ON COMPUTING THE NEWTON POLYGONS OF PLUS AND MINUS p-ADIC L-FUNCTIONS

SAI SANJEEV BALAKRISHNAN, ANTONIO LEI, AND BHARATHWAJ PALVANNAN

Abstract. Let $p \geq 3$ be a prime number and $E/\mathbb{Q}$ an elliptic curved with good supersingular reduction at p and $a_p(E) = 0$. In this article, we study the computation of the Newton polygons of Pollack's plus and minus p-adic L-functions attached to E. In particular, we furnish new examples where the assumption GCD in [Forum Math. Sigma, 7:Paper No. e25] holds. We also take this opportunity to rectify two imprecisions in the aforementioned article.

§0. Remarks on [LP19]

From the outset, we would like to take the opportunity to first highlight two imprecisions in the earlier work of the second and third author [LP19].

(1) In [LP19, Section 7.2], we provided a description of the modules, labelled $\mathcal{Z}$ and $\mathcal{Z}^{(\star)}$ appearing in our main result [LP19, Theorem 1] for various pairs of local conditions. Although the eventual description of these modules for the pair of local conditions corresponding to $\{++, +-\}$ is correct, our description relies on an inaccurate reasoning. We incorrectly assert that the pairing on [LP19, Page 57, Figure 3] is skew-symmetric. We thank Takenori Kataoka for bringing this point to our attention. We also thank Henri Darmon for clarifications on this issue. What we really need for our eventual description of $\mathcal{Z}$ and $\mathcal{Z}^{(\star)}$ is that the plus and minus local conditions are self-annihilators under the local pairing (this would have been automatic had the aforementioned pairing been skew-symmetric). We don't provide more details in this article, since the interested reader may refer to [Kat22] (especially Section 8), where Takenori Kataoka has generalized our main results, even considering the higher rank case as in [BCG$^+$22]. The main point is that one has to prove a Λ-adic version of the self-annihilation result, analogous to the one in the work of Byoung Du Kim [Kim07, Proposition 3.18].

(2) In [LP19, Table 2], several examples of elliptic curves E with good supersingular reduction at $p = 3$ and $a_p(E) = 0$, satisfying the Assumption GCD were given. However, the condition that p splits in the imaginary quadratic field K only holds for the curve 32A and $K = \mathbb{Q}(\sqrt{-107})$. In this article, we rectify this oversight and provide further examples for which Assumption GCD holds, where p does split in K but where p is not necessarily 3.

§1. Introduction

Let E denote an elliptic curve defined over $\mathbb{Q}$ with good supersingular reduction at an odd prime p and such that $a_p(E) = 0$. Let $\widetilde{\Gamma}$ denote the Galois group of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We shall identify the Iwasawa algebra $\mathbb{Z}_p[[\widetilde{\Gamma}]]$ with the ring of power series $\mathbb{Z}_p[[T]]$. Let $\mathcal{H}$ denote the subset of $\mathbb{Q}_p[[T]]$ containing the power series that converge on the p-adic open unit disk. We recall

2020 *Mathematics Subject Classification.* Primary 11R23; Secondary 11G05, 11G07, 11R34, 11S25.
Key words and phrases. Iwasawa theory for elliptic curves at supersingular primes.

from [Pol03, Theorem 5.6] that there exist $\theta_E^+, \theta_E^- \in \mathbb{Z}_p[[T]]$ such that

$$L_\lambda = \log_p^+ \theta_E^+ + \lambda \log_p^- \theta_E^-.$$

Here, λ is a root of the polynomial $x^2 + p$, the plus and minus logarithms $\log_p^\pm \in \mathcal{H}$ are defined in Pollack's work [Pol03, Lemma 4.1] and $L_\lambda \in \mathcal{H}$ is the classical p-adic L-function for the elliptic curve E constructed in works of Amice–Vélu and Višik [AV75, Viš76]. Let $K = \mathbb{Q}(\sqrt{-m})$ denote an imaginary quadratic field. Let E_K denote the quadratic twist of E by K.

The purpose of this article is to give new examples of elliptic curves satisfying the following three conditions:

(I) θ_E^+ is a unit in $\mathbb{Z}_p[[T]]$;
(II) $\theta_{E_K}^+$ and $\theta_{E_K}^-$ have no common irreducible factor in $\mathbb{Z}_p[[T]]$;
(III) $\theta_{E_K}^+$ and $\theta_{E_K}^-$ are not units in $\mathbb{Z}_p[[T]]$.

The direct computation of the modular symbols for the twists E_K becomes time-consuming as the discriminant of K increases. We discuss in Section 2 on how the modular symbols for the quadratic twist E_K can be expressed in terms of the modular symbols for E and the quadratic character associated to K; such a twisting formula speeds up the process for computing the modular symbols for E_K.

To verify the conditions (I), (II) and (III), we use Pollack's code available on [Pol] as our starting point. To verify (I), our code verifies that the Iwasawa invariants of θ_E^+ vanish. To verify (III), our code checks that for both $\theta_{E_K}^+$ and $\theta_{E_K}^-$, the Iwasawa λ invariants are non-zero. We produce examples where the valuation of the roots of $\theta_{E_K}^+$ and $\theta_{E_K}^-$ are different, thereby verifying (II) in our examples. In order to compute the p-adic valuations of the roots, we study the Newton polygons of $\theta_{E_K}^\pm$. The details are discussed in Sections 3 and 4. In particular, we prove a theoretical result (Proposition 2) showing that the Newton polygons of $\theta_{E_K}^\pm$ can be computed via their approximations. This may be of independent interest.

In [LP19], we were interested in annihilators of the dual of a *fine Selmer group*. For this purpose, we needed to relate algebraic p-adic L-functions with analytic p-adic L-functions, by appealing to the work of Pollack–Rubin [PR04] when the elliptic curve E has CM and the work of [Kob03] when the elliptic curve E does not have CM. To apply Kobayashi's result, we need to computationally verify that the p-adic Galois representation associated to E is surjective. The details of our calculations to show this surjectivity are discussed in Section 5.

The code used in our computations is available on Github [Bal]. The examples we have found are tabulated in Section 6.

Acknowledgement

We are grateful to Rob Pollack for answering many of our questions related to his code [Pol]. The first named author was supported by the Globalink Research Internship Program of MITACS hosted at Université Laval in the summer of 2022. The second named author's research is supported by the NSERC Discovery Grants Program RGPIN-2020-04259 and RGPAS-2020-00096. The third named author's research is partially supported by the SERB-MATRICS grant MTR/2022/000244.

§2. Computation of modular symbols for quadratic twists

The material presented in this section is already covered in [SW13, §3.7]. For the convenience of the reader, we reproduce the short computation.

Let $[r]^+$ (resp. $[r]^-$) denote the value of the normalized + (resp. −) modular symbol corresponding to the elliptic curve E, for $r \in \mathbb{Q}$, as discussed in [Pol03, Section 5.2][1] Let f denote the normalized eigen-newform corresponding to E. We have

$$[r]^+ = \frac{1}{2\Omega_E^+}\left[2\pi i\int_{i\infty}^{r} f(z)dz + 2\pi i\int_{i\infty}^{-r} f(z)dz\right], \tag{2.1}$$

$$[r]^- = \frac{1}{2\Omega_E^-}\left[2\pi i\int_{i\infty}^{r} f(z)dz - 2\pi i\int_{i\infty}^{-r} f(z)dz\right]. \tag{2.2}$$

Let $K = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field. We first concentrate on the case $m \equiv 3 \pmod 4$. The associated Dirichlet character in this case is given by $\chi(n) = \left(\frac{-m}{n}\right)$ for n coprime to m (and 0 otherwise). Hence, the conductor of the quadratic character is m in this case.

Let f_K denote the normalized eigen-newform corresponding to E_K.Then, by [MTT86, Eqn 8.5], we have

$$2\pi i\int_{i\infty}^{r} f_K(z)dz = \frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(a)2\pi i\int_{i\infty}^{r+\frac{a}{m}} f(z)dz, \tag{2.3}$$

where $\tau(\chi)$ is the Gauss sum of χ. On replacing r by $-r$ in (2.3), adding the new equation to the original one, and repeatedly applying (2.1) and (2.2), we obtain

$$\begin{aligned}
2\Omega_{E_K}^+[r]_K^+ &= \frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(a)\left(2\pi i\int_{i\infty}^{r+\frac{a}{m}} f(z)dz + 2\pi i\int_{i\infty}^{-r+\frac{a}{m}} f(z)dz\right)\\
&= \frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(a)\left(\Omega_E^+\left[r+\frac{a}{m}\right]^+ + \Omega_E^-\left[r+\frac{a}{m}\right]^- + \Omega_E^+\left[-r+\frac{a}{m}\right]^+ + \Omega_E^-\left[-r+\frac{a}{m}\right]^-\right)\\
&= \frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(a)\left(\Omega_E^+\left[r+\frac{a}{m}\right]^+ + \Omega_E^-\left[r+\frac{a}{m}\right]^-\right)\\
&\qquad + \frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(a)\left(\Omega_E^+\left[-r+\frac{a}{m}\right]^+ + \Omega_E^-\left[-r+\frac{a}{m}\right]^-\right)\\
&= \frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(a)\left(\Omega_E^+\left[r+\frac{a}{m}\right]^+ + \Omega_E^-\left[r+\frac{a}{m}\right]^-\right)\\
&\qquad + \frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(m-a)\left(\Omega_E^+\left[-r+1-\frac{a}{m}\right]^+ + \Omega_E^-\left[-r+1-\frac{a}{m}\right]^-\right)\\
&= \frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(a)\left(\Omega_E^+\left[r+\frac{a}{m}\right]^+ + \Omega_E^-\left[r+\frac{a}{m}\right]^-\right)\\
&\qquad + \frac{1}{\tau(\chi)}\sum_{a \bmod m}\chi(-a)\left(\Omega_E^+\left[-r-\frac{a}{m}\right]^+ + \Omega_E^-\left[-r-\frac{a}{m}\right]^-\right)\\
&= \frac{1}{\tau(\chi)}\sum_{a \bmod m}(\chi(a)+\chi(-a))\Omega_E^+\left[r+\frac{a}{m}\right]^+ + \frac{1}{\tau(\chi)}\sum_{a \bmod m}(\chi(a)-\chi(-a))\Omega_E^-\left[r+\frac{a}{m}\right]^-,
\end{aligned}$$

[1]Note that the ± that occurs in the superscript for the modular form is unrelated to that in $L_p^{\pm}$.

where we have made use of the fact that $[r]^+ = [-r]^+, [r]^- = -[-r]^-$ and $[r+1]^\pm = [r]^\pm$ in the last equation. Notice that as we are working with imaginary quadratic fields, $\chi(-1) = -1$ and hence $\chi(a) + \chi(-a) = 0$ and $\chi(a) - \chi(-a) = 2\chi(a)\ \forall a \in \mathbb{Z}/m\mathbb{Z}$. Hence, we deduce that

$$[r]_K^+ = \frac{\Omega_E^-}{\Omega_{E_K}^+ \tau(\chi)} \sum_{a \bmod m} \chi(a) \left[r + \frac{a}{m}\right]^-. \tag{2.4}$$

We need to evaluate the factor before the summation. As given by [MTT86, §11, (3)], there exists $\eta \in \{1, 2\}$ such that $\Omega_{E_K}^+ = \frac{\eta}{\sqrt{D}} \Omega_E^-$, where D is the discriminant of K. When $m \equiv 3 \pmod 4$, we have $D = -m$, $\tau(\chi) = i\sqrt{m}$.

$$[r]_K^+ = \frac{1}{\eta} \sum_{a \bmod m} \chi(a) \left[r + \frac{a}{m}\right]^-. \tag{2.5}$$

In the case when $m \not\equiv 3 \pmod 4$, the analog of the equation 2.4 becomes

$$[r]_K^+ = \frac{\Omega_E^-}{\Omega_{E_K}^+ \tau(\chi)} \sum_{a \bmod 4m} \chi(a) \left[r + \frac{a}{4m}\right]^-. \tag{2.6}$$

and as $\tau(\chi) = 2i\sqrt{m}$ and $D = -4m$, the analog of 2.5 becomes

$$[r]_K^+ = \frac{1}{\eta} \sum_{a \bmod 4m} \chi(a) \left[r + \frac{a}{4m}\right]^-. \tag{2.7}$$

Note that the factor $1/\eta$ does not play a role in our computations since it is a p-adic unit.

§3. The Iwasawa invariants of $\theta_{E_K}^\pm$

In this section, all the terms involved depend on the chosen elliptic curve E and the quadratic field K. For simplicity, we suppress the dependence of E and K in our notation, and we will henceforth denote $\theta_{E_K}^\pm$ by $L_p^\pm$. We recall below the Mazur–Tate element, at level n, defined in [MT87]:

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

where γ is a topological generator of $1 + p\mathbb{Z}_p$. We have the relations $\theta_n = \omega_n^+ L_{p,n+1}^+$ and $\theta_n = \omega_n^- L_{p,n+1}^-$, where

$$\omega_n^+ = \prod_{1 \leqslant 2k \leqslant n} \Phi_{2k}(1+T), \quad \omega_n^- = \prod_{1 \leqslant 2k-1 \leqslant n} \Phi_{2k-1}(1+T), \tag{3.1}$$

and $L_{p,n+1}^\pm$ are approximants of Pollack's plus and minus p-adic L-functions (see [Pol03, §6] for further details). Here, $\Phi_m(T) = \sum_{t=0}^{p-1} T^{p^{m-1}t}$ denotes the p^m-th cyclotomic polynomial. In particular, we have that $L_{p,n}^+(T) \to L_p^+(T)$ and $L_{p,n}^-(T) \to L_p^-(T)$ as $n \to \infty$ under the sup-norm topology. The Iwasawa invariants of $L_p^\pm$ can be realized by the Weierstrass Preparation theorem, which tells us that

$$L_p^+(T) = p^{\mu^+} P_+(T) U_+(T), \quad L_p^-(T) = p^{\mu^-} P_-(T) U_-(T),$$

where $P_\pm(T)$ are distinguished polynomials and $U_\pm(T)$ are units in the power series ring. The exponent $\mu^\pm$ is the μ-invariant of $L_p^\pm$. We denote the λ-invariant of $L_p^\pm$ to be $\lambda^\pm$ (they are equal to $\deg\ P_\pm$). These invariants can be calculated readily using Rob Pollack's code [Pol]. Conditions (I) and (III) can be verified using these invariants, as explained in the introduction.

We turn our attention to condition (II). If $E_K/\mathbb{Q}$ has positive rank, then a positive power of T divides both $L_p^{\pm}$, and thus condition (II) fails to hold. Therefore, we rule out such cases from our consideration.

In order to verify Assumption GCD, we study the roots of $P_{\pm}(T)$. By [Kob84, Corollary on P.106, §IV.4], if λ is a slope of an edge of the newton polygon whose horizontal length is k, then there are k roots of slope $-\lambda$. We compute these Newton polygons via those of $L_{p,n}^{\pm}$ for large enough n. This suffices since the Newton polygons $L_{p,n}^{\pm}$ converge to those of $L_p^{\pm}$ by [SW13, Proposition 3.5] (we thank Rob Pollack for pointing this out to us). In the next section, we study how large n needs to be in order to obtain the Newton polygon of $L_p^{\pm}$ from that of $L_{p,n}^{\pm}$.

§4. Determining the value of n for computing the Newton polygons of $L_p^{\pm}$ via $L_{p,n}^{\pm}$

Recall that the Newton polygon of a p-adic power series $\sum_{i=0}^{\infty} a_i T^i$ is the convex hull of the points $(i, v_p(a_i))$ in the Cartesian xy plane. Here, v_p denotes the p-adic valuation on $\mathbb{Z}_p$. We consider the p-adic L-function $L_p^+(T)$ (the treatment for $L_p^-(T)$ is similar). We retain the notation from the previous section and write

$$L_p^+(T) = \sum_{i=0}^{\infty} a_i T^i.$$

For the rest of this section, we assume:

(1) The μ-invariant of $L_p^+(T)$ is zero (i.e. it is not divisible by p);
(2) The constant term of $L_p^+(T)$ is non-zero.

These two assumptions hold in all the examples presented in §6. The first assumption can be verified using the existing code of Rob Pollack; this is implemented in [Bal]. The justification for why the second assumption holds is given below equation (4.1).

In this section, for ease of notation, we let d denote λ^+ and e denote the p-adic valuation of the constant term of $L_p^+(T)$.

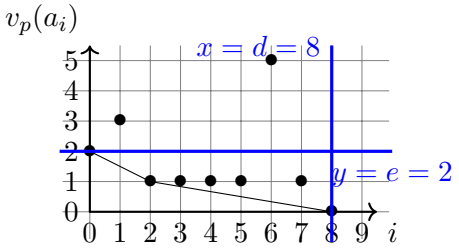

FIGURE 1. $L_{p,3}^+ = 18 + 432T + 9834T^2 + 69420T^3 + 318678T^4 + 1046316T^5 + 255344T^6 + 4781256T^7 + 7048322T^8 + 8336118T^9 + 8009632T^{10} + \ldots$.

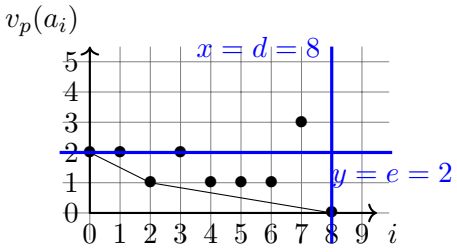

FIGURE 2. $L^+_{p,5} = 18 + 1044T + 28122T^2 + 1575216T^3 + 131578572T^4 + 8486189598T^5 + 398645362398T^6 + 14338769163066T^7 + 414499977694970T^8 + ...$

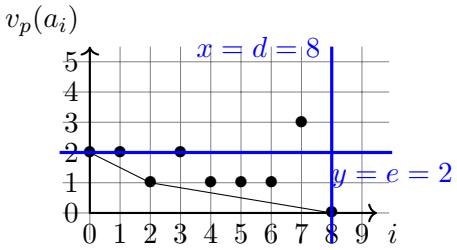

FIGURE 3. $L^+_{p,7} = 18+78336T+60573810T^2+35188130718T^3+15080956806318T^4+4902729944974332T^5 + 1271554307029401828T^6 + 274242979852466887296T^7 + 50692337810680957061662T^8 + 8207148515205569057299710T^9 + ...$

The figures correspond to successive approximations to $L^+_p(T)$ for the case when the elliptic curve E is $32A$, $p = 3$ and $K = \mathbb{Q}(\sqrt{-1907})$. In this example, $e = 2$ and $d = 8$.

In what follows, we show that there exists a positive integer[2] N such that the Newton Polygon of $L^+_p(T)$ coincides with that of $L^+_{p,n}(T)$, for $n \geq N$. We prove this by showing that the the set of points $(i, v_p(a_{n,i}))$ that lie within the rectangle bounded by the axes, along with the lines $x = d$ and $y = e$ eventually stabilize. The convex hull of these points determines the Newton polygon.

By [Pol03, Proposition 6.18], if n is odd, we have $L^+_p(T) \equiv L^+_{p,n+1}(T) \pmod{T\omega^-_n}$. Hence, we deduce that there exists a power series $P_n(T) \in \mathbb{Z}_p[[T]]$ such that

$$L^+_p(T) - L^+_{p,n+1}(T) = T\omega^-_n(T)P_n(T). \tag{4.1}$$

Since T divides the difference $L^+_p(T) - L^+_{p,n+1}(T)$, we see that the constant terms of $L^+_p(T)$ and $L^+_{p,n+1}(T)$ agree. In particular, the starting points of their Newton polygons agree. Therefore, to verify the assumption that the constant term of $L^+_p(T)$ is non-zero, it is enough for us to show that the constant term of $L^+_{p,n+1}(T)$ is non-zero, for some value of n.

Since $\Phi_n(T)$ is a cyclotomic polynomial, note that all non-leading coefficients of $\Phi_n(1 + T)$ are divisible by p. Looking at equation (3.1) tells us that for a similar reason, all non-leading coefficients of $\omega^-_n(T)$ are also divisible by p. Suppose we can find integers n and d_0 satisfying the following three conditions:

(1) the μ-invariant of $L^+_{p,n+1}(T)$ vanishes

[2]for the example where elliptic curve E is $32A$, $p = 3$ and $K = \mathbb{Q}(\sqrt{-1907})$, the quantity N turns out to be 7.

(2) The λ-invariant of $L^+_{p,n+1}(T)$ equals d_0, and
(3) $\deg(\omega_n^-(T)) > d_0$.

Then, (4.1) tells us the μ-invariant of $L^+_p(T)$ vanishes, and that $L^+_{p,n+1}(T)$ and $L^+_p(T)$ have the same λ-invariant. In our code (as in Pollack's code), we search for these integers n and d_0. This information is first only used to determine the λ-invariant and μ-invariant.

We introduce some notations. Let $q^-(n)$ denote the degree of $\omega_n^-(T)$. One finds that when n is odd, $q^-(n) = \frac{p^{n+1}-1}{p+1}$. (When n is even, $q^-(n) = q^-(n-1)$.) Let us write:

$$L^+_{p,n}(T) = \sum_{i=0}^{\infty} a_{n,i} T^i$$

$$\Phi_n(1+T) = \sum_{i=0}^{p^{n-1}(p-1)} b_{n,i} T^i$$

$$\omega_n^-(T) = \sum_{i=0}^{q^-(n)} c^-_{n,i} T^i$$

We show in Lemma 1 that when n is sufficiently large, the p-adic valuation of the coefficients of T^i in $\omega_n^-(T)$ is larger than e for $0 \le i \le d$. This lemma is used in Proposition 2 below. The proposition allows us to compare the vertices of the Newton polygons of $L^+_{p,n+1}(T)$ and $L^+_p(T)$ in the region of $0 \le x \le d$.

Lemma 1. Let d and e be non-negative integers. Let k be an odd integer such that $q^-(k) > d$. Let N equal $k + 2e$. Then, for every $n \ge N$, we have

$$v_p(c^-_{n,i}) > e, \qquad \forall\ 0 \le i \le d. \tag{4.2}$$

Proof. Notice that, for $n > N$, the polynomial $\omega_n^-(T)$ is divisible by $\omega_N^-(T)$ over $\mathbb{Z}_p[T]$. Therefore, for $0 \le i \le d$, we have

$$v_p(c^-_{n,i}) \ge v_p(c^-_{N,i}).$$

See for example [SW13, Lemma 3.4]. It is, therefore, enough to establish equation (4.2) for $n = N$.

We proceed by induction on e.
Suppose first that $e = 0$. In this case, N equals k. As remarked above, p divides $c_{k,i}$ for every $i < q^-(k) = q^-(N)$. Since d is less than $q^-(k)$,

$$v_p(c^-_{N,i}) > 0 = e, \quad \forall\ 0 \le i \le d.$$

Now, using the induction hypothesis, suppose that equation 4.2 holds for some non-negative integer $e-1$. In this case, $N_{e-1} = k + 2(e-1)$. In this case, we have

$$v_p(c^-_{k+2(e-1),i}) > e - 1, \quad \forall 0 \le i \le d.$$

We want to show equation 4.2 holds for $e \ge 1$. In this case, $N = k + 2e$. Note that

$$\omega_N^-(T) = \omega_{N-2}^-(T) \times \Phi_N(1+T). \tag{4.3}$$

As a result, for $0 \le i \le d$, we have:

$$c^-_{N,i} = \sum_{j=0}^{i} c^-_{N-2,j} b_{N,i-j}. \tag{4.4}$$

Since

$$\Phi_N(1+T) = \sum_{t=0}^{p-1} (1+T)^{p^{N-1}t},$$

we have p divides $b_{N,j}$ for $0 \leq j < p^{N-1}(p-1)$. One can deduce the following chain of inequalities

$$d < q^-(k) = \frac{p^{k+1}-1}{p+1} < p^{k+1}(p-1) \leq p^{N-1}(p-1) = \deg(\Phi_N(1+T)).$$

Consequently, for each index j in equation (4.4),

$$v_p\left(c^-_{N-2,j} b_{N,i-j}\right) > e - 1 + 1 = e.$$

Thus, from equation (4.4), we deduce that

$$v_p(c^-_{N,i}) > e - 1 + 1 = e$$

□

Proposition 2. Let N be the constant given in Lemma 1 with $e = v_p(a_0)$ (which is finite as $a_0 \neq 0$ by assumption). Let d be the λ-invariant of $L_p^+(T)$. Then, for all odd integers $n \geq N$, the Newton polygons of $L_p^+(T)$ and $L_{p,n+1}^+(T)$ coincide upto the line $x = d$.

Proof. Since $v_p(a_0) = e$, the Newton polygon of $L_p^+(T)$ upto $x = d$ lies below the line $y = e$. As discussed above, the same is true for $L_{p,n+1}^+(T)$. In particular, if the y-coordinate of $(i, v_p(a_i))$ (resp. $(i, v_p(a_{n+1,i}))$) is larger than e, then it is not a vertex of the Newton polygon of $L_p^+(T)$ (resp. $L_{p,n+1}^+(T)$). Therefore, it is enough to show that for $0 \leq i \leq d$:

- If $(i, v_p(a_i))$ lies on or above the line $y = e$, then so does $(i, v_p(a_{n+1,i}))$;
- If $(i, v_p(a_i))$ lies below the line $y = e$, then it coincides with $(i, v_p(a_{n+1,i}))$.

Using equation (4.1) that for $1 \leq i \leq d$, we have

$$v_p\left(a_i - a_{n+1,i}\right) \geq v_p(c^-_{n,i-1}). \tag{4.5}$$

It then follows from Lemma 1 that

$$v_p\left(a_i - a_{n+1,i}\right) \geq v_p(c^-_{n,i-1}) > e. \tag{4.6}$$

Case 1: $v_p(a_i) \geq e$**.**
By (4.6) and the strong triangle inequality, $v_p(a_i) \geq e$ implies that $v_p(a_{n+1,i}) \geq e$. Thus, neither $(i, v_p(a_i))$ nor $(i, v_p(a_{n+1,i}))$ is a vertex of the corresponding Newton polygon.
Case 2: $v_p(a_i) < e$**.**
Given that $v_p(a_i) < e$, in order for (4.6) to hold, we must have $v_p(a_{n+1,i}) = v_p(a_i) < e$. Hence, the points $(i, v_p(a_i)$ and $(i, v_p(a_{n+1,i}))$ coincide.
This concludes the proof. □

Hence, in order to compute the slopes of the roots of $L_p^+(T)$, it is enough to compute those of $L_{p,N+1}^+$ where N is as prescribed by Lemma 1. In the tables below, we denote by N^+ the integer such that it suffices to compute the newton polygons of $L_{p,N^++1}^+(T)$ to deduce the slopes of the root of $L_p^+(T)$, and similarly N^- the integer such that it suffices to compute the newton polygons of L_{p,N^-+1}^- to deduce the slopes of the root of L_p^-.

§5. Surjectivity of Galois representations

When the elliptic curve E does not have CM, we summarize how we verify surjectivity of Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ for the action of the absolute Galois group of $\mathbb{Q}$ on the p-adic Tate module of E. The verification follows the arguments provided in [LP19]; it is repeated here for the sake of completeness.

We first consider the case $p = 3$. First of all, note that $\det(\rho) : G_{\mathbb{Q}} \to \mathbb{Z}_3^{\times}$ is surjective as it coincides with the 3-adic cyclotomic character. Thus, the surjectivity of ρ follows once we show that the image of ρ contains $\mathrm{SL}_2(\mathbb{Z}_3)$. In order to achieve this, we consider the projection π of the image of ρ to $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, given by the action of the Galois group on the 9-torsion points of E. If this projection is the whole of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, then, by [Ser68, Exercise 1(b), Chapter IV, §3.4], the image of ρ contains $\mathrm{SL}_2(\mathbb{Z}_3)$, and we are done. Thus, we are reduced to showing $\mathrm{Gal}(\mathbb{Q}(E[9])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, from which it follows that the image of π is indeed $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$.

In our examples, we first verify that $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_3)$ on Sage, using Sage's in-built functionality, for all the elliptic curves in the two tables below. Note that the order of $\mathrm{GL}_2(\mathbb{F}_3)$ (in these examples, this group is isomorphic to $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$), is equal to $2^4 * 3$.

Since $\mathbb{Q}(E[3]) \subset \mathbb{Q}(E[9])$, and the cardinality of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ is $2^4 * 3^5$, it now suffices to prove that $3^5 | [\mathbb{Q}(E[9]) : \mathbb{Q}]$, which would imply that $\mathrm{Gal}(\mathbb{Q}(E[9])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, as required. We explain how we check the last divisibility.

Let $f(t)$ denote the 9-division polynomial whose roots are the x-coordinates of the nontrivial points on E which have order 9. Computations on Sage gives an irreducible factor $f_{36}(t)$ of $f(t)$ of degree 36. We choose a root α of $f_{36}(t)$ and construct $\mathbb{Q}(\alpha)$. We then factorize $f_{36}(t)$ over $\mathbb{Q}(\alpha)[T]$ to obtain an irreducible polynomial $g_{27}(t)$ of $f_{36}(t)$. Let β be a root of $g_{27}(t)$, and construct $\mathbb{Q}(\alpha, \beta) \subset \mathbb{Q}(E[9])$. We verify that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 36 * 27 = 3^5 * 4$, and thus $3^5 | [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$. Hence, we deduce that $3^5 | [\mathbb{Q}(E[9]) : \mathbb{Q}]$.

When the prime p under consideration is larger than 3, the image of ρ is closed in $\mathrm{SL}_2(\mathbb{Z}_p)$. Moreover, for all the examples we consider, we verify on Sage that the Galois representation $\overline{\rho} : \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective. In particular, the image of $\overline{\rho}$ contains $\mathrm{SL}_2(\mathbb{F}_p)$. Hence, by [Ser68, Lemma 3, §3.4], the p-adic representation ρ is also surjective, as its image contains $\mathrm{SL}_2(\mathbb{Z}_p)$. Combined with the fact that $\det(\rho) : G_{\mathbb{Q}} \to \mathbb{Z}_p^{\times}$ is surjective as it coincides with the cyclotomic character, we conclude that ρ is surjective.

§6. Data

As explained in [LP19, §8.4], Coates-Sujatha's conjecture on the pseudo-nullity of the fine Selmer group over the $\mathbb{Z}_p^2$-extension of K [CS05, Conjecture B] can also be verified unconditionally for these elliptic curves in the same fashion. More specifically, if E has CM (which is the case only for 32A), we are done. Otherwise, we proceed by proving the surjectivity of the p-adic Galois representation, as summarized in the previous section.

The table below summarizes the examples we have found. The Mordell–Weil rank over $\mathbb{Q}$ and the plus and minus μ-invariants of all these examples are zero. The last column describes the data relevant to the surjectivity of Galois representation discussed above.

The code used for producing the data produces values which match those in Pollack's tables mentioned in [Pol03].

The valuations of the roots are presented as $(r : s)$, which means that there are r roots of valuation s. For our purposes, this is enough to verify condition (II), since we have found that there are no roots with common valuation between $\theta^+_{E_K}$ and $\theta^-_{E_K}$.

TABLE 1. **Data for $\mathbb{Q}(\sqrt{-m})$ where $m \not\equiv 1(\mod 4)$**

E	p	K	λ^+	roots of $\theta^+_{E_K}$	N^+	λ^-	roots of $\theta^-_{E_K}$	N^-	Relevant information for ρ
17A	3	$\mathbb{Q}(\sqrt{-362})$	4	(4:1/2)	7	2	(2:1)	6	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
32A	3	$\mathbb{Q}(\sqrt{-458})$	4	(4:1/2)	7	2	(2:1)	6	E has CM
		$\mathbb{Q}(\sqrt{-737})$	2	(2:1)	7	4	(4:1/2)	6	
		$\mathbb{Q}(\sqrt{-794})$	2	(2:1)	7	4	(4:1/2)	6	
40A	3	$\mathbb{Q}(\sqrt{-281})$	4	(4:1/2)	7	2	(2:1)	6	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
52A	3	$\mathbb{Q}(\sqrt{-134})$	4	(4:1/2)	7	2	(2:1)	6	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
		$\mathbb{Q}(\sqrt{-302})$	2	(2:1)	7	4	(4:1/2)	6	
56A	3	$\mathbb{Q}(\sqrt{-122})$	2	(2:1)	7	6	(2:1/2)(4:1/4)	8	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
		$\mathbb{Q}(\sqrt{-278})$	4	(4:1/2)	7	2	(2:1)	6	
115A	3	$\mathbb{Q}(\sqrt{-41})$	2	(2:1)	7	4	(4:1/2)	6	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
		$\mathbb{Q}(\sqrt{-293})$	2	(2:1)	7	6	(2:1/2)(4:1/4)	8	
		$\mathbb{Q}(\sqrt{-413})$	2	(2:1)	7	4	(4:1/2)	6	
		$\mathbb{Q}(\sqrt{-461})$	2	(2:1)	7	4	(4:1/2)	6	
179A	3	$\mathbb{Q}(\sqrt{-101})$	2	(2:1)	7	4	(4:1/2)	6	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
		$\mathbb{Q}(\sqrt{-305})$	4	(4:1/2)	7	2	(2:1)	6	
		$\mathbb{Q}(\sqrt{-326})$	4	(4:1/2)	7	2	(2:1)	6	
182A	3	$\mathbb{Q}(\sqrt{-86})$	4	(4:1/4)	5	2	(2:1/2)	4	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
		$\mathbb{Q}(\sqrt{-101})$	4	(4:1/2)	7	2	(2:1)	6	
		$\mathbb{Q}(\sqrt{-158})$	2	(2:1/2)	5	8	(8:1/8)	6	
		$\mathbb{Q}(\sqrt{-458})$	4	(4:1/2)	7	2	(2:1)	6	
194A	3	$\mathbb{Q}(\sqrt{-386})$	4	(4:1/2)	7	2	(2:1)	6	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$

TABLE 2. **Data for $\mathbb{Q}(\sqrt{-m})$ where $m \equiv 1(\mod 4)$**

E	p	K	λ^+	roots of $\theta^+_{E_K}$	N^+	λ^-	roots of $\theta^-_{E_K}$	N^-	Relevant information for ρ
14A	5	$\mathbb{Q}(\sqrt{-4651})$	4	(4:1/2)	7	2	(2:1)	6	ρ_5 is surjective
17A	3	$\mathbb{Q}(\sqrt{-311})$	2	(2:1)	7	4	(4:1/2)	6	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
		$\mathbb{Q}(\sqrt{-347})$	2	(2:1)	7	4	(4:1/2)	6	
		$\mathbb{Q}(\sqrt{-635})$	4	(4:1/2)	7	2	(2:1)	6	
		$\mathbb{Q}(\sqrt{-827})$	4	(4:1/2)	7	2	(2:1)	6	
		$\mathbb{Q}(\sqrt{-923})$	2	(2:1)	7	4	(4:1/2)	6	
24A	7	$\mathbb{Q}(\sqrt{-1427})$	2	(2:1)	5	6	(2:1/2)(4:1/4)	6	ρ_7 is surjective
		$\mathbb{Q}(\sqrt{-1979})$	4	(4:1/2)	5	2	(2:1)	6	
32A	3	$\mathbb{Q}(\sqrt{-1307})$	2	(2:1)	7	4	(4:1/2)	6	E has CM
		$\mathbb{Q}(\sqrt{-1523})$	2	(2:1)	7	4	(4:1/2)	6	
		$\mathbb{Q}(\sqrt{-1619})$	6	(6:1/3)	7	2	(2:1)	6	
		$\mathbb{Q}(\sqrt{-1907})$	8	(2:1/2)(6:1/6)	7	2	(2:1)	6	
		$\mathbb{Q}(\sqrt{-2003})$	2	(2:1)	7	8	(2:1/2)(6:1/6)	8	
40A	3	$\mathbb{Q}(\sqrt{-263})$	4	(4:1/2)	7	2	(2:1)	6	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
		$\mathbb{Q}(\sqrt{-971})$	4	(4:1/2)	7	2	(2:1)	6	
		$\mathbb{Q}(\sqrt{-983})$	2	(2:1)	7	6	(2:1/2)(4:1/4)	8	
52A	3	$\mathbb{Q}(\sqrt{-59})$	6	(6:1/6)	5	2	(2:1/2)	4	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
		$\mathbb{Q}(\sqrt{-83})$	2	(2:1/2)	5	6	(6:1/6)	6	
		$\mathbb{Q}(\sqrt{-203})$	2	(2:1/2)	5	4	(4:1/4)	4	
		$\mathbb{Q}(\sqrt{-359})$	4	(4:1/2)	7	2	(2:1)	6	
		$\mathbb{Q}(\sqrt{-515})$	8	(8:1/8)	5	2	(2:1/2)	4	
56A	3	$\mathbb{Q}(\sqrt{-635})$	4	(4:1/2)	7	6	(6:1/3)	8	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
98A	5	$\mathbb{Q}(\sqrt{-131})$	2	(2:1)	5	4	(4:1/2)	6	ρ_5 is surjective
115A	3	$\mathbb{Q}(\sqrt{-263})$	2	(2:1)	7	6	(6:1/6)	8	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
		$\mathbb{Q}(\sqrt{-335})$	4	(4:1/2)	7	2	(2:1)	6	
179A	3	$\mathbb{Q}(\sqrt{-239})$	2	(2:1)	7	10	(4:1/4)(6:1/6)	8	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
182A	3	$\mathbb{Q}(\sqrt{-191})$	4	(4:1/4)	5	2	(2:1/2)	4	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
194A	3	$\mathbb{Q}(\sqrt{-239})$	6	(2:1)(4:1/2)	11	2	(2:2)	10	$3^5 \mid [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$
		$\mathbb{Q}(\sqrt{-263})$	10	(10:1/5)	7	2	(2:1)	6	
		$\mathbb{Q}(\sqrt{-359})$	4	(4:1)	11	2	(2:2)	10	
		$\mathbb{Q}(\sqrt{-863})$	4	(4:1/2)	7	2	(2:1)	6	

References

[AV75] Yvette Amice and Jacques Vélu. Distributions p-adiques associées aux séries de Hecke. In Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974), Astérisque, Nos. 24-25, pages 119–131. Soc. Math. France, Paris, 1975.

[Bal] Sai Sanjeev Balakrishnan. https://github.com/saisanjeev2001/Addendum-codim-2-cycles/blob/main/final code.sage.

[BCG+22] Frauke M. Bleher, Ted Chinburg, Ralph Greenberg, Mahesh Kakde, Romyar Sharifi, and Martin J. Taylor. Exterior powers in Iwasawa theory. J. Eur. Math. Soc. (JEMS), 24(3):967–1005, 2022.

[CS05] J. Coates and R. Sujatha. Fine Selmer groups of elliptic curves over p-adic Lie extensions. Math. Ann., 331(4):809–839, 2005.

[Kat22] Takenori Kataoka. Higher codimension Iwasawa theory for elliptic curves with supersingular reduction. arXiv preprint arXiv:2206.02352, 2022.

[Kim07] Byoung Du Kim. The parity conjecture for elliptic curves at supersingular reduction primes. Compos. Math., 143(1):47–72, 2007.

[Kob84] Neal Koblitz. p-adic numbers, p-adic analysis, and zeta-functions, volume 58 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1984.

[Kob03] Shinichi Kobayashi. Iwasawa theory for elliptic curves at supersingular primes. Invent. Math., 152(1):1–36, 2003.

[LP19] Antonio Lei and Bharathwaj Palvannan. Codimension two cycles in Iwasawa theory and elliptic curves with supersingular reduction. Forum Math. Sigma, 7:Paper No. e25, 81, 2019.

[MT87] B. Mazur and J. Tate. Refined conjectures of the "Birch and Swinnerton-Dyer type". Duke Math. J., 54(2):711–750, 1987.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum. On p-adic analogs of the conjectures of Birch and Swinnerton-Dyer. Invent. Math., 84:1–48, 1986.

[Pol] Robert Pollack. https://github.com/rpollack9974/Iwasawa-invariants/blob/master/IwInv.sage.

[Pol03] Robert Pollack. On the p-adic L-function of a modular form at a supersingular prime. Duke Math. J., 118(3):523–558, 2003.

[PR04] Robert Pollack and Karl Rubin. The main conjecture for CM elliptic curves at supersingular primes. Ann. of Math. (2), 159(1):447–464, 2004.

[Ser68] Jean-Pierre Serre. Abelian l-adic representations and elliptic curves. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[SW13] William Stein and Christian Wuthrich. Algorithms for the arithmetic of elliptic curves using Iwasawa theory. Math. Comp., 82(283):1757–1792, 2013.

[Viš76] Misha M. Višik. Nonarchimedean measures associated with Dirichlet series. Mat. Sb. (N.S.), 99(141)(2):248–260, 296, 1976.

Sai Sanjeev Balakrishnan
Department of Mathematics, Indian Institute of Science, Bangalore - 560012, India
Email address: saisb@iisc.ac.in

Antonio Lei
Department of Mathematics and Statistics, University of Ottawa, 150 Louis-Pasteur Pvt, Ottawa, ON, Canada K1N 6N5
Email address: antonio.lei@uottawa.ca

Bharathwaj Palvannan
Department of Mathematics, Indian Institute of Science, Bangalore - 560012, India
Email address: bharathwaj@iisc.ac.in