This is a ``preproof'' accepted article for *Canadian Mathematical Bulletin*
This version may be subject to change during the production process.
DOI: 10.4153/S000843952500013X

A BOUND ON THE μ-INVARIANTS OF SUPERSINGULAR ELLIPTIC CURVES

RYLAN GAJEK-LEONARD

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime of good supersingular reduction. Attached to E are pairs of Iwasawa invariants $\mu_p^\pm$ and $\lambda_p^\pm$ which encode arithmetic properties of E along the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. A well-known conjecture of B. Perrin-Riou and R. Pollack asserts that $\mu_p^\pm = 0$. We provide support for this conjecture by proving that for any $\ell \geq 0$, we have $\mu_p^\pm \leq 1$ for all but finitely many primes p with $\lambda_p^\pm = \ell$. Assuming a recent conjecture of D. Kundu and A. Ray, our result implies that $\mu_p^\pm \leq 1$ holds on a density 1 set of good supersingular primes for E.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve and fix a prime p of good reduction. Attached to E is the p-primary Selmer group $\mathrm{Sel}(E/\mathbb{Q}_{\mathrm{cyc}})$, where $\mathbb{Q}_{\mathrm{cyc}}$ denotes the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. This group fits into the exact sequence

$$0 \to E(\mathbb{Q}_{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}(E/\mathbb{Q}_{\mathrm{cyc}}) \to Ш(E/\mathbb{Q}_{\mathrm{cyc}}) \to 0, \tag{1}$$

where Ш denotes the p-part of the Shafarevich-Tate group, and therefore encodes many arithmetic properties of E along the cyclotomic line.

If p is a prime of ordinary reduction then $\mathrm{Sel}(E/\mathbb{Q}_{\mathrm{cyc}})$ is cotorsion as an Iwasawa module (see [6, Theorem 17.4]) and its characteristic ideal is therefore generated by a polynomial $L_p^{\mathrm{alg}} \in \mathbb{Z}_p[T]$. The algebraic Iwasawa invariants λ_p^{alg} and μ_p^{alg} measure the degree and p-divisibility of L_p^{alg}, respectively. If $E[p]$ is irreducible as a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module, a well-known conjecture of Greenberg [5, Conjecture 1.11] asserts that $\mu_p^{\mathrm{alg}} = 0$.

If p is a prime of supersingular reduction then $\mathrm{Sel}(E/\mathbb{Q}_{\mathrm{cyc}})$ is no longer cotorsion, however Kobayashi [8] introduced signed Selmer groups $\mathrm{Sel}^\pm(E/\mathbb{Q}_{\mathrm{cyc}})$ which are cotorsion and encode analogous arithmetic data. In particular, the characteristic ideals of $\mathrm{Sel}^\pm(E/\mathbb{Q}_{\mathrm{cyc}})$ are generated by polynomials $L_{p,\mathrm{alg}}^\pm \in \mathbb{Z}_p[T]$ which have associated pairs of Iwasawa invariants $\mu_{p,\mathrm{alg}}^\pm$ and $\lambda_{p,\mathrm{alg}}^\pm$. In the supersingular setting, $E[p]$ is automatically irreducible and it is similarly conjectured (see [13, Conjecture 6.3] and [12, Conjecture 7.1]) that $\mu_{p,\mathrm{alg}}^\pm = 0$.

Recently, Chakravarthy [2, Theorem 1.3] made progress towards Greenberg's conjecture by proving that $\mu_p^{\mathrm{alg}} \leq 1$ for all but finitely many primes of good ordinary reduction. In this article, we prove a similar result in the supersingular setting.

Theorem 1.1. *Let $\ell \geq 0$ and $* \in \{+,-\}$. Then $\mu_{p,\mathrm{an}}^* \leq 1$ for all but finitely many good supersingular primes p with $\lambda_{p,\mathrm{an}}^* = \ell$.*

2020 *Mathematics Subject Classification.* Primary 11R23.

Key words and phrases. Iwasawa theory, elliptic curves, p-adic L-functions.

In the above theorem, $\lambda^{\pm}_{p,\mathrm{an}}$ and $\mu^{\pm}_{p,\mathrm{an}}$ denote the Iwasawa invariants attached to the *analytic* p-adic L-functions $L^{\pm}_{p,\mathrm{an}} \in \mathbb{Z}_p[\![T]\!]$ defined by Pollack in [13]. The construction of these p-adic L-functions requires $a_p = 0$, which is automatically true when $p > 3$. The main conjecture of Iwasawa theory in this setting asserts that $L^{\pm}_{p,\mathrm{an}}$ and $L^{\pm}_{p,\mathrm{alg}}$ generate the same ideal in $\mathbb{Z}_p[\![T]\!]$, and in particular that

$$\lambda^{\pm}_{p,\mathrm{alg}} = \lambda^{\pm}_{p,\mathrm{an}} \qquad \text{and} \qquad \mu^{\pm}_{p,\mathrm{alg}} = \mu^{\pm}_{p,\mathrm{an}}. \tag{2}$$

Thus, Theorem 1.1 provides support for the vanishing of $\mu^{\pm}_{p,\mathrm{alg}}$.

Remark 1.2. The main conjecture is known to hold in many cases: the CM case was established by Pollack and Rubin [15], and Kobayashi [8, Theorem 1.3] proved the containment $(L^{\pm}_{p,\mathrm{an}}) \subseteq (L^{\pm}_{p,\mathrm{alg}})$ for non CM curves. A proof of the full supersingular main conjecture was recently announced by Burungale, Skinner, Tian, and Wan [1, Theorem 1.2].

We henceforth assume (2) and write $\lambda^{\pm}_p$, $\mu^{\pm}_p$ to mean either algebraic or analytic invariants. Letting r_E denote the Mordell-Weil rank of E, Kundu and Ray conjecture [7, Conjecture 3.17] that $\lambda^{\pm}_p = r_E$ on a density 1 set of good supersingular primes. Assuming this conjecture, the condition on λ-invariants in Theorem 1.1 could be removed and one would have the bound $\mu^{\pm}_p \leq 1$ on a density 1 set of good supersingular primes for E.

We remark that if $r_E = 0$ then [7, Theorem 3.8] implies that both $\lambda^{\pm}_p$ and $\mu^{\pm}_p$ vanish for all but finitely many primes p (in fact, $\mathrm{Sel}^{\pm}(E/\mathbb{Q}_{\mathrm{cyc}}) = 0$ for these primes). Thus, the primary contribution of Theorem 1.1 is in providing support for the vanishing of $\mu^{\pm}_p$ in the positive rank case. We also note that, under some mild assumptions, it is known [7, Lemma 3.3] that $\lambda^{\pm}_p \geq r_E$ for all good supersingular primes $p > 2$, thus the cases where $\ell < r_E$ in Theorem 1.1 are mostly vacuous.

The crux of Chakravarthy's proof in the ordinary setting is constructing a bound (which holds for all but finitely many p) on the size of the modular symbols defining the ordinary p-adic L-function. In the supersingular case, the signed p-adic L-functions are defined via a decomposition theorem of Pollack [13, Theorem 5.6], and in particular they are not as immediately understood in terms of modular symbols. The approach taken here is to instead apply Chakravarthy's bound to the sequence of Mazur-Tate elements θ_n for E (which are defined using modular symbols), where one can show (see Proposition 3.8) that there exists an integer n_0 such that for all but finitely many primes p,

$$\mu(\theta_n) \leq 1, \quad \text{for all } n \geq n_0. \tag{3}$$

The lower bound n_0 depends only on the conductor of E (and not on p). We then relate the Iwasawa invariants of the Mazur-Tate elements to those of the signed p-adic L-functions in order to deduce Theorem 1.1.

The assumption on λ-invariants in Theorem 1.1 comes from the fact that, while one can show that $\mu(\theta_n) = \mu^*_p$ for n large enough of fixed parity (see Proposition 3.1), in this case the lower bound on n in the asymptotic depends on both p and $\lambda^{\pm}_p$. The idea is that if we assume $\lambda^{\pm}_p$ does not vary with p then it is possible to take $p \gg 0$ so that $\mu(\theta_n) = \mu^*_p$ holds for *any* fixed n, and in particular for the n_0 appearing in (3).

https://doi.org/10.4153/S000843952500013X Published online by Cambridge University Press

1.1. **Acknowledgements.** We are grateful to A. Chakravarthy, J. Hatley, A. Lei, and the anonymous referee for their helpful comments in the preparation of this article.

2. Iwasawa invariants

Fix a prime p and let F be a nonzero power series in $\Lambda = \mathbb{Z}_p[\![T]\!]$. By the Weierstrass preparation theorem [18, Theorem 7.3] there are unique nonnegative integers λ and μ such that

$$F = p^{\mu} DU, \tag{4}$$

for some distinguished polynomial $D \in \mathbb{Z}_p[T]$ of degree λ and some $U \in \Lambda^\times$. (Recall that a polynomial $D \in \mathbb{Z}_p[T]$ is called *distinguished* if $D \equiv T^{\deg D} \bmod p$.) In terms of the coefficients of $F = \sum_{i\geq 0} a_i T^i$, we have

$$\mu = \min\{\operatorname{ord}_p(a_i) \mid i \geq 0\},$$
$$\lambda = \min\{\, i \mid \operatorname{ord}_p(a_i) = \mu\}.$$

2.1. **Refined Iwasawa invariants.** Let $\Gamma \cong \mathbb{Z}_p$ be the Galois group of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and let $\Gamma_n = \Gamma/\Gamma^{p^n} \cong \mathbb{Z}/p^n\mathbb{Z}$ denote the Galois group of its nth-layer. Let $\omega_n = (1+T)^{p^n} - 1$ and $\Lambda_n = \Lambda/(\omega_n)$. Fixing a topological generator $\gamma \in \Gamma$, one has isomorphisms $\Lambda \cong \mathbb{Z}_p[\![\Gamma]\!]$ and $\Lambda_n \cong \mathbb{Z}_p[\Gamma_n]$ induced by the map $\gamma \mapsto 1+T$. *Refined* Iwasawa invariants are those attached to elements of Λ_n. We now give two definitions of refined Iwasawa invariants – both useful in different contexts – and then show that they are equivalent.

2.1.1. *Definition via the division algorithm.* Since $\Lambda = \varprojlim \Lambda_n$, for each $n \geq 0$ there is a projection map $\pi_n : \Lambda \twoheadrightarrow \Lambda_n$, $F \mapsto F \bmod \omega_n$, and we can define the Iwasawa invariants of $\pi_n(F)$ as follows. Since ω_n is a distinguished polynomial, the division algorithm for distinguished polynomials in Λ allows us to write

$$F = \omega_n Q_n + F_n,$$

for some unique $Q_n \in \Lambda$ and a polynomial $F_n \in \mathbb{Z}_p[T]$ of degree $< p^n$. Define

$$\lambda(\pi_n(F)) = \lambda(F_n),$$
$$\mu(\pi_n(F)) = \mu(F_n).$$

2.1.2. *Definition via augmentation ideals.* Following [14] and [16], one can define the Iwasawa invariants of $\theta \in \mathbb{Z}_p[\Gamma_n]$ as follows. For each $n \geq 1$, the element $\gamma_n = \gamma \bmod \Gamma^{p^n}$ generates Γ_n and we define the μ-invariant of $\theta = \sum_{j=0}^{p^n-1} c_j \gamma_n^j$ by

$$\mu(\theta) = \min_{0\leq j \leq p^{n-1}} \operatorname{ord}_p(c_j).$$

For the λ-invariant, let $\theta' = p^{-\mu(\theta)}\theta \in \mathbb{Z}_p[\Gamma_n]$ and let I_n be the augmentation ideal of $\mathbb{F}_p[\Gamma_n]$. (Thus, I_n is the ideal generated by the image of $\gamma_n - 1$ in $\mathbb{F}_p[\Gamma_n]$.) Since θ' has nonzero image under the natural reduction map $\overline{(\cdot)} : \mathbb{Z}_p[\Gamma_n] \to \mathbb{F}_p[\Gamma_n]$ and all ideals of $\mathbb{F}_p[\Gamma_n]$ are powers of I_n, we can define

$$\lambda(\theta) = \operatorname{ord}_{I_n} \overline{\theta'} = \max\{j \mid \overline{\theta'} \in I_n^j\} \in \{0, 1, \ldots, p^n - 1\}.$$

(If $n = 0$ then $\theta \in \mathbb{Z}_p$ and we define $\mu(\theta) = \operatorname{ord}_p(\theta)$ and $\lambda(\theta) = 0$.)

https://doi.org/10.4153/S000843952500013X Published online by Cambridge University Press

2.1.3. *Equivalence of definitions.* We now show that the definitions of refined Iwasawa invariants given above agree.

Proposition 2.1. *Let $n \geq 0$ and $\theta \in \mathbb{Z}_p[\Gamma_n]$. If $F \in \mathbb{Z}_p[T]$ is the unique polynomial of degree $< p^n$ mapping to θ under the composition*

$$\Lambda \twoheadrightarrow \Lambda_n \xrightarrow{\cong} \mathbb{Z}_p[\Gamma_n], \quad T \mapsto \gamma_n - 1,$$

then $\lambda(\theta) = \lambda(F)$ and $\mu(\theta) = \mu(F)$. In particular, the Iwasawa invariants defined in §2.1.1 and §2.1.2 agree.

Proof. The case $n = 0$ is clear, so suppose $n \geq 1$. Write $\theta = p^{\mu(\theta)}\theta'$ for some $\theta' \in \mathbb{Z}_p[\Gamma_n]$. Let $F_{\theta'} \in \mathbb{Z}_p[T]$ be a representative of the image of θ' in Λ_n, so $F \equiv p^{\mu(\theta)}F_{\theta'} \mod \omega_n$. By the division algorithm, we can choose $F_{\theta'}$ such that $\deg F_{\theta'} < p^n$, in which case the degree of F forces the equality $F = p^{\mu(\theta)}F_{\theta'}$ in $\mathbb{Z}_p[T]$. Since $\theta' \equiv (\gamma_n - 1)^{\lambda(\theta)}\theta'' \mod p$ for some $\theta'' \in \mathbb{Z}_p[\Gamma_n]$, the commutativity of the diagram

$$\begin{array}{ccc} \mathbb{Z}_p[\Gamma_n] & \longrightarrow & \Lambda_n \\ \downarrow & & \downarrow \\ \mathbb{F}_p[\Gamma_n] & \longrightarrow & \mathbb{F}_p[T]/(\omega_n), \end{array}$$

where the horizontal maps are $\gamma_n \mapsto 1 + T$ and the vertical maps are reduction mod p, implies that $F_{\theta'} \equiv T^{\lambda(\theta)}F_{\theta''} \mod p$ for some $F_{\theta''} \in \mathcal{O}[T]$ of degree $< p^n$. Hensel's lemma [11, §II Lemma 4.6] now gives a factorization $F_{\theta'} = DU$ in $\mathbb{Z}_p[T]$, where $D, U \in \mathcal{O}[T]$ are such that $\deg D = \lambda(\theta)$ and $D \equiv T^{\lambda(\theta)} \mod p$ (so D is distinguished), and $U \equiv F_{\theta''} \mod p$ (so $U \in \Lambda^\times$ since the constant term of $F_{\theta''}$ does not vanish mod p by maximality of $\lambda(\theta)$). It follows that $F = p^{\mu(\theta)}DU$ and by uniqueness of the Weierstrass decomposition (4), we obtain $\mu(\theta) = \mu(F)$ and $\lambda(\theta) = \lambda(F)$. □

2.1.4. *Relating invariants in Λ and Λ_n.* The following lemma is known in the literature (see [14, Remark 4.3]), though we outline a proof for completeness.

Lemma 2.2. *Let $n \geq 0$ and $F \in \Lambda$. If $\lambda(F) < p^n$ then the Iwasawa invariants of F and $\pi_n(F)$ agree.*

Proof. We may assume $\mu(F) = 0$. Use the division algorithm to write

$$F = \omega_n Q_n + F_n. \tag{5}$$

If $\mu(F_n)$ were positive then (5) implies

$$F \equiv T^{p^n}Q_n \mod p,$$

which contradicts the fact that $\lambda(F) < p^n$. Hence we must have $\mu(F_n) = 0$. From (4), we can write $F = (T^{\lambda(F)} + pF_0)U$ for some $F_0 \in \mathbb{Z}_p[T]$ of degree $< \lambda(F)$. Combining this decomposition with (5) yields

$$F_n \equiv T^{\lambda(F)}(U - T^{p^n - \lambda(F)}Q_n) \mod p,$$

but since U is a unit and $\lambda(F) < p^n$, $U - T^{p^n - \lambda(F)}Q_n$ must also be a unit. It follows that $\lambda(F_n) = \lambda(F)$. □

3. Bounding the μ-invariant

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E and fix a prime p of good reduction such that $a_p = 0$.

3.1. **Mazur-Tate elements.** Let $L_p^\pm \in \Lambda$ and $\theta_n \in \mathbb{Q}[T]$ denote the plus/minus p-adic L-functions and Mazur-Tate elements for E, as defined in §§2.9 and 6.15 of [13], respectively. The definition of both $L_p^\pm$ and θ_n depend on a choice of complex periods $\Omega_E^\pm \in \mathbb{C}$. We henceforth assume that $\Omega_E^\pm$ are p-cohomological periods for E, in the sense of [16, §2.2]. The choice of cohomological periods ensures that the coefficients of θ_n are p-integral (cf. [16, Remark 2.2]), thus we can view each θ_n as an element of the localization $\mathbb{Z}_{(p)}[T] \subseteq \mathbb{Q}[T]$.

We now relate the Iwasawa invariants of θ_n to those of $L_p^\pm$ by showing that the *even* Mazur-Tate elements recover the *minus* invariants of the p-adic L-function, and vice-versa. Let $q_1 = q_0 = 0$ and define for $n \geq 2$ the sequence

$$q_n = \begin{cases} p^{n-1} - p^{n-2} + \cdots + p - 1 & n \text{ even}, \\ p^{n-1} - p^{n-2} + \cdots + p^2 - p & n \text{ odd}. \end{cases}$$

Let $\lambda_p^\pm$ and $\mu_p^\pm$ denote the Iwasawa invariant of $L_p^\pm$.

Proposition 3.1. *If $n \geq 0$ is even (resp., odd) and $\lambda_p^- < p^n - q_n$ (resp., $\lambda_p^+ < p^n - q_n$), then*

$$\mu(\theta_n) = \mu_p^\pm,$$
$$\lambda(\theta_n) = \lambda_p^\pm + q_n,$$

where $\pm$ is opposite the parity of n.

Proof. This follows from the argument of [4, page 3], which we reproduce in brief here. Let $\varepsilon_n = \operatorname{sgn}(-1)^n$ denote the parity of n. By [13, Proposition 6.18], we have

$$\theta_n \equiv \omega_n^{-\varepsilon_n} L_p^{-\varepsilon_n} \bmod \omega_n. \tag{6}$$

Here

$$\omega_n^+ = \prod_{\substack{1 \leq i \leq n \\ i \text{ even}}} \Phi_{p^i}(1+T) \qquad \text{and} \qquad \omega_n^- = \prod_{\substack{1 \leq i \leq n \\ i \text{ odd}}} \Phi_{p^i}(1+T),$$

where $\Phi_{p^i}(T)$ is the p^ith cyclotomic polynomial. Since $\lambda(\Phi_{p^n}(1+T)) = p^n - p^{n-1}$, we have $\lambda\big(\omega_n^{-\varepsilon_n} L_p^{-\varepsilon_n}\big) = q_n + \lambda_p^{-\varepsilon_n}$. As the sequence $p^n - q_n$ tends to infinity, we may therefore take n large enough so that $\lambda\big(\omega_n^{-\varepsilon_n} L_p^{-\varepsilon_n}\big) < p^n$. The result now follows from Lemma 2.2. □

Remark 3.2. The formula for λ-invariants in Proposition 3.1 can also be found in [12, §5], [16, Theorem 4.1], and [17, Corollary 8.9], where it is instead deduced from a 3-term compatibility relation (see [16, Proposition 2.5], for example) satisfied by Mazur-Tate elements.

We now fix an integer $\ell \geq 0$ and let $X^\pm(E, \ell)$ denote the set of all good supersingular primes $p > 3$ for which $\lambda_p^\pm = \ell$.

Remark 3.3. It is conjectured [7, Conjecture 3.17] that $\lambda_p^\pm$ coincides with the Mordell-Weil rank on a density 1 set of good supersingular primes, thus one expects $X^\pm(E, \ell)$ to have density 0 except when $\ell = r_E$.

Corollary 3.4. *Fix $n \geq 1$. For all but finitely many $p \in X^{\pm}(E,\ell)$, we have*

$$\mu_p^{\pm} = \mu(\theta_n)$$

where $\pm$ is opposite the parity of n.

Proof. Since $\lambda_p^{\pm} = \ell$, we can take p large enough so that $\lambda_p^{\pm} < p^n - q_n$. For such p, Proposition 3.1 yields the desired result. □

3.2. **Modular symbols.** Let f be the cuspidal newform attached to E via modularity. For $r \in \mathbb{Q}$, recall the modular symbols of [9] defined by

$$[r]^{\pm} = \frac{\pi i}{\Omega_E^{\pm}}\bigg(\int_r^{i\infty} f(z)dz \pm \int_{-r}^{i\infty} f(z)dz\bigg).$$

For odd primes p we have by definition (see [13, Definition 6.15])

$$\theta_n = \sum_{a \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times} [a/p^{n+1}]^+ \gamma_n^{\log_\gamma a} \in \mathbb{Z}_p[\Gamma_n].$$

Here $0 \leq \log_\gamma(a) \leq p^n - 1$ is the unique integer for which $a \equiv \omega(a)(1+p)^{\log_\gamma(a)} \bmod p^{n+1}$, where $\omega : (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ is the mod p cyclotomic character (sending $a \bmod p^{n+1}$ to the $(p-1)$st root of unity $\omega(a) \in \mathbb{Z}_p^\times$ with $\omega(a) \equiv a \bmod p$.) Write $\boldsymbol{\mu}_{p-1}$ for the set of $(p-1)$st roots of unity in $\mathbb{Z}_p^\times$, and if $\alpha \in \mathbb{Z}_p$ define $[\alpha/p^n]^{\pm} = [a/p^n]^{\pm}$ where $\alpha \equiv a \bmod p^n$.

Lemma 3.5. *Let p be an odd prime of good reduction. For any $n \geq 0$ we have*

$$\mu(\theta_n) = \min_{0 \leq j \leq p^n - 1} \operatorname{ord}_p\Bigg(\sum_{\eta \in \boldsymbol{\mu}_{p-1}} \bigg[\frac{\eta(1+p)^j}{p^{n+1}}\bigg]^+\Bigg).$$

Proof. Since $\log_\gamma(a) = \log_\gamma(b)$ if and only if $a\omega(a)^{-1} = b\omega(b)^{-1} \bmod p^{n+1}$, we have

$$\theta_n = \sum_{j=0}^{p^n-1} \sum_{\eta \in \boldsymbol{\mu}_{p-1}} \bigg[\frac{\eta(1+p)^j}{p^{n+1}}\bigg]^+ \gamma_n^j. \tag{7}$$

The result now follows from Definition 2.1.2. □

Lemma 3.6. *Let $n \geq 0$ and $C \in \mathbb{R}$. For all but finitely many primes p, if $a \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ then*

$$\left| C\bigg[\frac{a}{p^{n+1}}\bigg]^+ \right| < p.$$

Proof. By Chakravarthy's bound [2, Proposition 4.1], there are constants c_1 and c_2 depending only on the conductor of E (and not p) such that for any $x \in \mathbb{Q}$,

$$|[x]^+| \leq c_1 + c_2 \log(\text{denominator}(x)).$$

The result now follows by letting $x = a/p^{n+1}$ and taking p large enough so that $c_1 + c_2 \log(p^{n+1}) < \frac{p}{|C|}$. □

Lemma 3.7. *Let p be an odd prime of good reduction. There is a constant n_0 depending only on N_E such that if $n \geq n_0$ then*

$$\sum_{\eta \in \boldsymbol{\mu}_{p-1}} \bigg[\frac{\eta(1+p)^j}{p^{n+1}}\bigg]^+ \neq 0$$

for some $0 \leq j \leq p^n - 1$.

https://doi.org/10.4153/S000843952500013X Published online by Cambridge University Press

Proof. Since p is a good prime, a result of Chinta [3, Theorem 2] guarantees the existence of an integer n_0 (depending only on N_E and not on p) such that if $n \geq n_0$ and χ is a Dirichlet character of conductor p^n then $L(E, \chi, 1) \neq 0$. Let χ be an even Dirichlet character of p-power order and conductor p^n with $n \geq n_0$. Setting $v = 1 + p$, we now have

$$\begin{aligned}\sum_{j=0}^{p^n-1} \sum_{\eta \in \boldsymbol{\mu}_{p-1}} \chi(\eta v^j) \left[\frac{\eta v^j}{p^{n+1}}\right]^+ &= \sum_{a \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times} \chi(a) \left[\frac{a}{p^{n+1}}\right]^+ \\ &= \tau(\bar{\chi}) \frac{L(E, \chi, 1)}{\Omega_E^+} \\ &\neq 0.\end{aligned}$$

Here $\tau(\chi)$ is a Gauss sum and the middle equality above is due to [10, (8.6)]. It follows that there is some $0 \leq j \leq p^n - 1$ for which

$$\sum_{\eta \in \boldsymbol{\mu}_{p-1}} \chi(\eta v^j) \left[\frac{\eta v^j}{p^{n+1}}\right]^+ = \chi(v^j) \sum_{\eta \in \boldsymbol{\mu}_{p-1}} \left[\frac{\eta v^j}{p^{n+1}}\right]^+ \neq 0,$$

where the middle equality follows from the fact that χ has p-power order and η is a $(p-1)$st root of unity. The result follows. ☐

3.3. **Main result.** We now prove our main theorem. First, we give a bound on the μ-invariants of Mazur-Tate elements.

Proposition 3.8. *There is a constant n_0 depending only on N_E such that if $n \geq n_0$ then $\mu(\theta_n) \leq 1$ for all but finitely many primes p.*

Proof. Let n_0 be as in Lemma 3.7 and take $n \geq n_0$, so that

$$\sum_{\eta \in \boldsymbol{\mu}_{p-1}} \left[\frac{\eta(1+p)^j}{p^{n+1}}\right]^+ \neq 0 \tag{8}$$

holds for all good primes $p > 2$ and some $0 \leq j \leq p^n - 1$. Note the sum in (8) is the jth coefficient of θ_n when written in the form (7). In particular, since $\theta_n \in \mathbb{Z}_{(p)}[T]$, this sum is a rational number whose denominator is d_n not divisible by p. Thus $d_n \sum_{\eta \in \boldsymbol{\mu}_{p-1}} [\eta(1+p)^j/p^{n+1}]^+$ is a nonzero integer, and from Lemma 3.6 we can take p large enough so that

$$\left| d_n \sum_{\eta \in \boldsymbol{\mu}_{p-1}} \left[\frac{\eta(1+p)^j}{p^{n+1}}\right]^+ \right| \leq \sum_{\eta \in \boldsymbol{\mu}_{p-1}} \left| d_n \left[\frac{\eta(1+p)^j}{p^{n+1}}\right]^+ \right| < (p-1)p < p^2.$$

It now follows that

$$\operatorname{ord}_p \left(\sum_{\eta \in \boldsymbol{\mu}_{p-1}} \left[\frac{\eta(1+p)^j}{p^{n+1}}\right]^+ \right) = \operatorname{ord}_p \left(d_n \sum_{\eta \in \boldsymbol{\mu}_{p-1}} \left[\frac{\eta(1+p)^j}{p^{n+1}}\right]^+ \right) \leq 1.$$

From Lemma 3.5, we now have that $\mu(\theta_n) \leq 1$. ☐

Remark 3.9. It is interesting to note that the bound in Proposition 3.8 applies to both ordinary and supersingular primes. In particular, if p is an ordinary prime then by [16, (4)] we have $\mu_p = \mu(\theta_n(f_\alpha))$ for $n \gg 0$, where $\mu_p = \mu(L_p^{\text{an}})$ and f_α is the p-stabilization of f to level pN at a root α of the Hecke polynomial $X^2 - a_p X + p$. It is therefore tempting to try to deduce Chakravarthy's result [2, Theorem 1.3] that $\mu_p \leq 1$ for all but finitely many p from Proposition 3.8, however this does not immediately follow since the Iwasawa invariants of $\theta_n(E)$ and $\theta_n(f_\alpha)$ need not always agree (see [16, Example 3.4]).

Proof of Theorem 1.1. Fix $\ell \geq 0$. It suffices to show that for all but finitely many primes $p \in X^{\pm}(E, \ell)$, we have $\mu_p^{\pm} \leq 1$. By Proposition 3.8, there exists an odd integer n^+ and an even integer n^-, neither of which depends on p, such that $\mu(\theta_{n^{\pm}}) \leq 1$ holds for all but finitely many p. But by Corollary 3.4, for either choice of sign $* \in \{+, -\}$ we have $\mu_p^* = \mu(\theta_{n^*})$ for all but finitely many $p \in X^*(E, \ell)$. $\square$

References

[1] A. Burungale, C. Skinner, Y. Tian, and X. Wan, *Zeta elements for elliptic curves and applications*, preprint (2024), arXiv:2409.01350.

[2] A. Chakravarthy, *The Iwasawa μ-invariants of elliptic curves over $\mathbb{Q}$*, preprint (2024), arXiv:2408.07826.

[3] G. Chinta, *Analytic ranks of elliptic curves over cyclotomic fields*, Journal für die reine und angewandte mathematik (2002), 13–24.

[4] R. Gajek-Leonard, *Iwasawa invariants of modular forms with $a_p = 0$*, preprint (2023), arXiv:2302.05748

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

[6] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque, no. 295 (2004), 117–290.

[7] D. Kundu and A. Ray, *Statistics for Iwasawa Invariants of Elliptic Curves*, Trans. Amer. Math. Soc., 374 (2021), no. 11, 7945–7965.

[8] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math., 152 (2003), no. 1, 1–36.

[9] B. Mazur, J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math. J., 54 (1987), no. 2, 711–750.

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

[11] J. Neukirch, *Algebraic Number Theory*, Springer (1999)

[12] B. Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, Experiment. Math., 12 (2003), no. 2, 155–186.

[13] R. Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. 118 (2003), no. 3, 523–558.

[14] R. Pollack, *An algebraic version of a theorem of Kurihara*, J. Number Theory, 110 (2005), pp. 164-177.

[15] R. Pollack and K. Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math., 159 (2004), no. 1, 447-464.

[16] R. Pollack and T. Weston, *Mazur-Tate elements of nonordinary modular forms*, Duke Math. J., 156 (2011), no. 3, 349–385.

[17] F. Sprung, *On pairs of p-adic L-functions for weight-two modular forms*, Algebra & Number Theory, 11 (2017), no. 4, 885–928.

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

Department of Mathematics, Union College, Bailey Hall 206B, Schenectady, NY 12308, USA

Email address: gajekler@union.edu

https://doi.org/10.4153/S000843952500013X Published online by Cambridge University Press