leq k \leq \left[\frac{n-1}{2}\right]$.

Therefore, we can write

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

But from Lemma 7.10, we see that $p^{\left[\frac{n+1}{2}\right]} \cdot G_n^+ \in \mathbf{Z}_p[[T]]$. Hence g_n^+ has integral coefficients.

Taking limits yields,

$$G^+(T) = \Phi^+(T) \cdot g^+(T) \quad \text{with} \quad g^+(T) \in \mathbf{Z}_p[[T]].$$

Similarly for $g^-(T)$ and for $p = 2$. □

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

Theorem 7.11. *Let $E/\mathbf{Q}$ be an elliptic curve and p a prime number. Then for only finitely many χ of p-power order, we have that $L(E, \chi, 1) = 0$.*

Proof. See [18] □

Corollary 7.12. *$L_p(E, \alpha, T)$, $g^+(T)$ and $g^-(T)$ are all non-zero functions.*

Corollary 7.13. *Let $E/\mathbf{Q}$ be an elliptic curve and p a prime so that $a_p = 0$. Then $L_p(E, \alpha, T)$ and $L_p(E, \overline{\alpha}, T)$ have only finitely many common zeroes.*

Proof. Any common zero of $L_p(E, \alpha, T)$ and $L_p(E, \overline{\alpha}, T)$ is a zero of both $G^+(T)$ and $G^-(T)$. By Theorem 7.11, there are only finitely many zeroes of $L_p(E, \alpha, T)$ in the form $\zeta_n - 1$. Further, by Theorem 7.1 and Corollary 7.12, there are only finitely many zeroes of $G^+(T)$ and $G^-(T)$ not in the form $\zeta_n - 1$. This completes the argument.

□

7.2.3 Functional equations for $g^+(T)$ and $g^-(T)$

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

$$L_p(E, \alpha, \chi_u) = \epsilon_N \cdot u^{-\log_\gamma \langle N \rangle} \cdot L_p(E, \alpha, \chi_{u^{-1}})$$

where ϵ_N is the negative of then sign of f_E (i.e. $w_N(f_E) = -\epsilon_N f_E$). For ease of notation, let $c = -\log_\gamma \langle N \rangle$. In terms of $L_p(E, \alpha, T)$ we have

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

Both g^+ and g^- satisfy a functional equation of this type.

Theorem 7.14. *With g^+ and g^- as in Theorem 7.1,*

$$g^+(T) = \epsilon_N \cdot (1+T)^c \cdot g^+\left(\frac{1}{1+T} - 1\right) \quad \textit{and}$$
$$g^-(T) = \epsilon_N \cdot (1+T)^c \cdot g^-\left(\frac{1}{1+T} - 1\right).$$

Proof. From Lemma 6.4, we know that

$$\Phi^+\left(\frac{1}{1+T} - 1\right) = \Phi^+(T) \quad \text{and} \quad \Phi^-\left(\frac{1}{1+T} - 1\right) = \Phi^-(T).$$

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

$$\Phi^+(T) \cdot \left(g^+(T) - \epsilon_N (1+T)^c g^+\left(\frac{1}{1+T} - 1\right)\right)$$
$$= \Phi^-(T) \cdot \left(g^-(T) - \epsilon_N (1+T)^c g^-\left(\frac{1}{1+T} - 1\right)\right) \cdot \alpha.$$

But the non-zero coefficients of the LHS have valuations in $\mathbf{Z}$ while on the RHS each has valuation $\frac{n}{2}$ with n an odd integer. This forces both sides to be identically zero and the functional equations for g^+ and g^- follow. □

8 Consequences of main result for elliptic curves

Let $\mathbf{Q}_\infty/\mathbf{Q}$ be the cyclotomic $\mathbf{Z}_p$ extension and let $\mathbf{Q}_n$ be the unique subextension with degree p^n. In this section we will discuss the analytic behavior of $E(\mathbf{Q}_n)$ and $\text{Ш}(E/\mathbf{Q}_n)_{p^\infty}$ as n grows: i.e the behavior as predicted by the Birch and Swinnerton-Dyer conjecture. This behavior will be described by the Iwasawa invariants of the p-adic L-function of E.

8.1 Iwasawa invariants of p-adic L-functions

Let p be an ordinary prime and hence $L_p(E,T) \in \mathbf{Z}_p[[T]] \otimes \mathbf{Q}_p$ (conjecturally in $\mathbf{Z}_p[[T]]$). By the p-adic Weierstrass preparation theorem, we can uniquely write,

$$L_p(E,T) = p^\mu \cdot P(T) \cdot U(T)$$

where μ is an integer, $P(T)$ is a distinguished polynomial of degree λ and $U(T)$ is a unit power series. The values of μ and λ are the Iwasawa invariants of $L_p(E,T)$.

If p is supersingular, however, it does not make sense to discuss the μ and λ invariants of $L_p(E,\alpha,T)$. Instead, we can discuss the μ and λ invariants of $g^\pm$ from Theorem 7.1. Precisely, write

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

where $\mu^\pm$ is a non-negative integer (this uses Theorem 7.8), $P^\pm$ is a distinguished polynomial of degrees $\lambda^\pm$ and $U^\pm$ are unit power series.

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

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

8.2 Growth of the Mordell-Weil group in the cyclotomic direction

Let E be an elliptic curve over $\mathbf{Q}$ and let p be any prime number (not necessarily supersingular for E).

Definition 8.1. The (p-adic) analytic rank of $E(\mathbf{Q}_n)$ is defined by

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

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

Remark 8.2. This should conjecturally agree with the (complex) analytic rank of $E(\mathbf{Q}_n)$ defined by the order of vanishing of the complex L-series $L(E/\mathbf{Q}_n, s)$ at 1 as long as E has good reduction at p.

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

Lemma 8.3. *Let $E/\mathbf{Q}$ be an elliptic curve and p a supersingular prime for E with $a_p = 0$. Then,*

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

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

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

from which the result follows. □

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

Lemma 8.4. *Let $E/\mathbf{Q}$ be an elliptic curve and $p \equiv 3 \pmod 4$ a supersingular prime for E. If ζ is a p^n-th root of unity then*

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

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

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

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

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

which yields the result. □

By a theorem of Rohrlich (Theorem 7.11), it is known that $E(\mathbf{Q}_\infty)$ has finite analytic rank. (This is now known algebraically via Kato's Euler system even in the supersingular case - see [19].)

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

Corollary 8.5. *For $p \equiv 3 \pmod 4$ a supersingular prime of E such that $a_p = 0$,*

$$r^{an}(E(\mathbf{Q}_\infty)) \leq \lambda^+_{MW} + \lambda^-_{MW}.$$

Proof. It will suffice to prove the following claim.

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

Let $m = \operatorname{ord}_{\zeta_n - 1} L_p(E, \alpha, T)$ and we shall prove this by induction on m. For $m = 1$,

$$L_p(f, \alpha, T) = g^+(T) \cdot \Phi^+(T) + g^-(T) \cdot \Phi^-(T) \cdot \alpha$$

implies

$$L_p(E, \alpha, \zeta_{2k-1} - 1) = g^+(\zeta_{2k-1} - 1) \cdot \Phi^+(\zeta_{2k-1} - 1) \text{ and}$$
$$L_p(E, \alpha, \zeta_{2k} - 1) = g^-(\zeta_{2k} - 1) \cdot \Phi^-(\zeta_{2k} - 1) \cdot \alpha.$$

Since $\Phi^+(\zeta_{2k-1} - 1)$ and $\Phi^-(\zeta_{2k} - 1)$ are both non-zero, $L_p(E, \alpha, T)$ vanishing at some root of unity implies that $g^+(T)$ or $g^-(T)$ will vanish at that root of unity.

Now for $m > 1$, from Lemma 8.4 we have that both $L_p^{(m)}(E, \alpha, T)$ and $L_p^{(m)}(E, \overline{\alpha}, T)$ vanish to order m at $\zeta_n - 1$. Assume for now that n is odd. Then $G^+(T) = L_p^{(m)}(E, \alpha, T) + L_p^{(m)}(E, \overline{\alpha}, T)$ vanishes at least to order m at $\zeta_n - 1$. Since $G^+(T) = g^+(T) \cdot \Phi^+$ and Φ^+ is non-zero at $\zeta_n - 1$, we have that $g^+(T)$ also vanishes at least to order m at $\zeta_n - 1$. The case of n even follows in the same manner. □

Remark 8.6. Unlike in the ordinary case, equality is not always achieved in the above corollary. For example, if $E(\mathbf{Q}_\infty) = E(\mathbf{Q}) = \mathbf{Z}$ then $r^{\mathrm{an}} = \lambda^+_{MW} = \lambda^-_{MW} = 1$.

The following corollary makes use of Kato's Euler system and Theorem 7.8.

Corollary 8.7. *Suppose that E does not admit complex multiplication and p is an odd prime with $a_p = 0$ such that $p \nmid \frac{L(E,1)}{\Omega_E}$. Then $E(\mathbf{Q}_\infty)$ is finite.*

Proof. We have that

$$L_\alpha(0) = \left(1 - \frac{1}{\alpha}\right)^2 \frac{L(E,1)}{\Omega_E}$$

and hence

$$\Phi^+(0) \cdot g^+(0) + \Phi^-(0) \cdot g^-(0) \cdot \alpha = \left(\frac{p-1}{p} + \frac{2}{p} \cdot \alpha\right) \frac{L(E,1)}{\Omega_E}. \tag{10}$$

Note that $\Phi^+(0) = \Phi^-(0) = 1/p$. Hence, both $g^+(0)$ and $g^-(0)$ are units (since p is odd). This forces the Iwasawa invariants of g^+ and g^- to be zero and in particular $\lambda^\pm_{MW} = 0$. Therefore, $L(E, \chi, 1) \neq 0$ for all χ of p-power order and conductor. Then from Kato's Euler system (see [19, Theorem 8.1]), we have that $E(\mathbf{Q}_\infty)$ is finite. □

Remark 8.8. The above corollary is false for $p = 2$. If $E = X_0(19)$ then $\dfrac{L(E,1)}{\Omega_E} = \dfrac{1}{3}$. However, $E(\mathbf{Q}(\sqrt{2}))$ is infinite and $\mathbf{Q}(\sqrt{2})$ is the first step of the cyclotomic $\mathbf{Z}_2$-extension.

8.3 Growth of the Tate-Shafarevich group in the cyclotomic direction

Let E be an elliptic curve over $\mathbf{Q}$ with supersingular reduction at p. As in the previous section, let $\mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$ extension of $\mathbf{Q}$ with $\mathbf{Q}_n$ the unique subextension with degree p^n over $\mathbf{Q}$. In this section, we will derive asymptotic formulas for the p-part of the analytic size of $Ш(E/\mathbf{Q}_n)$ (that is, the size of $Ш(E/\mathbf{Q}_n)_{p^\infty}$ as predicted by the Birch and Swinnerton-Dyer conjecture).

In [9], Kurihara has derived formulas in the supersingular case for the algebraic size of the p-part of $Ш(E/\mathbf{Q}_n)$ when p does not divide $\frac{L(E,1)}{\Omega_E}$ and the Tamagawa numbers of E (plus a few more technical hypotheses). In this situation, the analytic formulas derived below coincide with his algebraic formulas.

We will follow the same method used in section 3.3. By picking n so large that $E(\mathbf{Q}_{n+1}) = E(\mathbf{Q}_n)$, $\mathrm{Tam}(E/\mathbf{Q}_{n+1}) = \mathrm{Tam}(E/\mathbf{Q}_n)$ and $L(E,\chi,1) \neq 0$ for χ of conductor p^n, we have that

$$\frac{\#Ш^{\mathrm{an}}(E/\mathbf{Q}_{n+1})}{\#Ш^{\mathrm{an}}(E/\mathbf{Q}_n)} = \left(\prod_{\chi} \frac{L(E/\mathbf{Q},\chi,1)}{\Omega_{E/\mathbf{Q}}}\right) \cdot c_n \tag{11}$$

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

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

where r is the rank of E over $\mathbf{Q}_\infty$. Recall that the number $\#Ш^{\mathrm{an}}(E/\mathbf{Q}_n)$ is defined to be the size that the Birch and Swinnerton-Dyer conjecture predicts for the Tate-Shafarevich group (see section 3.3).

To compute the valuation of the product in (11) we will use the p-adic L-functions of E and Theorem 7.1. Compare the following lemma to [9, Prop 2.1].

Lemma 8.9. *Let $E/\mathbf{Q}$ be an elliptic curve and p a prime such that $a_p = 0$. Let χ be a character of $\mathbf{Z}_p^\times$ that factors thru $1 + q\mathbf{Z}_p$ and sends γ to a p^n-th root of unity. Denote by $\tau(\chi)$ the corresponding Gauss sum. Then for p odd and n large enough,*

$$\mathrm{ord}_p\left(\tau(\chi) \cdot \frac{L(E,\chi^{-1},1)}{\Omega_E}\right) = \begin{cases} \dfrac{p^{n-1} - p^{n-2} + \cdots + p - 1 + \lambda^-}{p^{n-1}(p-1)} + \mu^- & 2 \mid n \\[2ex] \dfrac{p^{n-1} - p^{n-2} + \cdots + p^2 - p + \lambda^+}{p^{n-1}(p-1)} + \mu^+ & 2 \nmid n. \end{cases}$$

For $p = 2$, the Iwasawa invariants of g^+ and g^- are interchanged.

Proof. We argue for p and n odd. From the interpolation property (Proposition 4.14) we have that,

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

Hence,

$$\tau(\chi)\cdot\frac{L(E,\chi^{-1},1)}{\Omega_E}=\pm\alpha^{n+1}\cdot L_p(E,\alpha,\zeta_n-1) \tag{12}$$

as $\tau(\chi)\cdot\tau(\overline{\chi})=\pm p^{n+1}$. To compute the valuation of the RHS we use Theorem 7.1. We have that,

$$L_p(E,\alpha,\zeta_n-1)=\Phi^+(\zeta_n-1)\cdot g^+(\zeta_n-1) \tag{13}$$

As usual, write $g^+=p^{\mu^+}\cdot P^+\cdot U^+$. Since P^+ is a distinguished polynomial, if $\lambda^+\cdot\mathrm{ord}_p(\zeta_n-1)<1$ then the leading term of P^+ dominates and

$$\mathrm{ord}_p(g^+(\zeta_n-1))=\mu^++\frac{\lambda^+}{p^{n-1}(p-1)}. \tag{14}$$

To compute the valuation of $\Phi^+(\zeta_n-1)$, we compute the valuations of $\Phi_{2k}(\zeta_n)$ for all k. Note that

$$\Phi_k(T)=\frac{T^{p^k}-1}{T^{p^{k-1}}-1}=1+T^{p^{k-1}}+\cdots+T^{(p-1)p^{k-1}}.$$

If $2k<n$ then

$$\Phi_{2k}(\zeta_n)=\frac{(\zeta_n)^{p^{2k}}-1}{(\zeta_n)^{p^{2k-1}}-1}=\frac{\zeta_{n-2k}-1}{\zeta_{n-2k+1}-1}$$

and hence

$$\mathrm{ord}_p(\Phi_{2k}(\zeta_n))=\frac{p^{2k}-p^{2k-1}}{p^{n-1}(p-1)}.$$

For $2k>n$,

$$\Phi_{2k}(\zeta_n)=1+(\zeta_n)^{p^{2k-1}}+\cdots+(\zeta_n)^{p^{2k-1}(p-1)}=p$$

since $2k-1\geq n$. Hence,

$$\mathrm{ord}_p\left(\frac{\Phi_{2k}(\zeta_n)}{p}\right)=0.$$

Since $\Phi^+(T)=\frac{1}{p}\cdot\prod_{k=1}^{\infty}\frac{\Phi_{2k}(T+1)}{p}$,

$$\mathrm{ord}_p(\Phi^+(\zeta_n-1))=\frac{p^{n-1}-p^{n-2}+\cdots+p^2-p}{p^{n-1}(p-1)}-\frac{n+1}{2}.$$

Finally from (12),(13) and (14) we have that

$$\mathrm{ord}_p(\tau(\chi)\cdot L(E,\chi^{-1},1))=\frac{p^{n-1}-p^{n-2}+\cdots+p^2-p+\lambda^+}{p^{n-1}(p-1)}+\mu^+.$$

□

The following proposition describes the change in size of the p-part of the (analytic) Tate-Shafarevich group in each step of the cyclotomic $\mathbf{Z}_p$-extension.

Proposition 8.10. *Let*

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

Then

$$f_n^{an} = \begin{cases} p^{n-1} - p^{n-2} + \cdots + p - 1 + (\lambda^- - r) + p^{n-1}(p-1)\cdot\mu^- & 2 \mid n \\ p^{n-1} - p^{n-2} + \cdots + p^2 - p + (\lambda^+ - r) + p^{n-1}(p-1)\cdot\mu^+ & 2 \nmid n \end{cases}$$

for p odd and for $p = 2$ the roles of g^+ and g^- are reversed.

Proof. This follows from Lemma 8.9, (11) and the fact that

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

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

Remark 8.11. When p is ordinary,

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

as described in section 3.3. Here $\lambda^{\mathrm{an}} - r$ is conjecturally equal to $\lambda^{\mathrm{an}}_{\text{Ш}}$.

However, $\lambda^+ - r$ will not in general be equal to $\lambda^+_{\text{Ш}}$ since λ^+_{MW} contains information about the rank on every other level of the tower. It need not even be $\lambda^+_{\text{Ш}} - \lambda^-_{MW}$ as P^+_{MW} need not be relatively prime to P^-_{MW}.

We will now combine the above formulas to give an asymptotic formula for $\mathrm{ord}_p(\#\text{Ш}^{\mathrm{an}}(E/\mathbf{Q}_n))$.

Proposition 8.12. *Let*

$$e_n^{an} = \mathrm{ord}_p(\#\text{Ш}^{an}(E/\mathbf{Q}_n)).$$

Then for n large enough,

$$e_n = \begin{cases} p^{n-1} + p^{n-3} + \cdots + p + \frac{n}{2}\cdot(\lambda^- + \lambda^+ - 2r - 1) + \\ \sum_{k=1}^{\frac{n}{2}}\left(p^{2k-1}(p-1)\cdot\mu^- + p^{2k-2}(p-1)\cdot\mu^+\right) + \nu & 2 \mid n \\ \\ p^{n-1} + p^{n-3} + \cdots + p^2 + \frac{n-1}{2}\cdot(\lambda^- + \lambda^+ - 2r - 1) + \\ \sum_{k=1}^{\frac{n-1}{2}} p^{2k-1}(p-1)\cdot\mu^- + \sum_{k=1}^{\frac{n+1}{2}} p^{2k-2}(p-1)\cdot\mu^+ + \nu' & 2 \nmid n \end{cases}$$

where ν and ν' are non-negative constants independent of n.

Proof. This is just a consequence of Proposition 8.10.

□

In the ordinary case, when $E[p]$ is irreducible Greenberg has conjectured that the μ-invariant vanishes (see [4, Conjecture 1.11]). The fact that $E[p]$ is always irreducible when p is supersingular along with some numerical data (see section 9) leads us to extend his conjecture to the supersingular case.

Conjecture 8.13. Let $E/\mathbf{Q}$ be an elliptic curve and p a prime such that $a_p = 0$. Then $\mu^+ = \mu^- = 0$.

The above formulas simplify greatly if this conjecture is true. In this case, following Y. Ihara's suggestion in [9], we can reformulate the above equations using rational invariants μ and λ.

Proposition 8.14. *Assume $\mu^+ = \mu^- = 0$. Then*

$$e_n = [\mu p^n + \lambda n + \nu] \quad \textit{with} \quad \mu = \frac{p}{p^2-1} \quad , \quad \lambda = \frac{\lambda^+ + \lambda^- - 1}{2} - r$$

and where ν is some constant independent of n.

We will now put ourselves in the setting of [9] and assume that p is odd and does not divide $\frac{L(E,1)}{\Omega_E}$. In this case, μ^+, μ^-, λ^+ and λ^- all vanish and the above analytic formulas compare nicely with the algebraic formulas of Kurihara.

Proposition 8.15. *Assume that p is odd, E does not admit complex multiplication and*

$$p \nmid \frac{L(E,1)}{\Omega_E}.$$

Then for all $n \geq 1$,

$$\#\text{Ш}^{an}(E/\mathbf{Q}_n)_{p^\infty} = \begin{cases} p^{n-1} + p^{n-3} + \cdots + p - \dfrac{n}{2} & 2 \mid n \\ p^{n-1} + p^{n-3} + \cdots + p^2 - \dfrac{n-1}{2} & 2 \nmid n. \end{cases}$$

Proof. As in Corollary 8.7, we have that $\mu^\pm = \lambda^\pm = 0$. Also from Corollary 8.7, we know that $E(\mathbf{Q}_\infty)$ is finite and hence $r = 0$. Note that the condition "n large enough" in Lemma 8.9 reduces to $n \geq 1$ when $\lambda^+ = \lambda^- = 0$ and we can take $\nu = \nu' = 0$. Therefore, the formulas of Proposition 8.12 reduce to the formulas we are seeking.

□

Remark 8.16. Again when $p = 2$ the above proposition is false. Indeed, in this case, $\text{ord}_2(g^+(0)) = 0$ and $\text{ord}_2(g^-(0)) = 2$. Hence, one of μ^- or λ^- is necessarily positive.

9 Tables of Iwasawa invariants for supersingular curves

We conclude with tables of values of $\mu^{\pm}$,$\lambda^{\pm}_{\text{III}}$ and $\lambda^{\pm}_{MW}$ for various elliptic curves and supersingular primes p with $a_p = 0$. The first series of tables lists these invariants for all strong Weil curves of conductor less than 1000. These curves are indexed by William Stein's notation (which differs slightly from Cremona's notation for conductor less than 450 but is ordered more systematically).

In the column labeled "roots" the general entry $(r : s)$ represents r roots of slope s. A small dot next to such an entry signifies that these are p-cyclotomic roots. The question marks appearing sporadically are unfortunate and hopefully will be removed soon (after many more hours of computer calculations). For these cases, a fine enough Riemann sum has not yet been calculated to ensure the accuracy of the $\lambda^{\pm}$-invariant.

If the Iwasawa invariants of a curve and a prime are all zero they are not included in the table. If the curve is rank 1 over **Q** and the only non-zero invariant at p is $\lambda^{\pm}_{MW} = 1$ then this data is also not included in the table. Furthermore, the root at 0 for any rank 1 curve over **Q** is not included in the "roots" column except for curves of rank 2.

The second set of tables lists data for a fixed prime and a base curve twisted by various quadratic characters. The tables are in the same format as described above. Currently we have included the strong Weil curves $14A$ with $p = 5$, $17A$ with $p = 3$, $19A$ with $p = 2$, $27A$ with $p = 2$ and 5, $32A$ with $p = 3$ and $40A$ with $p = 3$. Data for the twists by quadratic characters with positive discriminant less than 200 is listed for all of these curves. For some of them, the twists by characters with negative discriminant up to -200 are also listed. Again, when the invariants are zero or are simply non-zero because of the sign of the functional equation the data is not listed.

9.1 Curves with conductor less than 1000

Curve	r	p	$\lambda^{+}_{\text{Ш}}$	λ^{+}_{MW}	roots	$\lambda^{-}_{\text{Ш}}$	λ^{-}_{MW}	roots
19A	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
27A	0	2	0	0	-	0	5	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{4})^{\cdot}$
35A	0	2	0	0	-	0	5	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{4})^{\cdot}$
37B	0	2	0	0	-	0	5	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{4})^{\cdot}$
43A	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
51A	0	2	0	0	-	14	1	$(1{:}1)^{\cdot}$ $(14{:}\frac{1}{14})$
77A	1	2	1	1	$(1{:}1)$	2	1	$(2{:}\frac{1}{2})$
77C	0	2	0	2	$(2{:}\frac{1}{2})^{\cdot}$	2	1	$(1{:}1)^{\cdot}$ $(2{:}1)$
91A	1	3	0	1	-	0	7	$(6{:}\frac{1}{6})^{\cdot}$
91B	1	2	5	11	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$ $(4{:}\frac{1}{2})$ $(8{:}\frac{1}{8})^{\cdot}$	0	1	-
101A	1	2	1	3	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$	0	1	-
106A	1	7	2	1	$(2{:}\frac{1}{2})$	0	1	-
121A	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
123A	1	2	1	3	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$	0	1	-
129A	1	2	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	2	$(1{:}1)^{\cdot}$
131A	1	2	1	1	$(1{:}1)$	0	1	-
141A	1	2	1	1	$(1{:}1)$	0	1	-
143A	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
145A	1	3	0	1	-	0	7	$(6{:}\frac{1}{6})^{\cdot}$
153D	1	2	0	1	-	10	6	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{4})^{\cdot}$ $(10{:}\frac{1}{5})$
154C	0	3	2	0	$(2{:}\frac{1}{2})$	2	0	$(2{:}\frac{1}{2})$
155A	1	2	3	3	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$	0	1	- $(2{:}\frac{1}{2})$
163A	1	2	5	3	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$ $(4{:}\frac{1}{4})$	0	1	-
?163A	1	3	2	3	$(2{:}\frac{3}{2})$ $(2{:}\frac{1}{2})^{\cdot}$	0	1	-
171D	1	2	1	1	$(1{:}1)$	0	5	$(4{:}\frac{1}{4})^{\cdot}$
175A	1	2	0	1	-	4	2	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{2})$
185C	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
187B	0	2	4	0	$(4{:}\frac{1}{4})$	4	1	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{2})$

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^+_{\text{Ш}}$	λ^+_{MW}	roots	$\lambda^-_{\text{Ш}}$	λ^-_{MW}	roots
189B	0	2	0	0	-	0	5	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{4})^{\cdot}$
189D	1	2	1	3	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$	0	1	-
?197A	1	5	2	5	$(2{:}1)$ $(4{:}\frac{1}{4})^{\cdot}$	0	1	-
201B	1	7	2	1	$(2{:}\frac{1}{2})$	0	1	-
205C	1	11	0	1	-	4	1	$(4{:}\frac{1}{4})$
207A	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
209A	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
215A	1	2	2	1	$(2{:}\frac{1}{2})$	0	2	$(1{:}1)^{\cdot}$
219C	1	2	1	1	$(1{:}1)$	0	1	-
225A	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
225A	1	11	0	1	-	2	1	$(2{:}\frac{1}{2})$
225B	0	2	1	0	$(1{:}1)$	2	0	$(2{:}\frac{3}{2})$
238A	1	3	2	3	$(2{:}\frac{1}{2})^{\cdot}$ $(2{:}\frac{1}{2})$	0	1	-
243A	1	2	7	1	$(1{:}1)$ $(6{:}\frac{1}{6})$	0	1	-
243B	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
245B	1	2	1	1	$(1{:}1)$	6	1	$(6{:}\frac{1}{3})$
248C	1	3	0	1	-	4	1	$(4{:}\frac{1}{4})$
254A	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
254B	0	3	0	2	$(2{:}\frac{1}{2})^{\cdot}$	4	0	$(4{:}\frac{1}{4})$
256A	1	3	0	1	-	0	7	$(6{:}\frac{1}{6})^{\cdot}$
256B	1	7	2	1	$(2{:}\frac{1}{2})$	0	1	-
259A	0	3	0	2	$(2{:}\frac{1}{2})^{\cdot}$	6	0	$(6{:}\frac{1}{6})$
267A	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
267B	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
269A	1	2	1	1	$(1{:}1)$	1	2	$(1{:}1)^{\cdot}$ $(1{:}1)$
272A	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
?272D	1	11	0	1	-	4	1	$(4{:}\frac{1}{4})$
274A	1	5	0	5	$(4{:}\frac{1}{4})^{\cdot}$	0	1	-
290A	1	3	4	1	$(4{:}\frac{1}{4})$	0	1	-
291A	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
298A	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^+_{\text{Ш}}$	λ^+_{MW}	roots	$\lambda^-_{\text{Ш}}$	λ^-_{MW}	roots
?298B	1	11	0	1	-	2	1	$(2{:}\frac{1}{2})$
303A	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
306B	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
307A	0	2	0	0	-	6	1	$(1{:}1)^{\cdot}$ $(6{:}\frac{1}{6})$
314A	1	3	6	1	$(6{:}\frac{1}{6})$	0	1	-
315B	0	2	0	0	-	0	5	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{4})^{\cdot}$
320A	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
323A	0	2	0	0	-	0	5	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{4})^{\cdot}$
325A	1	2	1	3	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$	0	1	-
325E	1	2	3	1	$(2{:}2)$ $(1{:}1)$	0	1	-
326A	1	3	4	1	$(4{:}\frac{1}{4})$	0	1	-
333D	1	2	1	1	$(1{:}1)$	0	1	-
333D	1	5	2	1	$(2{:}1)$	0	1	-
335A	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
339B	1	2	1	1	$(1{:}1)$	0	1	-
?342D	1	11	0	1	-	2	1	$(2{:}\frac{1}{2})$
345A	0	2	1	0	$(1{:}1)$	2	0	$(2{:}\frac{3}{2})$
345E	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
348B	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
354A	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
355A	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
357A	0	2	2	0	$(2{:}\frac{1}{2})$	16	1	$(1{:}1)^{\cdot}$ $(16{:}\frac{1}{8})$
357B	1	2	1	1	$(1{:}1)$	16	1	$(16{:}\frac{1}{8})$
361A	1	2	0	1	-	2	2	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
361A	1	3	2	3	$(2{:}\frac{1}{2})^{\cdot}$ $(2{:}\frac{1}{2})$	0	1	-
361B	0	2	1	0	$(1{:}1)$	3	1	$(1{:}1)^{\cdot}$ $(1{:}1)$ $(2{:}\frac{1}{2})$
368A	1	3	2	1	$(2{:}\frac{1}{2})$	0	1	-
369B	1	2	4	1	$(4{:}\frac{1}{4})$	0	2	$(1{:}1)^{\cdot}$
370A	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
371B	0	3	2	0	$(2{:}\frac{1}{2})$	2	0	$(2{:}\frac{1}{2})$
374A	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^{+}_{Ш}$	λ^{+}_{MW}	roots	$\lambda^{-}_{Ш}$	λ^{-}_{MW}	roots
377A	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
380B	1	3	0	1	-	2	1	$(2{:}1)$
381B	1	2	1	1	$(1{:}1)$	0	1	-
385A	1	3	2	1	$(2{:}\frac{1}{2})$	0	1	-
387C	0	2	4	0	$(4{:}\frac{1}{4})$	2	1	$(1{:}1)^{\cdot}$ $(2{:}1)$
392E	1	3	2	1	$(2{:}\frac{1}{2})$	0	1	-
399A	1	5	0	1	-	4	1	$(4{:}\frac{1}{4})$
399B	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
400A	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
405A	1	2	1	3	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$	0	1	-
405D	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
406A	1	3	4	1	$(4{:}\frac{1}{4})$	0	1	-
410B	1	3	0	1	-	2	1	$(2{:}1)$
410D	0	3	2	0	$(2{:}\frac{1}{2})$	4	0	$(4{:}\frac{1}{4})$
422A	1	3	4	1	$(4{:}\frac{1}{4})$	2	1	$(2{:}\frac{1}{2})$
423E	1	2	0	1	-	6	2	$(1{:}1)^{\cdot}$ $(6{:}\frac{1}{2})$
423F	1	7	2	1	$(2{:}\frac{1}{2})$	0	1	-
427A	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
427B	0	2	0	0	-	8	1	$(1{:}1)^{\cdot}$ $(8{:}\frac{1}{8})$
429A	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
429A	1	7	2	1	$(2{:}\frac{1}{2})$	0	1	-
?434A	1	3	0	1	-	4	1	$(2{:}\frac{5}{2})$ $(2{:}\frac{1}{2})$
435A	0	2	0	0	-	6	1	$(1{:}1)^{\cdot}$ $(6{:}\frac{1}{6})$
435B	0	2	0	0	-	6	1	$(1{:}1)^{\cdot}$ $(6{:}\frac{1}{6})$
437B	1	2	1	1	$(1{:}1)$	3	2	$(1{:}1)^{\cdot}$ $(1{:}1)$ $(2{:}\frac{1}{2})$
438A	1	5	2	1	$(2{:}1)$	0	1	-
438C	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
440B	0	3	0	2	$(2{:}\frac{1}{2})^{\cdot}$	2	0	$(2{:}\frac{1}{2})$
440D	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
441A	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
441B	0	2	1	0	$(1{:}1)$	2	0	$(2{:}\frac{3}{2})$

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^+_{\text{Ш}}$	λ^+_{MW}	roots	$\lambda^-_{\text{Ш}}$	λ^-_{MW}	roots
442E	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	2	1	$(2{:}\frac{1}{2})$
443A	1	2	1	3	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$	0	1	-
446A	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
448A	1	3	0	1	-	6	1	$(2{:}1)$ $(4{:}\frac{1}{4})$
448G	1	3	2	1	$(2{:}\frac{1}{2})$	0	1	-
448H	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
451A	1	2	1	1	$(1{:}1)$	2	1	$(2{:}\frac{1}{2})$
455A	1	3	0	1	-	6	1	$(2{:}\frac{1}{2})$ $(4{:}\frac{1}{4})$
455B	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
459C	0	2	0	0	-	6	1	$(1{:}1)^{\cdot}$ $(6{:}\frac{1}{6})$
459F	0	2	0	0	-	6	1	$(1{:}1)^{\cdot}$ $(6{:}\frac{1}{6})$
?459H	1	11	0	1	-	2	1	$(2{:}\frac{1}{2})$
467A	1	2	1	11	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$ $(8{:}\frac{1}{8})^{\cdot}$	0	1	-
473A	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
475A	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
477A	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
481A	1	3	0	1	-	4	1	$(4{:}\frac{1}{4})$
485A	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
485B	1	2	1	3	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$	1	2	$(1{:}1)^{\cdot}$ $(1{:}1)$
485B	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
486A	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
?494A	1	11	0	1	-	2	1	$(2{:}\frac{1}{2})$
496A	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	7	$(6{:}\frac{1}{6})^{\cdot}$
497A	1	5	4	1	$(4{:}\frac{1}{4})$	4	1	$(4{:}\frac{1}{4})$
505A	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
506D	1	3	2	1	$(2{:}\frac{1}{2})$	0	1	-
513A	1	5	0	1	-	6	1	$(6{:}\frac{1}{6})$
514A	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
517B	0	2	4	0	$(4{:}\frac{1}{4})$	4	1	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{2})$
522G	0	11	2	0	$(2{:}\frac{1}{2})$	0	0	-

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^{+}_{\text{Ш}}$	λ^{+}_{MW}	roots	$\lambda^{-}_{\text{Ш}}$	λ^{-}_{MW}	roots
528A	1	5	0	5	$(4{:}\frac{1}{4})^{\cdot}$	0	1	-
528G	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
537B	0	2	1	0	$(1{:}1)$	2	0	$(2{:}\frac{3}{2})$
537C	0	2	1	0	$(1{:}1)$	2	0	$(2{:}\frac{3}{2})$
539A	0	2	4	0	$(4{:}\frac{1}{4})$	4	1	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{2})$
539B	0	2	4	0	$(4{:}\frac{1}{4})$	4	1	$(1{:}1)^{\cdot}$ $(4{:}\frac{1}{2})$
542A	0	7	2	0	$(2{:}\frac{1}{2})$	0	0	-
542B	1	5	0	5	$(4{:}\frac{1}{4})^{\cdot}$	0	1	-
544A	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
550G	1	7	2	1	$(2{:}\frac{1}{2})$	0	1	-
?552E	1	11	0	1	-	2	1	$(2{:}\frac{1}{2})$
555A	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
555B	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
560D	1	3	6	1	$(6{:}\frac{1}{6})$	0	1	-
561A	0	2	1	0	$(1{:}1)$	2	0	$(2{:}\frac{3}{2})$
561B	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
566A	1	3	0	1	-	2	1	$(2{:}1)$
571A	0	2	2	0	$(2{:}1)$	4	1	$(1{:}1)^{\cdot}$ $(2{:}1)$ $(2{:}\frac{1}{2})$
575A	1	3	4	3	$(2{:}\frac{1}{2})^{\cdot}$ $(4{:}\frac{1}{4})$	0	1	-
575B	1	3	6	1	$(6{:}\frac{1}{6})$	0	1	-
?576H	1	11	0	1	-	2	1	$(2{:}\frac{1}{2})$
580B	1	3	4	3	$(2{:}\frac{1}{2})^{\cdot}$ $(4{:}\frac{1}{4})$	2	1	$(2{:}\frac{3}{2})$
?582A	1	5	0	1	-	4	1	$(2{:}1)$ $(2{:}\frac{1}{2})$
585B	0	2	1	0	$(1{:}1)$	2	0	$(2{:}\frac{3}{2})$
585D	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
588B	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
590C	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
591A	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
591A	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
598A	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
598A	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^{+}_{\text{Ш}}$	λ^{+}_{MW}	roots	$\lambda^{-}_{\text{Ш}}$	λ^{-}_{MW}	roots
608A	1	3	0	1	-	4	1	$(4{:}\frac{1}{4})$
608D	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
608F	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
?610B	1	7	2	1	$(2{:}1)$	0	1	-
615A	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
615B	1	2	4	1	$(4{:}\frac{1}{4})$	0	2	$(1{:}1)^{\cdot}$
616A	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
616E	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
622A	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
624A	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
626A	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
627A	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
627B	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
629A	1	3	0	1	-	4	1	$(4{:}\frac{1}{2})$
629C	1	2	1	3	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$	4	5	$(4{:}\frac{1}{4})^{\cdot}$ $(4{:}\frac{1}{4})$
?629C	1	5	0	1	-	2	1	$(2{:}1)$
629D	1	3	0	1	-	2	1	$(2{:}1)$
635A	1	2	1	1	$(1{:}1)$	0	1	-
637A	1	3	0	1	-	0	7	$(6{:}\frac{1}{6})^{\cdot}$
637B	0	2	18	0	$(2{:}\frac{1}{2})$ $(16{:}\frac{1}{16})$	2	1	$(2{:}\frac{3}{2})$ $(1{:}1)^{\cdot}$
640A	1	3	0	1	-	4	1	$(4{:}\frac{1}{4})$
640B	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
640H	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
644B	1	5	0	5	$(4{:}\frac{1}{4})^{\cdot}$	0	1	-
645E	1	2	3	1	$(1{:}1)$ $(2{:}\frac{1}{2})$	2	1	$(2{:}2)$
651D	1	11	0	11	$(10{:}\frac{1}{10})^{\cdot}$	0	1	-
651E	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
656A	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
657C	1	2	2	1	$(2{:}\frac{1}{2})$	0	2	$(1{:}1)^{\cdot}$
?657C	1	11	0	1	-	2	1	$(2{:}\frac{1}{2})$
658E	1	3	2	1	$(2{:}\frac{1}{2})$	0	1	-

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^+_{\text{Ш}}$	λ^+_{MW}	roots	$\lambda^-_{\text{Ш}}$	λ^-_{MW}	roots
665B	1	3	8	3	$(2{:}\frac{1}{2})^{\cdot}\ (8{:}\frac{1}{8})$	0	1	-
670C	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
674B	1	3	2	3	$(2{:}\frac{1}{2})^{\cdot}\ (2{:}\frac{1}{2})$	0	1	-
675A	1	2	1	1	$(1{:}1)$	6	1	$(6{:}\frac{1}{6})$
675A	1	11	2	1	$(2{:}\frac{1}{2})$	0	1	-
675C	0	2	0	0	-	4	1	$(1{:}1)^{\cdot}\ (4{:}\frac{1}{4})$
675E	0	2	0	0	-	0	5	$(1{:}1)^{\cdot}\ (4{:}\frac{1}{4})^{\cdot}$
676A	0	3	2	0	$(2{:}\frac{1}{2})$	2	0	$(2{:}\frac{1}{2})$
677A	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
680A	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
?680A	1	11	0	1	-	2	1	$(2{:}\frac{1}{2})$
681A	1	2	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	2	$(1{:}1)^{\cdot}$
?681A	1	5	0	1	-	2	1	$(2{:}1)$
681D	0	2	3	0	$(1{:}1)\ (2{:}\frac{1}{2})$	2	0	$(2{:}2)$
681E	1	2	2	1	$(2{:}2)$	0	2	$(1{:}1)^{\cdot}$
682A	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
685A	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
688A	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
688C	1	7	6	1	$(6{:}\frac{1}{6})$	0	1	-
690E	1	7	0	1	-	4	1	$(4{:}\frac{1}{4})$
690G	0	7	2	0	$(2{:}\frac{1}{2})$	0	0	-
693B	1	2	1	1	$(1{:}1)$	2	1	$(2{:}\frac{1}{2})$
693C	0	2	2	0	$(2{:}\frac{1}{2})$	2	1	$(1{:}1)^{\cdot}\ (2{:}1)$
703A	0	2	1	0	$(1{:}1)$	5	1	$(1{:}1)^{\cdot}\ (1{:}1)$ $(4{:}\frac{1}{4})$
703B	1	3	0	1	-	2	1	$(2{:}\frac{3}{2})$
705A	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
705C	0	2	1	0	$(1{:}1)$	2	0	$(2{:}\frac{3}{2})$
706B	1	3	0	1	-	2	1	$(2{:}\frac{3}{2})$
706C	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
?711A	1	5	0	1	-	4	1	$(4{:}\frac{1}{2})$
714F	1	11	2	1	$(2{:}\frac{1}{2})$	0	1	-

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^+_{\text{Ш}}$	λ^+_{MW}	roots	$\lambda^-_{\text{Ш}}$	λ^-_{MW}	roots
715A	1	2	1	3	$(1{:}1)\ (2{:}\frac{1}{2})^{\cdot}$	0	1	-
720H	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
722A	1	5	2	1	$(2{:}1)$	0	1	-
722F	1	5	0	1	-	6	1	$(6{:}\frac{1}{6})$
723A	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
723B	1	2	3	1	$(3{:}1)$	0	1	-
726A	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
734A	0	5	2	0	$(2{:}\frac{1}{2})$	2	0	$(2{:}\frac{1}{2})$
735C	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
735D	0	2	1	0	$(1{:}1)$	2	0	$(2{:}\frac{3}{2})$
741C	0	11	0	0	-	0	0	-
741E	1	2	1	1	$(1{:}1)$	3	2	$(2{:}\frac{3}{2})\ (1{:}1)^{\cdot}$ $(1{:}1)$
742A	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
752A	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
752A	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
753B	0	2	1	0	$(1{:}1)$	3	1	$(1{:}1)^{\cdot}\ (1{:}1)$ $(2{:}\frac{1}{2})$
753C	1	2	0	1	-	2	2	$(1{:}1)^{\cdot}\ (2{:}1)$
754C	1	11	2	1	$(2{:}\frac{1}{2})$	0	1	-
755A	1	2	1	1	$(1{:}1)$	0	1	-
759B	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
760E	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
775A	1	2	6	1	$(6{:}\frac{1}{6})$	0	2	$(1{:}1)^{\cdot}$
776A	1	11	2	1	$(2{:}\frac{1}{2})$	0	1	-
777C	0	2	1	0	$(1{:}1)$	4	0	$(4{:}\frac{3}{4})$
?777D	1	11	0	1	-	2	1	$(2{:}1)$
777G	1	2	0	1	-	2	2	$(2{:}2)\ (1{:}1)^{\cdot}$
781A	0	2	0	0	-	4	1	$(1{:}1)^{\cdot}\ (4{:}\frac{1}{4})$
781B	1	2	1	1	$(1{:}1)$	0	1	-
782A	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
784H	1	3	0	1	-	4	1	$(4{:}\frac{1}{2})$
784H	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^{+}_{\text{Ш}}$	λ^{+}_{MW}	roots	$\lambda^{-}_{\text{Ш}}$	λ^{-}_{MW}	roots
784J	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
791C	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
792A	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-
793A	1	3	6	3	$(2{:}\frac{1}{2})^{\cdot}$ $(6{:}\frac{1}{6})$	0	1	-
?794A	1	11	1	1	$(1{:}2)$	1	1	$(1{:}1)$
795B	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
795C	0	2	0	0	-	2	1	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
800H	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
801A	0	2	1	0	$(1{:}1)$	4	0	$(2{:}1)$ $(2{:}\frac{1}{2})$
801C	1	2	0	1	-	2	2	$(1{:}1)^{\cdot}$ $(2{:}\frac{1}{2})$
807A	0	2	1	0	$(1{:}1)$	3	1	$(1{:}1)^{\cdot}$ $(1{:}1)$ $(2{:}\frac{1}{2})$
811A	1	2	1	1	$(1{:}1)$	0	1	-
811A	1	3	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
811A	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
813B	1	2	1	1	$(1{:}1)$	0	1	-
813B	1	11	0	11	$(10{:}\frac{1}{10})^{\cdot}$	0	1	-
814B	1	3	6	3	$(2{:}\frac{1}{2})^{\cdot}$ $(4{:}\frac{1}{4})$ $(2{:}\frac{1}{2})$	0	1	-
815A	1	2	8	1	$(2{:}1)$ $(6{:}\frac{1}{6})$	0	2	$(1{:}1)^{\cdot}$
816H	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
?817A	1	2	2	1	$(1{:}5)$ $(1{:}1)$	1	1	$(1{:}7)$
817B	1	2	2	1	$(2{:}1)$	0	2	$(1{:}1)^{\cdot}$
819E	0	2	18	0	$(18{:}\frac{1}{18})$	2	1	$(1{:}1)^{\cdot}$ $(2{:}1)$
825A	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
825C	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
827A	1	2	1	3	$(1{:}1)$ $(2{:}\frac{1}{2})^{\cdot}$	0	1	-
827A	1	5	0	5	$(4{:}\frac{1}{4})^{\cdot}$	2	1	$(2{:}\frac{1}{2})$
827A	1	7	0	1	-	2	1	$(2{:}\frac{1}{2})$
829A	1	2	1	1	$(1{:}1)$	2	5	$(2{:}\frac{1}{2})$ $(4{:}\frac{1}{4})^{\cdot}$
834A	0	7	2	0	$(2{:}\frac{1}{2})$	0	0	-
843A	1	5	0	1	-	4	1	$(4{:}\frac{1}{4})$
846B	1	5	2	1	$(2{:}\frac{1}{2})$	0	1	-

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^{+}_{\text{Ш}}$	λ^{+}_{MW}	roots	$\lambda^{-}_{\text{Ш}}$	λ^{-}_{MW}	roots
847A	0	2	3	0	(3:1)	4	0	(2:2) (2:$\frac{1}{2}$)
847B	1	2	2	1	(2:$\frac{1}{2}$)	2	2	(1:1)$^{\cdot}$ (2:1)
850C	1	7	2	1	(2:$\frac{1}{2}$)	0	1	-
851A	1	5	0	5	(4:$\frac{1}{4}$)$^{\cdot}$	0	1	-
?856A	1	5	0	1	-	2	1	(2:1)
856C	1	7	0	1	-	2	1	(2:$\frac{1}{2}$)
862C	0	3	0	2	(2:$\frac{1}{2}$)$^{\cdot}$	0	6	(6:$\frac{1}{6}$)$^{\cdot}$
866A	1	11	2	1	(2:$\frac{1}{2}$)	0	1	-
867A	1	2	3	1	(1:1) (2:$\frac{1}{2}$)	18	1	(18:$\frac{1}{9}$)
880A	1	3	0	1	-	2	1	(2:$\frac{1}{2}$)
885C	1	2	1	3	(1:1) (2:$\frac{1}{2}$)$^{\cdot}$	0	1	-
885C	1	7	0	1	-	2	1	(2:$\frac{1}{2}$)
886A	1	3	0	1	-	0	7	(6:$\frac{1}{6}$)$^{\cdot}$
886D	1	3	0	1	-	4	1	(4:$\frac{1}{4}$)
886D	1	5	2	1	(2:$\frac{1}{2}$)	0	1	-
886E	1	3	0	1	-	4	1	(4:$\frac{1}{2}$)
888C	1	7	2	1	(2:$\frac{1}{2}$)	0	1	-
890A	1	3	0	3	(2:$\frac{1}{2}$)$^{\cdot}$	0	1	-
891B	0	2	0	0	-	4	1	(1:1)$^{\cdot}$ (4:$\frac{1}{4}$)
891F	0	2	0	0	-	0	5	(1:1)$^{\cdot}$ (4:$\frac{1}{4}$)$^{\cdot}$
892B	1	5	2	5	(2:$\frac{1}{2}$) (4:$\frac{1}{4}$)$^{\cdot}$	0	1	-
894E	1	5	6	1	(6:$\frac{1}{6}$)	0	1	-
896B	1	3	0	3	(2:$\frac{1}{2}$)$^{\cdot}$	2	1	(2:$\frac{1}{2}$)
896B	1	5	0	5	(4:$\frac{1}{4}$)$^{\cdot}$	0	1	-
896D	1	3	4	3	(2:$\frac{1}{2}$)$^{\cdot}$ (4:$\frac{1}{4}$)	0	1	-
896D	1	5	0	1	-	2	1	(2:$\frac{1}{2}$)
897C	1	7	2	1	(2:$\frac{1}{2}$)	0	1	-
?899A	1	11	0	1	-	2	1	(2:$\frac{1}{2}$)
901C	0	2	0	0	-	10	1	(1:1)$^{\cdot}$ (10:$\frac{1}{10}$)
901D	0	3	4	0	(4:$\frac{1}{4}$)	4	0	(4:$\frac{1}{4}$)
903A	1	2	4	1	(4:$\frac{1}{4}$)	2	2	(1:1)$^{\cdot}$ (2:1)
903B	0	2	5	0	(1:1) (4:$\frac{1}{4}$)	4	0	(2:$\frac{3}{2}$) (2:$\frac{1}{2}$)
904A	1	3	0	3	(2:$\frac{1}{2}$)$^{\cdot}$	2	1	(2:$\frac{1}{2}$)

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^{+}_{\text{Ш}}$	λ^{+}_{MW}	roots	$\lambda^{-}_{\text{Ш}}$	λ^{-}_{MW}	roots
904A	1	5	0	1	-	2	1	$(2:\frac{1}{2})$
?905A	1	11	0	1	-	2	1	$(2:\frac{1}{2})$
909A	0	2	2	0	$(2:\frac{1}{2})$	4	1	$(1:1)^{\cdot}$ $(4:\frac{1}{2})$
?909C	1	2	1	1	$(1:1)$	3	2	$(2:2)$ $(1:1)^{\cdot}$ $(1:1)$
910F	1	3	4	1	$(4:\frac{1}{4})$	0	1	-
912G	1	7	0	1	-	4	1	$(4:\frac{1}{4})$
914A	1	3	0	1	-	2	1	$(2:\frac{1}{2})$
914A	1	7	0	1	-	2	1	$(2:\frac{1}{2})$
916A	0	3	0	2	$(2:\frac{1}{2})^{\cdot}$	2	0	$(2:\frac{1}{2})$
918A	1	11	2	1	$(2:\frac{1}{2})$	0	1	-
921B	1	2	0	1	-	0	2	$(1:1)^{\cdot}$
921B	1	5	0	1	-	2	1	$(2:\frac{1}{2})$
923A	0	2	0	0	-	8	1	$(1:1)^{\cdot}$ $(8:\frac{1}{8})$
925A	1	2	1	1	$(1:1)$	2	1	$(2:\frac{1}{2})$
925B	1	2	1	1	$(1:1)$	5	2	$(1:1)^{\cdot}$ $(1:1)$ $(4:\frac{1}{2})$
928A	1	7	0	1	-	2	1	$(2:\frac{1}{2})$
931B	0	2	0	0	-	2	1	$(1:1)^{\cdot}$ $(2:\frac{1}{2})$
933A	1	2	9	3	$(1:1)$ $(2:\frac{1}{2})^{\cdot}$ $(8:\frac{1}{8})$	3	2	$(1:1)^{\cdot}$ $(3:1)$
933B	1	2	11	1	$(1:1)$ $(10:\frac{1}{10})$	4	1	$(4:\frac{1}{2})$
935A	1	2	0	1	-	0	2	$(1:1)^{\cdot}$
935B	0	2	1	0	$(1:1)$	2	0	$(2:\frac{3}{2})$
939A	1	2	1	1	$(1:1)$	0	1	-
?942C	1	11	0	1	-	2	1	$(2:\frac{1}{2})$
954D	1	5	0	1	-	2	1	$(2:\frac{1}{2})$
954E	1	5	0	1	-	2	1	$(2:\frac{1}{2})$
960B	1	7	2	1	$(2:\frac{1}{2})$	0	1	-
966E	1	5	0	1	-	2	1	$(2:\frac{1}{2})$
968B	0	3	2	0	$(2:\frac{1}{2})$	2	0	$(2:\frac{1}{2})$
968D	1	3	0	3	$(2:\frac{1}{2})^{\cdot}$	0	1	-

Conductor less than 1000 (continued)

Curve	r	p	$\lambda^+_{\text{Ш}}$	λ^+_{MW}	roots	$\lambda^-_{\text{Ш}}$	λ^-_{MW}	roots
972C	1	5	0	1	-	2	1	$(2{:}\frac{1}{2})$
972D	1	5	0	5	$(4{:}\frac{1}{4})^{\cdot}$	0	1	-
973B	1	2	1	1	(1:1)	0	1	-
973B	1	5	2	1	(2:1)	0	1	-
975F	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
975J	1	2	0	1	-	0	2	$(1{:}1)^{\cdot}$
976C	1	3	0	1	-	2	1	$(2{:}\frac{1}{2})$
979A	0	2	0	0	-	8	1	$(1{:}1)^{\cdot}$ $(8{:}\frac{1}{8})$
985A	0	3	0	2	$(2{:}\frac{1}{2})^{\cdot}$	2	0	$(2{:}\frac{1}{2})$
986F	1	3	0	1	-	2	7	(2:1) $(6{:}\frac{1}{6})^{\cdot}$
990E	1	7	2	1	$(2{:}\frac{1}{2})$	0	1	-
994A	1	5	2	1	$(2{:}\frac{1}{2})$	2	1	$(2{:}\frac{1}{2})$
995B	1	2	1	1	(1:1)	0	1	-
?997B	1	2	1	1	(1:6)	3	2	(3:2) $(1{:}1)^{\cdot}$

9.2 Twists of $14A$ with $p = 5$

D	r	$\lambda^+_{Ш}$	λ^+_{MW}	roots	$\lambda^-_{Ш}$	λ^-_{MW}	roots
17	1	0	5	$(4{:}\frac{1}{4})^{\cdot}$	0	1	-
37	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
41	1	0	1	-	4	1	$(4{:}\frac{1}{4})$
53	1	4	1	$(4{:}\frac{1}{4})$	0	1	-
89	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
129	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
-11	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
?-23	2	4	2	$(2{:}\infty)^{\cdot}\ (4{:}\frac{1}{2})$	2	2	$(2{:}\infty)^{\cdot}\ (2{:}\frac{3}{2})$
-43	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
-51	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
-103	1	2	1	$(2{:}\frac{1}{2})$	2	1	$(2{:}\frac{1}{2})$
-159	1	0	1	-	2	1	$(2{:}\frac{1}{2})$

9.3 Twists of $17A$ with $p = 3$

D	r	$\lambda^+_{Ш}$	λ^+_{MW}	roots	$\lambda^-_{Ш}$	λ^-_{MW}	roots
29	1	6	1	$(6{:}\frac{1}{6})$	0	1	-
37	1	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
40	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
41	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
44	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
56	1	4	1	$(4{:}\frac{1}{4})$	0	1	-
65	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
76	2	0	2	$(2{:}\infty)^{\cdot}$	0	2	$(2{:}\infty)^{\cdot}$
104	2	2	2	$(2{:}\infty)^{\cdot}$ $(2{:}\frac{1}{2})$	2	2	$(2{:}\infty)^{\cdot}$ $(2{:}1)$
109	1	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
113	1	4	1	$(4{:}\frac{1}{4})$	0	1	-
124	1	6	1	$(6{:}\frac{1}{6})$	0	1	-
133	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
145	2	0	2	$(2{:}\infty)^{\cdot}$	4	2	$(2{:}\infty)^{\cdot}$ $(4{:}\frac{1}{4})$
157	2	6	2	$(2{:}\infty)^{\cdot}$ $(6{:}\frac{1}{6})$	0	2	$(2{:}\infty)^{\cdot}$
?173	1	0	1	-	6	1	$(2{:}2)$ $(4{:}\frac{1}{4})$
184	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
185	2	2	2	$(2{:}\infty)^{\cdot}$ $(2{:}1)$	0	2	$(2{:}\infty)^{\cdot}$
193	1	6	1	$(6{:}\frac{1}{6})$	6	1	$(6{:}\frac{1}{6})$
197	1	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-

Twists of $17A$ with $p = 3$ (continued)

D	r	λ^{+}_{III}	λ^{+}_{MW}	roots	λ^{-}_{III}	λ^{-}_{MW}	roots
-8	1	0	1	-	2	1	(2:1)
-19	1	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
-47	1	0	1	-	2	1	$(2{:}\frac{3}{2})$
-52	1	0	1	-	4	1	$(4{:}\frac{1}{4})$
-55	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
-56	2	0	2	$(2{:}\infty)^{\cdot}$	0	2	$(2{:}\infty)^{\cdot}$
?-59	1	0	1	-	4	1	(4:1)
-95	2	0	2	$(2{:}\infty)^{\cdot}$	0	2	$(2{:}\infty)^{\cdot}$
-104	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
-115	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
-139	0	2	0	(2:1)	2	0	(2:1)
-151	1	2	1	$(2{:}\frac{3}{2})$	4	1	$(4{:}\frac{1}{2})$
-152	1	0	3	$(2{:}\frac{1}{2})^{\cdot}$	0	1	-
-155	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
-164	2	0	4	$(2{:}\infty)^{\cdot}$ $(2{:}\frac{1}{2})^{\cdot}$	0	2	$(2{:}\infty)^{\cdot}$
-167	0	2	2	$(4{:}\frac{1}{2})^{\cdot}$	8	0	$(2{:}\frac{1}{2})$ $(6{:}\frac{1}{6})$
-179	1	4	3	$(2{:}\frac{1}{2})^{\cdot}$ $(4{:}\frac{1}{4})$	0	1	-
-184	2	0	2	$(2{:}\infty)^{\cdot}$	2	2	$(2{:}\infty)^{\cdot}$ (2:1)
-199	0	2	0	(2:1)	2	0	(2:1)

9.4 Twists of $19A$ with $p = 2$

D	r	$\lambda^{+}_{Ш}$	λ^{+}_{MW}	roots	$\lambda^{-}_{Ш}$	λ^{-}_{MW}	roots
1	0	0	0	-	2	1	(1:1)$^{\cdot}$ (2:$\frac{1}{2}$)
5	0	0	0	-	2	1	(1:1)$^{\cdot}$ (2:$\frac{1}{2}$)
13	1	1	1	(1:1)	4	1	(4:$\frac{3}{4}$)
17	0	0	0	-	2	1	(1:1)$^{\cdot}$ (2:$\frac{1}{2}$)
21	1	1	1	(1:1)	4	1	(4:$\frac{1}{4}$)
29	1	1	1	(1:1)	4	1	(4:$\frac{1}{4}$)
33	1	1	1	(1:1)	4	1	(4:$\frac{1}{4}$)
37	1	1	1	(1:1)	4	1	(4:$\frac{1}{4}$)
41	1	1	3	(1:1) (2:$\frac{1}{2}$)$^{\cdot}$	6	1	(6:$\frac{1}{6}$)
53	1	1	1	(1:1)	4	1	(4:$\frac{1}{4}$)
61	0	0	0	-	2	1	(1:1)$^{\cdot}$ (2:$\frac{1}{2}$)
?65	1	1	1	(1:1)	3	2	(2:$\frac{5}{2}$) (1:1)$^{\cdot}$ (1:1)
?69	1	3	3	(1:1) (2:$\frac{1}{2}$)$^{\cdot}$ (2:$\frac{1}{2}$)	7	2	(2:2) (2:1)$^{\cdot}$ (4:$\frac{1}{4}$)
73	0	0	0	-	2	1	(1:1)$^{\cdot}$ (2:$\frac{1}{2}$)
77	0	0	0	-	2	1	(1:1)$^{\cdot}$ (2:$\frac{1}{2}$)
85	0	0	0	-	2	1	(1:1)$^{\cdot}$ (2:$\frac{1}{2}$)
89	1	3	1	(3:1)	6	1	(6:$\frac{1}{6}$)
93	0	18	0	(4:$\frac{1}{4}$) (14:$\frac{1}{14}$)	20	1	(1:1)$^{\cdot}$ (2:1) (18:$\frac{1}{18}$)
?97	1	15	1	(2:$\frac{3}{2}$) (1:1) (12:$\frac{1}{12}$)	18	1	(2:2) (16:$\frac{1}{16}$)
101	0	2	0	(2:1)	4	1	(1:1)$^{\cdot}$ (4:$\frac{3}{4}$)
105	1	1	1	(1:1)	4	1	(4:$\frac{1}{4}$)
109	1	1	1	(1:1)	4	1	(4:$\frac{1}{4}$)
113	1	7	1	(1:1) (6:$\frac{1}{2}$)	10	1	(10:$\frac{1}{10}$)
129	1	1	1	(1:1)	4	1	(4:$\frac{1}{4}$)
137	0	0	0	-	2	1	(1:1)$^{\cdot}$ (2:$\frac{1}{2}$)
141	1	1	1	(1:1)	4	1	(4:$\frac{1}{4}$)
145	1	1	1	(1:1)	4	1	(4:$\frac{1}{4}$)
149	0	0	0	-	2	1	(1:1)$^{\cdot}$ (2:$\frac{1}{2}$)

Twists of $19A$ with $p = 2$ (continued)

D	r	$\lambda^+_{\text{Ш}}$	λ^+_{MW}	roots	$\lambda^-_{\text{Ш}}$	λ^-_{MW}	roots
?157	2	0	2	$(2{:}\infty)^{\cdot}$	2	3	$(2{:}\infty)^{\cdot}$ $(2{:}\frac{5}{2})$ $(1{:}1)^{\cdot}$
161	0	4	0	$(4{:}1)$	6	1	$(2{:}\frac{3}{2})$ $(1{:}1)^{\cdot}$ $(4{:}\frac{1}{2})$
165	1	1	1	$(1{:}1)$	4	1	$(4{:}\frac{1}{4})$
?173	1	1	1	$(1{:}1)$	3	2	$(2{:}\frac{5}{2})$ $(1{:}1)^{\cdot}$ $(1{:}1)$
177	0	4	0	$(4{:}\frac{1}{2})$	6	1	$(1{:}1)^{\cdot}$ $(2{:}1)$ $(4{:}\frac{1}{4})$
181	1	1	1	$(1{:}1)$	3	2	$(1{:}1)^{\cdot}$ $(1{:}1)$ $(2{:}\frac{1}{2})$
185	1	1	1	$(1{:}1)$	4	1	$(4{:}\frac{1}{4})$
?193	1	31	1	$(1{:}2)$ $(4{:}1)$ $(26{:}\frac{1}{26})$	34	1	$(34{:}\frac{1}{34})$
197	0	2	0	$(2{:}1)$	4	1	$(1{:}1)^{\cdot}$ $(2{:}1)$ $(2{:}\frac{1}{2})$

9.5 Twists of $27A$ with $p = 2$

D	r	$\lambda^{+}_{\text{Ш}}$	λ^{+}_{MW}	roots	$\lambda^{-}_{\text{Ш}}$	λ^{-}_{MW}	roots
1	0	0	0	-	0	5	$(1{:}1)^{\cdot}\ (4{:}\frac{1}{4})^{\cdot}$
5	1	1	1	$(1{:}1)$	6	1	$(6{:}\frac{1}{6})$
13	0	0	0	-	4	1	$(1{:}1)^{\cdot}\ (4{:}\frac{1}{4})$
17	1	7	1	$(1{:}1)\ (6{:}\frac{1}{6})$	12	1	$(12{:}\frac{1}{12})$
29	1	1	1	$(1{:}1)$	5	2	$(1{:}1)^{\cdot}\ (1{:}1)\ (4{:}\frac{1}{4})$
37	0	0	0	-	4	1	$(1{:}1)^{\cdot}\ (4{:}\frac{1}{4})$
41	1	3	1	$(2{:}\frac{3}{2})\ (1{:}1)$	7	2	$(1{:}1)^{\cdot}\ (1{:}1)\ (6{:}\frac{1}{6})$
53	1	1	1	$(1{:}1)$	1	6	$(1{:}1)^{\cdot}\ (1{:}1)\ (4{:}\frac{1}{4})^{\cdot}$
61	0	0	0	-	4	1	$(1{:}1)^{\cdot}\ (4{:}\frac{1}{4})$
65	1	1	1	$(1{:}1)$	6	1	$(6{:}\frac{1}{6})$
73	0	0	0	-	4	1	$(1{:}1)^{\cdot}\ (4{:}\frac{1}{4})$
77	1	1	1	$(1{:}1)$	6	1	$(6{:}\frac{1}{6})$
85	2	8	2	$(2{:}\infty)^{\cdot}\ (2{:}1)\ (6{:}\frac{1}{6})$	12	3	$(2{:}\infty)^{\cdot}\ (1{:}1)^{\cdot}\ (12{:}\frac{1}{12})$
89	1	3	1	$(1{:}1)\ (2{:}\frac{1}{2})$	8	1	$(8{:}\frac{1}{8})$
97	0	0	0	-	4	1	$(1{:}1)^{\cdot}\ (4{:}\frac{1}{4})$
101	1	1	1	$(1{:}1)$	5	2	$(1{:}1)^{\cdot}\ (1{:}1)\ (4{:}\frac{1}{2})$
109	2	0	2	$(2{:}\infty)^{\cdot}$	4	3	$(2{:}\infty)^{\cdot}\ (1{:}1)^{\cdot}\ (4{:}\frac{3}{4})$
113	1	7	1	$(1{:}1)\ (6{:}\frac{1}{6})$	12	1	$(12{:}\frac{1}{12})$
133	0	0	0	-	4	1	$(1{:}1)^{\cdot}\ (4{:}\frac{1}{4})$
137	1	3	1	$(1{:}1)\ (2{:}\frac{1}{2})$	8	1	$(8{:}\frac{1}{8})$
145	0	4	0	$(4{:}\frac{1}{2})$	8	1	$(1{:}1)^{\cdot}\ (2{:}1)\ (6{:}\frac{1}{6})$
149	1	1	1	$(1{:}1)$	6	1	$(2{:}\frac{3}{2})\ (4{:}\frac{1}{4})$
157	0	2	0	$(2{:}1)$	6	1	$(1{:}1)^{\cdot}\ (6{:}\frac{1}{2})$

Twists of $27A$ with $p = 2$ (continued)

D	r	$\lambda^+_{Ш}$	λ^+_{MW}	roots	$\lambda^-_{Ш}$	λ^-_{MW}	roots
161	1	3	1	(1:1) (2:$\frac{1}{2}$)	8	1	(8:$\frac{1}{8}$)
?173	1	1	1	(1:1)	5	2	$(1{:}1)^{\cdot}$ (1:1) (4:$\frac{3}{4}$)
181	0	0	0	-	4	1	$(1{:}1)^{\cdot}$ (4:$\frac{1}{4}$)
185	1	1	1	(1:1)	6	1	(6:$\frac{1}{6}$)
193	0	0	0	-	4	1	$(1{:}1)^{\cdot}$ (4:$\frac{1}{4}$)
197	1	1	1	(1:1)	6	1	(6:$\frac{1}{6}$)

9.6 Twists of $27A$ with $p = 5$

D	r	$\lambda^{+}_{Ш}$	λ^{+}_{MW}	roots	$\lambda^{-}_{Ш}$	λ^{-}_{MW}	roots
53	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
77	1	2	1	(2:1)	0	1	-
89	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
101	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
?104	1	0	1	-	2	1	(2:1)
109	2	0	2	$(2{:}\infty)^{\cdot}$	2	2	$(2{:}\infty)^{\cdot}$ $(2{:}\frac{1}{2})$
113	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
?149	1	0	1	-	2	1	$(2{:}\frac{3}{2})$
152	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
172	2	0	2	$(2{:}\infty)^{\cdot}$	0	2	$(2{:}\infty)^{\cdot}$
197	1	0	1	-	4	1	$(4{:}\frac{1}{4})$
-11	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
-31	2	0	2	$(2{:}\infty)^{\cdot}$	0	2	$(2{:}\infty)^{\cdot}$
-68	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
-104	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
-107	1	2	1	$(2{:}\frac{1}{2})$	0	1	-

9.7 Twists of $32A$ with $p = 3$

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

9.8 Twists of $40A$ with $p = 3$

D	r	$\lambda^{+}_{\text{Ш}}$	λ^{+}_{MW}	roots	$\lambda^{-}_{\text{Ш}}$	λ^{-}_{MW}	roots
17	1	0	1	-	6	1	$(2{:}\frac{1}{2})$ $(4{:}\frac{1}{4})$
61	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
73	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
97	1	0	1	-	2	1	$(2{:}1)$
101	1	4	1	$(4{:}\frac{1}{2})$	2	1	$(2{:}1)$
109	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
113	1	4	1	$(4{:}\frac{1}{4})$	0	1	-
133	2	0	2	$(2{:}\infty)^{\cdot}$	0	2	$(2{:}\infty)^{\cdot}$
137	1	4	1	$(4{:}\frac{1}{2})$	0	1	-
149	1	4	1	$(4{:}\frac{1}{2})$	0	1	-
157	0	2	0	$(2{:}1)$	2	0	$(2{:}1)$
181	1	4	1	$(2{:}\frac{1}{2})^{\cdot}$ $(2{:}\frac{1}{2})$	0	1	-
193	1	2	1	$(2{:}\frac{3}{2})$	0	1	-
?-43	1	0	1	-	2	1	$(2{:}2)$
-79	1	4	1	$(4{:}\frac{1}{4})$	0	1	-
-83	1	6	1	$(6{:}\frac{1}{3})$	0	1	-
-91	2	0	2	$(2{:}\infty)^{\cdot}$	0	2	$(2{:}\infty)^{\cdot}$
-107	1	6	1	$(6{:}\frac{1}{6})$	0	1	-
-119	1	6	1	$(2{:}\frac{1}{2})^{\cdot}$ $(4{:}\frac{1}{2})$	0	1	-
-127	0	2	0	$(2{:}1)$	4	0	$(4{:}\frac{1}{2})$
-151	1	2	1	$(2{:}\frac{1}{2})$	0	1	-
-163	1	4	1	$(2{:}\frac{1}{2})^{\cdot}$ $(2{:}\frac{1}{2})$	6	1	$(6{:}\frac{1}{3})$
-187	1	0	1	-	2	1	$(2{:}\frac{1}{2})$
-191	1	4	1	$(4{:}\frac{1}{2})$	0	1	-

References

[1] Y. Amice and J. Vélu, Distributions p-adiques associées aux séries de Hecke. (French), in *Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974)*, 119–131. Astérisque, Nos. 24-25, Soc. Math. France, Paris, 1975.

[2] J. E. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge Univ. Press, Cambridge, 1997.

[3] F. Q. Gouvêa, *p-adic numbers*, Second edition, Springer, Berlin, 1997.

[4] R. Greenberg, Iwasawa theory for elliptic curves, in *Arithmetic theory of elliptic curves (Cetraro, 1997)*, 51–144, Lecture Notes in Math., 1716, Springer, Berlin, 1999.

[5] Ralph Greenberg, Iwasawa Theory - Past and Present, On web page: `www.math.washington.edu/~greenber/research.html`.

[6] R. Greenberg and G. Stevens, On the conjecture of Mazur, Tate and Teitelbaum, in *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, 183–211, Contemp. Math., 165, Amer. Math. Soc., Providence, RI, 1994.

[7] K. Iwasawa, On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc. **65** (1959), 183–226.

[8] K. Kato, Euler systems, Iwasawa theory and Selmer groups, to appear.

[9] M. Kurihara, On the Tate-Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, preprint.

[10] M. Lazard, Les zéros des fonctions analytiques d'une variable sur un corps valué complet. (French) Inst. Hautes Études Sci. Publ. Math. No. **14** (1962), 47–75.

[11] Ju. I. Manin, Parabolic points and zeta functions of modular curves Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[12] Ju. I. Manin, Cyclotomic Fields and Modular Curves, Uspehi Mat. Nauk **26** (1971), no. 6(162), 7–71.

[13] Ju. I. Manin, Periods of cusp forms, and p-adic Hecke series, Mat. Sb. (N.S.) **92(134)** (1973), 378–401, 503.

[14] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Invent. Math. **18** (1972), 183–266.

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

[16] B. Mazur, J. Tate and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math. **84** (1986), no. 1, 1–48.

[17] B. Perrin-Riou, Théorie d'Iwasawa p-adique locale et globale. (French) [Local and global p-adic Iwasawa theory], Invent. Math. **99** (1990), no. 2, 247–292.

[18] D. E. Rohrlich, On L-functions of elliptic curves and cyclotomic towers, Invent. Math. **75** (1984), no. 3, 409–423.

[19] K. Rubin, Euler systems and modular elliptic curves, in *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, 351–367, Cambridge Univ. Press, Cambridge, 1998.

[20] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), no. 4, 259–331.

[21] J. H. Silverman, *The arithmetic of elliptic curves*, Corrected reprint of the 1986 original, Springer, New York, 1992.

[22] M. M. Višik, Nonarchimedean measures associated with Dirichlet series. (Russian) Mat. Sb. (N.S.) **99(141)** (1976), no. 2, 248–260.

[23] M. M. Višik and Ju. I. Manin, p-adic Hecke series of imaginary quadratic fields, Mat. Sb. (N.S.) **95(137)** (1974), 357–383, 471.

[24] L. C. Washington, *Introduction to cyclotomic fields*, Second edition, Springer, New York, 1997.