JOURNAL OF NUMBER THEORY **25**, 20–33 (1987)

On the μ-Invariant of p-Adic L-Functions Attached to Elliptic Curves with Complex Multiplication

LEILA SCHNEPS

Université de Paris-Sud, Faculté de Mathématiques,
Bâtiment 425, 91405 Orsay, France

Communicated by M. Waldschmidt

Received January 5, 1985

The main result of this paper proves that the μ-invariant is zero for the Iwasawa module which arises naturally in the study of p-power descent on an elliptic curve with complex multiplication and good ordinary reduction at the prime p. © 1987 Academic Press, Inc.

0. INTRODUCTION

Let E be an elliptic curve defined over a quadratic imaginary field K, with complex multiplication by K, and let p be a prime different from 2 and 3, where E has good reduction, and which splits in K, say $(p)=\mathfrak{p}\mathfrak{p}^*$. Let F_∞ be the field obtained by adjoining to K all $\mathfrak{p}^n$-division points on E $(n=1, 2,...)$, and let M_∞ be the maximal abelian p-extension of F_∞ unramified outside p. Write X_∞ for the Galois group of M_∞ over F_∞, endowed with its natural action of the Galois group $\mathrm{Gal}(F_\infty/K)$. Let $\Gamma=\mathrm{Gal}(F_\infty/F_0)$, where $F_0=K(E_\mathfrak{p})$. It is well known that X_∞ is a finitely generated $\mathbb{Z}_p[[\Gamma]]$-trosion $\mathbb{Z}_p[[\Gamma]]$-module. The aim of this paper is to prove that the μ-invariant of X_∞ is zero.

Our methods have been inspired by the recent work of Sinnott [9] in the cyclotomic case. The same result has been obtained independently and simultaneously by Gillard [5]; the key difference between his approach and the one in this paper is in the proof of algebraic independence (Theorem III here, I.2 in [5]). In particular, Gillard studies the schematic closure of a certain subvariety of E^n, whereas here we consider the Zariski closure of a certain subgroup of the formal group of $\tilde{E}^n$, $\tilde{E}$ being the curve reduced mod p, which permits us to establish the theorem by elementary methods. This is the only point in Sinnott's article which does not generalize easily to the elliptic case. It is also noteworthy, however, that in

0022-314X/87 $3.00

applying the results to the p-adic L-functions, Gillard used those constructed by himself in an earlier article [10], whereas here we follow the construction of the p-adic L-functions $L_{p,i}$ for $1 \leqslant i \leqslant p-2$ given in [1].

1. Notation

Let K be an imaginary quadratic field of class number 1, with ring of integers $\mathcal{O}$. Let E be an elliptic curve defined over K, with complex multiplication by $\mathcal{O}$, and let ψ be the Grossencharakter of E over K. We fix an algebraic closure $\bar{K}$ of K and an embedding $\bar{K} \subsetneq \mathbb{C}$. Let S be the set containing 2, 3, and rational primes q such that E does not have good reduction for at least one prime lying over q. Let p be a rational prime which is not in S, and such that p splits in K: $(p) = \mathfrak{p}\mathfrak{p}^*$. Let $\pi = \psi(\mathfrak{p})$. Let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$ and let $I_{\mathfrak{p}}$ be the ring of integers of the completion of the maximal abelian unramified extension of $K_{\mathfrak{p}}$. We fix a Weierstrass model for E,

$$y^2 = 4x^3 - g_2 x - g_3 \tag{1}$$

such that $g_2, g_3 \in \mathcal{O}$, and $g_2^3 - 27g_3^2$ are minimal at all primes of K not lying above a prime in S. Let L be the period lattice of the Weierstrass $\wp$-function associated with this model. Since K has class number 1, there is an $\Omega \in L$ such that $L = \Omega\mathcal{O}$.

Let $L(\bar{\psi}^k, s)$ be the complex Hecke L-function of $\bar{\psi}^k$. Let $\Omega_{\mathfrak{p}}$ be a p-adic period of E. We follow the notation of [1] in reviewing the construction of the p-adic L-functions $L_{\mathfrak{p},i}(s)$ for $1 \leqslant i \leqslant p-2$, such that for each integer $k \geqslant 1$, $k \equiv i \pmod{p-1}$,

$$\Omega_{\mathfrak{p}}^{-k} L_{\mathfrak{p},i}(k) = (k-1)!\,(1 - (\psi^k(\mathfrak{p})/N_{\mathfrak{p}}))\,\Omega^{-k} L(\bar{\psi}^k, k). \tag{2}$$

Note that the interpolated L-function is the primitive one.

Let $\phi(z, L) = (\wp(z\, L), \wp'(z, L))$. Let ω be the Teichmüller character on $\mathbb{Z}_p$, and for each $x \in \mathbb{Z}_p^*$, let $\langle x \rangle = x/\omega(x)$. Let $\hat{E}$ denote the formal group giving the kernel of reduction modulo $\mathfrak{p}$ on E: a local parameter for $\hat{E}$ is given by $t = -2x/y$. If we consider z to be the parameter for the additive formal group $\hat{G}_a$, then $t = -2\wp(z)/\wp'(z)$ gives the exponential map from $\hat{G}_a$ to $\hat{E}$. If we let w be the parameter for the multiplicative formal group $\hat{G}_m$, then since $\hat{E}$ has height 1 (since p is split), there exists a power series $\delta(w) \in wI_{\mathfrak{p}}[[w]]$ which gives an isomorphism of formal groups $\delta\colon \hat{G}_m \to \hat{E}$. The p-adic period is, by definition, the coefficient of w in δ: it is determined up to a unit in $\mathbb{Z}_p^*$.

We now introduce the basic rational functions on E (see [2] for details). Let $\alpha \in \mathcal{O}$, $\alpha \neq 0$ or a unit, and let E_α denote the kernel of α on E. For each

i, $0 \leqslant i \leqslant p-2$, such that $f_i \neq 1$, let Q_i be a primitive f_i-division point on E. Define

$$\xi_\alpha(P) = \prod_{\substack{R \in E_\alpha \\ R \neq 0}} (x(P) - x(R)) \qquad \text{and} \qquad \xi_{\alpha, Q_i}(P) = \prod_{\tau \in G_{f_i}} \xi_\alpha(P + Q_i^\tau), \quad (3)$$

where $G_{f_i} = \mathrm{Gal}(K(E_{f_i})/K)$. We have the following equation [1]. For any ideal ℓ of $\mathcal{O}$ prime to α and to f_1,

$$\prod_{S \in E_\ell} \xi_{\alpha, Q_i}(P + S) \sim \xi_{\alpha, Q_i \sigma_\ell}(\psi(\ell) P), \tag{4}$$

where σ_ℓ is the Artin symbol of ℓ relative to $K(E_{f_i})/K$, and the symbol $\sim$ means that the quotient of the two functions is a constant in K^*.

We now consider the development of the rational functions in (3) in the parameter z of the additive formal group, and define

$$R_{\alpha,i}(z, L) = \begin{cases} \xi_\alpha(\phi(z, L)) & \text{if } f_i = 1, \\ \xi_{\alpha, Q_i}(\phi(z, L)) & \text{otherwise.} \end{cases}$$

Let $m_i =$ card(Gal$(K(E_{f_i})/K)$) for each i. Consider the set $\mathcal{U}$ of maps μ: $A \rightarrow \mathbb{Z}$, where A is the set of elements of $\mathcal{O}$ prime to f_1 and to $\mathfrak{p}$, and where

$$\mu(\alpha) = 0 \text{ for almost all } \alpha \in A \qquad \text{and} \qquad \sum_{\alpha \in A} \mu(\alpha)(N\alpha - 1) = 0.$$

For $\mu \in \mathcal{U}$, let $\tilde{R}_{\mu,i}(z, L) = \prod_{\alpha \in A} (\alpha^{2m_i} R_{\alpha,i}(z, L))^{\mu(\alpha)}$. Then $(d/dz) \log \tilde{R}_{\mu,i}$ (z, L) has a Laurent series expansion in t which is an integral power series in $I_{\mathfrak{p}}[[t]]$, and for a suitable choice of μ, this is the series underlying the construction of the $L_{\mathfrak{p},i}(s)$ (see [1, 3]).

In order to complete the construction, we need to introduce several basic facts about gamma-transforms (for more details see [9]). Let Λ_m be the space of $I_{\mathfrak{p}}$-valued measures on $\mathbb{Z}_p$, and let C denote a compact-open subset of $\mathbb{Z}_p$:

(a) There is an isomorphism $\Lambda_m \rightarrow I_{\mathfrak{p}}[[w]]$ given by $\lambda \mapsto H_\lambda(w)$, where $H_\lambda(w) = \sum_{n \geqslant 0} (\int_{\mathbb{Z}_p} \binom{x}{n} \, d\lambda) \, w^n = \int_{\mathbb{Z}_p} (1 + w)^x \, d\lambda$.

(b) Let $f(x) = \sum_i a_i \zeta_i^x$ be the characteristic function of C, where ζ_i are p-power roots of unity [9]. We define a measure $\lambda|_C$ by restricting λ to C and extending by zero. Then the power series $H_{\lambda|_C}(w)$ associated to $\lambda|_C$ is given by

$$\sum a_i H_\lambda(\zeta_i(1 + w) - 1). \tag{5}$$

In particular, if $C=\mathbb{Z}_p^*$, we write λ^* for $\lambda|_{\mathbb{Z}_p^*}$ and $H_\lambda^*(w)$ for $H_{\lambda^*}(w)$. We then have

$$H_\lambda^*(w)=H_\lambda(w)-\frac{1}{p}\sum_{\zeta^p=1}H_\lambda(\zeta(1+w)-1). \tag{6}$$

(c) We define the measure $\lambda\circ\gamma$ for $\gamma\in\mathbb{Z}_p^*$ by $\lambda\circ\gamma(C)=\lambda(\gamma C)$. Then $H_{\lambda\circ\gamma}(w)=H_\lambda(w^{\gamma^{-1}})$, and we have the formula

$$\lambda\circ\gamma|_C=\lambda|_{\gamma C}\circ\gamma. \tag{7}$$

(d) We now discuss the gamma-transform. Let $J(t)\in I_\wp[[t]]$, and set $\tilde{J}(w)\in I_\wp[[w]]$ equal to $J(\delta(w))$ viewed as a power series in w. Let λ be the measure associated to the series $\tilde{J}(w)$. For each i, $0\leqslant i\leqslant p-2$, we define

$$\Gamma_\lambda^{(i)}(s)=\int_{\mathbb{Z}_p^*}\langle x\rangle^s\,\omega^i(x)\,d\lambda \tag{8}$$

and we may thus speak of the gamma transform of a measure associated with a power series in t. Clearly $\Gamma_\lambda^{(i)}(s)$ is an Iwasawa function, i.e., if u is a topological generator of $1+pZ_p$, then there exists a power series $G_i(w)\in I_\wp[[w]]$ such that $G_i(u^s-1)=\Gamma_\lambda^{(i)}(s)$. Let ϕ: $\mathbb{Z}_p\to U=1+pZ_p$ be the isomorphism given by $y\mapsto u^y$. Then as a power series, $G_i(w)$ corresponds to the measure in Λ_m given by

$$\left(\sum_\varepsilon \varepsilon^i\lambda\circ\varepsilon|_U\right)\circ\phi, \tag{9}$$

where the sum is over the $(p-1)$th roots of unity in $\mathbb{Z}_p$ (see [9]). By (c) above, we may write (9) as

$$\left(\sum_\varepsilon \varepsilon^i\lambda|_{\varepsilon U}\circ\varepsilon\right)\circ\phi. \tag{10}$$

We now apply the gamma-transform of (d) to the measure whose associated power series in t is the Laurent expansion of $(d/dz)\log\tilde{R}_{\mu,i}(z,L)$. Up to multiplication by units in the Iwasawa algebra, this gives the functions $L_{\wp,i}(s)$ for $1\leqslant i\leqslant p-2$ (see [1] for the complete construction). Now, the μ-invariant of $\Gamma_\lambda^{(i)}(s)$ is considered by definition to be the μ-invariant of the associated power series $G_i(w)$, i.e., the infimum of the valuations of its coefficients. Thus it clearly suffices to study the μ-invariant of the gamma-transform to determine the μ-invariant of $L_{\wp,i}(s)$.

2. μ-Invariants of Certain Gamma-Transforms

Let E be an elliptic curve as in Section 1, and let $R(P)$ be a rational function on E: by a slight abuse of notation we write $R(t)$ for the expansion of R as a Laurent series in t, where $t = -2x/y$ is a local parameter at zero on $\hat{E}$. We suppose that $R(t) \in I_{\mathfrak{p}}[[t]]$.

Let δ: $\hat{G}_m \to \hat{E}$ be the isomorphism of formal groups as in Section 1, and consider a measure λ on $\mathbb{Z}_p$ with values in $I_{\mathfrak{p}}$ whose associated power series in $I_{\mathfrak{p}}[[w]]$ has the form $R(\delta(w))$ for $R(P)$ as above. Let W denote the set of roots of unity in K. The aim of this section is to apply the methods used by Sinnott in the cyclotomic case (see [9]) to prove

Theorem I. *For each i, $0 \leqslant i \leqslant p-2$, we have the formula*

$$\mu\left(\sum_{v \in W} \omega^i(v)\, \lambda^* \circ (v)\right) = \mu(\Gamma_\lambda^{(i)}(s)).$$

Before the proof of Theorem I, we need several preliminary remarks. Let r be the number of roots of unity in K, $m = (p-1)/r$, and $\beta_1, ..., \beta_n$ be a basis for the $\mathcal{O}$-module generated by the $(p-1)$th roots of unity in $\mathbb{Z}_p$. For $1 \leqslant j \leqslant m$, let ε_j be representatives of the $(p-1)$th roots of unity modulo W. Then

$$\varepsilon_j = \sum_i a_{ij} \beta_i, \qquad a_{ij} \in \mathcal{O} \tag{11}$$

for $1 \leqslant j \leqslant m$.

Now, since we are considering μ-invariants, we will wish to consider the reduction of our power series $R(\delta(w))$ modulo $\mathfrak{p}$. To this end, we denote by $\tilde{\delta}(w)$ the power series $\delta(w)$ modulo $\mathfrak{p}$, so $\tilde{\delta}(w)$ has coefficients in $\bar{\mathbb{F}}_p$, the algebraic closure of $\mathbb{F}_p$. Letting $\tilde{E}$ denote the curve reduced mod $\mathfrak{p}$, we see that $\tilde{\delta}(w)$ gives a formal group isomorphism from the multiplicative formal group in characteristic p to the formal group of $\tilde{E}$, which we denote by $\hat{\varepsilon}$. But since the points of $\hat{E}$ all reduce to $0 \bmod \mathfrak{p}$, we let $B = \bar{\mathbb{F}}_p[[T]]$ for an indeterminate T, and we extend the field of definition of $\tilde{E}$ to the quotient field of B. We also consider B to be the underlying set for $\hat{G}_m$ in characteristic p. Then $\tilde{\delta}$ converges to a value on $\hat{\varepsilon}$ whenever w has its value in the maximal ideal of B, which is the ideal generated by T.

We now recall that for each element $\beta \in \mathbb{Z}_p$, there exists a unique power series, usually denoted $[\beta]$ (t), such that $[\beta](t) \equiv \beta t \pmod{\deg 2}$ and $[\beta](t)$ is an endomorphism of $\hat{E}$ (see [8]). We use the notation $q_\beta(t) = [\beta](t)$ and write $\tilde{q}_\beta(t)$ for the reduction of $q_\beta(t) \bmod \mathfrak{p}$.

Now, let E^n be the abelian variety consisting of the product of n copies of E, and let $t_1, ..., t_n$ be the copies of t coming from the n coordinate projections $E^n \to E$. Let $K(E^n)$ denote the field of rational functions on E^n developed out in their Laurent expansions at $t_1,\dots, t_n$, and let $A = K(E^n) \cap I_{\wp}[[t_1,\dots, t_n]]$. In the same vein, we write $\tilde{A} = K(\tilde{E}^n) \cap B[[t_1,\dots, t_n]]$ for rational functions on the reduced abelian variety.

We now state two independence results which are fundamental to the proof of Theorem I. For the a_{ij} as in (11), we have

THEOREM II. *For $1 \leqslant j \leqslant m$, let $\Phi_j\colon \tilde{E}^n \to \tilde{E}$ be the map given by*

$$\Phi_j(P_1,\dots, P_n) = \sum_i a_{ij} P_i,$$

and suppose $r_1,\dots, r_m$ are rational functions on $\tilde{E}$ such that

$$\sum_{j=1}^{m} r_j(\Phi_j(x)) = 0 \qquad \text{for all} \quad x \in \tilde{E}^n.$$

Then each r_j is a constant function on $\tilde{E}$.

THEOREM III. *Let $\Theta\colon B[[t_1,\dots, t_n]] \to B[[t]]$ be the map given by $\Theta(t_i) = q_{\beta_i}(t)$. Then the restriction of Θ to $\tilde{A}$ is injective in the sense that if $r \in \tilde{A}$ and $r(\tilde{q}_{\beta_1}(t),\dots, \tilde{q}_{\beta_n}(t)) = 0$, then $r = 0$ identically.*

Theorems II and III will be proven at the end of this section. We now proceed to the proof of Theorem I. Let λ be a measure on $\mathbb{Z}_p$ as before whose associated power series has the form $R(\delta(w)) \in I_{\wp}[[w]]$ for $R \in A$. We have

PROPOSITION. *Let C be a compact-open set in $\mathbb{Z}_p$. Then the power series associated to $\lambda|_C$ has the form $R_C(\delta(w))$, where R_C is also a rational function on E.*

Proof. We may write $\sum_i b_i \zeta_i^x$ for the characteristic function of C, as in Section 1(b). Then the power series associated to $\lambda|_C$ is given by $\sum_i b_i R(\delta(\zeta_i(1+w)-1))$. Now, since δ is an isomorphism of formal groups, and $\zeta_i - 1$ is in the maximal ideal of $I_{\wp}$, we see that $\zeta_i - 1$ corresponds under δ to the t coordinate of a π-power division point V_i on E. Thus,

$$\begin{aligned}\sum_i b_i R(\delta(\zeta_i(1+w)-1)) &= \sum_i b_i R(\delta(\zeta_i - 1) \oplus_E \delta(w)) \\ &= \sum_i b_i R(t(V_i) \oplus_E t),\end{aligned}$$

which is the expansion of $\sum_i b_i R(V_i \oplus_E P)$ in t. By definition, this function is $R_C(P)$. But R_C is a rational function on E since addition on E is rational, and $\lambda|_C$ is associated to $R_C(\delta(w))$, which concludes the proof.

Now, for each i, $0 \leqslant i \leqslant p-2$, define a measure

$$\kappa_i = \sum_{v \in W} \omega^i(v)\, \lambda^* \circ (v).$$

We first remark that κ_i is associated with a rational function in $\delta(w)$ on E. For by the preceding proposition, λ^* is associated with a rational function $R^*(\delta(w))$, and then by Section 1(c), $\lambda^* \circ (v)$ is associated to $R^*(\delta((1+w)^{v^{-1}}-1)) = R^*([v^{-1}](\delta(w))) = R(v^{-1}P)$ on E. Now, we are considering the μ-invariant of a measure to be the μ-invariant of its associated power series; this is how we investigate the μ-invariants in the statement of Theorem I, which we recall as

$$\mu\left(\sum_{v \in W} \omega^i(v)\, \lambda^* \circ (v)\right) = \mu(\Gamma_\lambda^{(i)}(s)). \tag{12}$$

In fact, proving the simpler formula

$$\mu(\kappa_i) = \mu(\Gamma_{\kappa_i}^{(i)}(s)) \tag{13}$$

is equivalent to proving (12), for the left-hand sides are the same by definition, and for the right-hand sides we have

$$\begin{aligned}
\Gamma_{\kappa_i}^{(i)}(s) &= \sum_{v \in W} \omega^i(v) \int_{\mathbb{Z}_p^*} \langle x \rangle^s\, \omega^i(x)\, d\lambda^* \circ (v) \\
&= \sum_{v \in W} \omega^i(v) \int_{\mathbb{Z}_p^*} \langle v^{-1}x \rangle^s\, \omega^i(v^{-1}x)\, d\lambda^* \\
&= \sum_{v \in W} \omega^i(v)\, \omega^i(v^{-1}) \int_{\mathbb{Z}_p^*} \langle x \rangle^s\, \omega^i(x)\, d\lambda \\
&= r\Gamma_\lambda^{(i)}(s).
\end{aligned}$$

Thus, since we have stipulated that $p \neq 2$ or 3, and r must always be 2, 4, or 6, we have

$$\mu(\Gamma_\lambda^{(i)}(s)) = \mu(\Gamma_{\kappa_i}^{(i)}(s)).$$

To prove (13), we prove that divisibility by π of κ_i (i.e., of its associated power series) implies that of $\Gamma_{\kappa_i}^{(i)}(s)$ and vice versa, thus, cancelling the factors of π from both sides gives (13). The first implication is evident, since if π divides κ_i then it certainly divides $\sum_\varepsilon \varepsilon^i \kappa_i \circ \varepsilon|_U$ (Eq. (9)), so $\Gamma_{\kappa_i}^{(i)}(s)$, by Section 1(d). The second implication is not trivial. Suppose π divides $\sum_\varepsilon \varepsilon^i \kappa_i \circ \varepsilon|_U$. Then π divides $r \sum_{j=1}^m \varepsilon_j^{-i} \kappa_i|_{(\varepsilon_j^{-1}U)} \circ (\varepsilon_j^{-1})$, reformulating as in (10).

Let $r_j(\delta(w))$ be the power series corresponding to the measure $\varepsilon_j^{-i}\kappa_i|_{(\varepsilon_j^{-1}U)}$. We may then write the assumption that π divides the gamma-transform as

$$\sum_{j=1}^{m} r_j(\delta((1+w)^{\varepsilon_j}-1)) \equiv 0 \ (\mathrm{mod}\ \pi I_{\mathfrak{p}}[[w]]). \tag{14}$$

Considering the rational functions $\tilde{r}_j$ on $\tilde{E}$ and the whole situation in characteristic p, we have

$$\sum_{j=1}^{m} \tilde{r}_j([\tilde{\varepsilon}_j]\,\tilde{\delta}(w))=0. \tag{15}$$

Thus using the notation $\tilde{q}_{\varepsilon_j}(t)$ for $[\varepsilon_j](t)$ reduced mod $\mathfrak{p}$, we have

$$\sum_{j=1}^{m} \tilde{r}_j(\tilde{q}_{\varepsilon_j}(t))=0. \tag{16}$$

Now, in the notation of Theorem II, let Φ_j: $\tilde{E}^n \to \tilde{E}$ be defined by

$$\Phi_j(t_1,\dots,t_n)=\sum_{i=1}^{n} \tilde{q}_{a_{ij}}(t_i),$$

for the a_{ij} as in (11). Then (16) may be written

$$\sum_{j=1}^{m} \tilde{r}_j(\Phi_j(\tilde{q}_{\beta_1}(t),\dots,\tilde{q}_{\beta_n}(t))=0. \tag{17}$$

Now, by Theorem III, this statement implies that the function $\sum_{j=1}^{m} \tilde{r}_j \circ \Phi_j$ on $\tilde{E}^n$ is identically zero, and by Theorem II, we obtain that each $\tilde{r}_j$ is then a constant function on $\tilde{E}$, so that $\sum_{j=1}^{m} \tilde{r}_j=0$, or equivalently, $\sum_{j=1}^{m} r_j \equiv 0$ (mod $\pi I_{\mathfrak{p}}[[w]]$).

Finally, recalling that $r_j(P)$ was the rational function on E associated to the measure $\varepsilon_j^{-i}\kappa_i|_{(\varepsilon_j^{-1}U)}$, we obtain

$$\begin{aligned}\kappa_i &= \sum_{j=1}^{m} \sum_{v\in W} \varepsilon_j^{-i}\kappa_i|_{(\varepsilon_j^{-1}U)} \circ (v)\\ &= \sum_{v\in W}\left(\sum_{j=1}^{m} r_j(vP)\right) \equiv 0 \ (\mathrm{mod}\ \mathfrak{p}),\end{aligned}$$

so κ_i is divisible by π, which concludes the proof.

We note that since the p-adic L-function is constructed by taking the gamma-transform of a measure whose power series is exactly the development in w of a rational function on E, we may apply Theorem I to obtain information on their μ-invariant. This is done in Section 3. We now prove Theorems II and III.

Proof of Theorem II. First, note that since $\varepsilon_j = \sum_{i=1}^{n} a_{ij}\beta_i$ and $\Phi_j(P_1, \ldots, P_n) = \sum_{i=1}^{n} a_{ij} P_i$, we must have the condition

$$a \circ \Phi_i = b \circ \Phi_j \Leftrightarrow a = b = 0$$

for $a, b \in \mathcal{O}$, and $i \neq j$, since this is clearly true of the ε_j. This and algebraicity are the only conditions on the Φ_j which are needed in the proof of Theorem 2. The algebraicity of the Φ_j means that since they are certainly not constant maps, they must be surjective onto E. Now, let $K_j = \operatorname{Ker} \Phi_j$. We will show that whenever $i \neq j$, $\Phi_i|_{K_j}$ is still surjective onto E. If it were not, it would be constant, so its image would be e, the identity element of E. Now, obviously, $\Phi_j|_{K_j} = e$, so we have induced maps

$$\bar{\Phi}_j : \tilde{E}^n/K_j \to \tilde{E} \qquad \text{and} \qquad \bar{\Phi}_i : \tilde{E}^n/K_j \to \tilde{E}.$$

Thus, $\bar{\Phi}_i \circ \bar{\Phi}_j^{-1}$ is an endomorphism of E, so some $\gamma \in \mathcal{O}$. But then $1 \circ \Phi_i = \gamma \circ \Phi_j$, which is not possible. So $\Phi_i|_{K_j}$ is surjective.

Now, let $P_0 \in \tilde{E}$ be a point at which r_m has a pole. Then $r_m(P_0 \oplus_{\tilde{\varepsilon}} P)$ has a pole at e. Choose R_0 in $\tilde{E}^n$ such that $\Phi_m(R_0) = P_0$; then we still must have

$$\sum_{j=1}^{m} r_j \circ \Phi_j(R_0 + R) = 0 \qquad \forall R \in \tilde{E}^n,$$

so it suffices to know Theorem II for the functions $r_j(\Phi_j(R_0) \oplus_{\tilde{\varepsilon}} P)$, i.e., we may suppose that r_m has a pole at e.

Let D_j be the set of poles of r_j; then $\Phi_j^{-1}(D_j) \cap K_m$, for $1 \leqslant j \leqslant m$, must have codimension 1 in K_m, otherwise Φ_j would be constant on K_m, which is not the case. So $\sum_{j=1}^{m-1} \Phi_j^{-1}(D_j) \cap K_m$ has codimension 1 in K_m. Thus, we can choose an R_1 in K_m such that $\Phi_j(R_1) \notin D_j$, $1 \leqslant j \leqslant m-1$. We can now write

$$r_m \circ \Phi_m(R) = r_m \circ \Phi_m(R_1 + R) = -\sum_{j=1}^{m-1} r_j \circ \Phi_j(R_1 + R).$$

But the right-hand side is regular, implying that r_m has no pole at e! Evidently, the procedure works for each of the r_j in the same way, so they are all constant functions on $\tilde{E}$. This concludes the proof of Theorem II.

Proof of Theorem III. We need a long series of lemmas.

LEMMA 1. *Let H be a Zariski-closed subgroup $\not\subseteq \tilde{E}^n$. Then there exists a non-trivial homomorphism Φ: $\tilde{E}^n \to \tilde{E}$ such that $H \subset \operatorname{Ker} \Phi$.*

Proof. Let I_i: $\tilde{E} \to \tilde{E}^n$ be inclusion of the ith factor for $1 \leqslant i \leqslant n$. Then since H is a proper subgroup, there exists j between 1 and n such that

$\operatorname{Im} I_j \not\subseteq H$. Thus the composition $\tau\colon \tilde{E} \xrightarrow{I_j} \tilde{E}^n \to \tilde{E}^n/H$ is non-trivial, and since H is closed, $\tilde{E}^n/H$ is an abelian variety. So the dual $\tau^*\colon (\tilde{E}^n/H)^* \to \tilde{E}$ (as abelian varieties) is non-trivial. But $\tilde{E}^n/H$ is isogenous to $(\tilde{E}^n/H)^*$, so choosing an isogeny $f\colon \tilde{E}^n/H \to (\tilde{E}/H)^*$, we have $\tau^* \circ f\colon \tilde{E}^n/H \to \tilde{E}$ non-trivial. Then $\Phi\colon \tilde{E}^n \to \tilde{E}^n/H \xrightarrow{\tau^* \circ f} \tilde{E}$ is non-trivial and $H \subset \operatorname{Ker} \Phi$.

Lemma 2. *Let $\Phi\colon \tilde{E}^n \to \tilde{E}$ be a homomorphism. Then Φ has the form*

$$\Phi(Q_1, \ldots, Q_n) = \sum_{i=1}^{n} \alpha_i Q_i, \qquad \alpha_i \in \mathcal{O}.$$

Proof. In the notation above, set $\alpha_i = \Phi \circ I_i\colon \tilde{E} \to \tilde{E}$. Then

$$\Phi(Q_1, \ldots, Q_n) = \Phi\left(\sum_{i=1}^{n} I_i(Q_i) \right) = \sum_{i=1}^{n} \alpha_i Q_i.$$

Lemma 3. *If G is a subgroup of $\tilde{E}^n$, and H is its Zariski closure, then H is also a subgroup.*

Proof. It suffices to show that H is closed under addition and inverses. Let $A\colon H \times H \to H'$ be addition. For any algebraic map ϕ which is zero on G, we know ϕ must be zero on H. But then $\phi \circ A$ is zero on $H \times H$ since it is zero on $G \times G$ and $H \times H$ is the Zariski closure of $G \times G$. But this means ϕ is zero on H', so $H' \subset H$. The argument for inverses is analogous.

Lemma 4. *Let $\beta_1, \ldots, \beta_n$ be elements of $\mathbb{Z}_p$ which are linearly independent over $\mathcal{O}$, and write $t = \tilde{\delta}(w)$ as usual. Let F be the algebraic closure of the quotient field of the ring B, R the ring of integers of F, and M the maximal ideal of R. Let*

$$G = \{ (\tilde{q}_{\beta_1}(t), \ldots, \tilde{q}_{\beta_n}(t)) \mid t = \tilde{\delta}(w),\ w \in M \}.$$

Then G is Zariski dense in $\tilde{E}^n$ (considered to be defined over F).

Proof. Recall that whenever w is in M, then $\tilde{\delta}(w)$ converges to an actual value on the formal group of $\tilde{E}$. Let H denote the Zariski closure of G. Then by Lemma 3, H is a subgroup of $\tilde{E}^n$. If $H \neq \tilde{E}^n$, then by Lemmas 1 and 2, there exist elements $\alpha_1, \ldots, \alpha_n \in \mathcal{O}$, not all zero, such that

$$\sum_{i=1}^{n} \alpha_i Q_i = 0 \qquad \forall (Q_1, \ldots, Q_n) \in H.$$

But then, we may write this as

$$\sum_{i=1}^{n} \alpha_i \tilde{q}_{\beta_i}(t) = \sum_{i=1}^{n} \alpha_i [\tilde{\beta}_i](t) = \left[\sum_{i=1}^{n} \alpha_i \tilde{\beta}_i \right](t) = 0$$

for all t on the formal group of $\tilde{E}$, so $\sum_{i=1}^{n} \alpha_i \beta_i = 0$. But this is not possible, so we must have $H = \tilde{E}^n$.

We may conclude the proof of Theorem 3. Suppose that for some $r \in \tilde{A}$, we have $\Theta(r) = 0$. This means

$$r(\tilde{q}_{\beta_1}(t),..., \tilde{q}_{\beta_n}(t)) = 0.$$

But r is continuous in the Zariski topology, so it must be zero on all of $\tilde{E}^n$.

3. The μ-Invariant of the p-Adic L-Function

The aim of this section is to apply the results of Section 2 to the measure associated to the p-adic L-function, as discussed in Section 1. In particular, we prove

Theorem IV. $\mu(X_{\infty}) = 0$.

In order to do so, we show that the μ-invariant of each $L_{\not{p},i}(s)$ is zero. Indeed, it is shown in [1] that the μ-invariant of X_{∞} is equal to the sum of the μ-invariants of the $L_{\not{p},i}(s)$ for $1 \leqslant i \leqslant p-2$.

Recall from Section 1 that for each i, $1 \leqslant i \leqslant p-2$, and for a suitable choice of μ, the integral power series expansion of the rational function on the curve

$$\frac{d}{dz} \log \tilde{R}_{\mu,i}(z, L) = \frac{d}{dz} \log \prod_{\alpha} (\alpha^{2m_i} R_{\alpha,i}(z, L))^{\mu(\alpha)} \tag{18}$$

is exactly the power series which gives the measure associated to $L_{\not{p},i}(s)$ as in Section 1(a).

Lemma 1. *For each i, $1 \leqslant i \leqslant p-2$, we have $\mu(\lambda_i) = 0$, where the series associated to λ_i is the development in w of $(d/dz) \log \tilde{R}_{\mu,i}(z, L)$.*

Proof. We show that as a rational function on E, $(d/dz) \log \tilde{R}_{\mu,i}(z, L)$ does not reduce to zero mod $\not{p}$, in fact, we exhibit its poles on $\tilde{E}$. Recall that $r = \# W$.

Let $S = \{\alpha \in A \mid \mu(\alpha) \neq 0\}$, and $\mathscr{L} = \{R \in E \mid R$ is a point of α-division for some $\alpha \in S\}$. Now, since all $\alpha \in S$ are prime to $\not{p}$ and prime to each other (see [1, Lemma II.7; 3, Lemma 28]), we have that reduction mod$\not{p}$ is injective on $\mathscr{L}$. We separate the proof into two cases.

Case 1. $f_i = 1$, i.e., r divides i. We explicitly write down the rational function on the curve from (18):

$$\begin{aligned}\sum_{\alpha\in A}\mu(\alpha)\frac{d}{dz}\log\prod_{\substack{R\in E_\alpha,\\ R\neq 0}}(x(P)-x(R))\\ =\sum_{\alpha\in A}\mu(\alpha)\sum_{R}\frac{-2y(P)}{x(P)-x(R)},\end{aligned}\tag{19}$$

from which it is easy to see that the poles must come from the points 0 and $R\in\mathscr{L}$. Now, in fact, the residue at 0 is exactly $\sum_{\alpha\in A}\mu(\alpha)(N\alpha-1)=0$, so there is no pole there. However, the residue at each R is $-2\mu(\alpha)$, and since $\mu(\alpha)=\pm 1$ (see [1]), this does not reduce to zero mod $\mathfrak{p}$. Moreover, since reduction mod $\mathfrak{p}$ is injective on $\mathscr{L}$, all the points in $\mathscr{L}$ give poles of the reduced function on $\tilde{E}$.

Case 2. $f_i\neq 1$. The only difference with Case 1 is in the explicit expression of the function associated to λ_i:

$$\begin{aligned}\sum_{\alpha}\mu(\alpha)\frac{d}{dz}\log\prod_{R}\prod_{\tau}(x(P+Q_i^\tau)-x(R))\\ =\sum_{\alpha}\sum_{R}\sum_{\tau}\mu(\alpha)\frac{-2y(P+Q_i^\tau)}{x(P+Q_i^\tau)-x(R)}.\end{aligned}$$

Here again, the poles come from the points $-Q_i^\tau$ and $R-Q_i^\tau$ for all $\tau\in G_{f_i}$ and $R\in\mathscr{L}$. Now, the residue of each pole at $-Q_i^\tau$ is again $\sum_\alpha\mu(\alpha)(N\alpha-1)=0$, so there are actually no poles there. But the poles coming from the $R-Q_i^\tau$ have residue $-2\mu(\alpha)$, which as before is prime to $\mathfrak{p}$ for each α (see [3, Lemma 28]). Moreover, since each $R-Q_i^\tau$ is a primitive αf_i-division point, again reduction mod $\mathfrak{p}$ is injective on this set, so each $R-Q_i^\tau$ gives a pole of the reduced function on $\tilde{E}$. This concludes the proof.

LEMMA 2. *The μ-invariant of λ_i^* is zero.*

Proof. In fact, we show that the μ-invariant of $\lambda_i|_{p\mathbb{Z}_p}$ is not zero, from which the result follows. Note that the characteristic function of $p\mathbb{Z}_p$ is $(1/p)\sum_{\zeta^p=1}\zeta^x$. Now, the power series associated with λ_i is the development in w of $\sum_{\alpha\in A}\mu(\alpha)(d/dz)\log\xi_{\alpha,Q_i}(P)$ when $f_i\neq 1$, so by Section 1(b), the power series associated with $\lambda_i|_{p\mathbb{Z}_p}$ is $\sum_{\alpha\in A}\mu(\alpha)(d/dz)\log\prod_{S\in E_\pi}\xi_{\alpha,Q_i}(P+S)$, which by the functional equation (4) given in Section 1, can be written

$$\sum_{\alpha\in A}\mu(\alpha)\frac{1}{p}\left[\frac{d}{dz}\log\xi_{\alpha,Q_i\sigma_{\mathfrak{p}}}([\pi]P)\right].\tag{20}$$

Now, by the chain rule, we can write $\sum_{\alpha \in A} \mu(\alpha)(\pi/p)[(d/dz) \log \xi_{\alpha, Q_i \sigma_{\mathfrak{p}}}]([\pi]P)$ for (20), which allows us to reduce modulo $\mathfrak{p}$. The poles of this function come from the points $-Q_i^{\tau\sigma_{\mathfrak{p}}} + S$ and $R - Q_i^{\tau\sigma_{\mathfrak{p}}} + S$ for all $\tau \in G_{f_i}$, $R \in \mathscr{L}$, and $S \in E_\pi$. But all the S reduce to zero mod $\mathfrak{p}$, so evidently the residue of each pole is a multiple of p, and thus reduces to zero mod $\mathfrak{p}$. Thus the rational function in (20) is divisible by p, which concludes the proof.

LEMMA 3. *The μ-invariant of the measure*

$$\sum_{v \in W} \omega^i(v)\, \lambda_i^* \circ (v)$$

is zero.

Proof. As usual, we divide into two cases.

Case 1. $f_i = 1$, i.e., r divides i. In this case, the measure in the lemma becomes simply $\sum_{v \in W} \lambda_i^* \circ (v)$, since $\omega^i(v) = 1$ for each $v \in W$. But the poles of λ_i^* are given by the points $R \in \mathscr{L}$, and the v are isomorphisms of E, so they only permute the poles. So $\lambda_i^* \circ (v) = \lambda_i^*$ for each v, and the measure can be written $r\lambda_i^*$. Now the result of Lemma 2 concludes the proof.

Case 2. $f_i \neq 1$. Let us consider the set of poles of the form

$$P_R = \{R - Q_i^\tau \mid \tau \in G_{f_i}\}.$$

We attach a P_R to each $R \in \mathscr{L}$. For each P_R, let $v^{-1}P_R$ denote the set $\{v^{-1}(R - Q_i^\tau) \mid \tau \in G_{f_i}\}$. Now, since the orbit of Q_i under the τ lies entirely in one congruence class modulo W, the $v^{-1}P_R$ are completely disjoint sets for R fixed and v varying in W. We show, moreover, that if $v^{-1}P_{R_1} = v^{-1}P_{R_2}$, then $R_1 = R_2$. For first of all, R_1 and R_2 would have to be points of α-division for the same α. But then, letting f_i act on both sides of the equality, we would have $R_1 = R_2$. This shows that for v fixed, the poles of $\lambda_i^* \circ (v)$ are given by the $v^{-1}P_R$ for $R \in \mathscr{L}$, and that all these poles are distinct. It remains to be shown that no pole of $\lambda_i^* \circ (v_1)$ can be a pole of $\lambda_i^* \circ (v_2)$ if $v_1 \neq v_2$. Suppose we had R_1, R_2, τ_1, and τ_2 such that $v_1^{-1}(R_1 - Q_i^{\tau_1}) = v_2^{-1}(R_2 - Q_i^{\tau_2})$. First, we see immediately that R_1 and R_2 must be points of α-division for the same α. But then, letting α act on both sides, we obtain

$$v_1^{-1}(-Q_i^{\tau_1}) = v_2^{-1}(-Q_i^{\tau_2}),$$

which is impossible if $v_1 \neq v_2$ since the two points would be in different congruence classes mod W.

We have now proved that all the poles of $\sum_{v \in W} \omega^i(v)\, \lambda_i^* \circ (v)$ come from

$v^{-1}P_R$ for all $v \in W$ and $R \in \mathscr{L}$. Applying the methods in the proof of Lemma 1 to these points, we easily compute that the residues all have the form $v\mu(\alpha)$ for some $v \in W$, and as before, that this is never congruent to $0 \bmod \not{p}$: similarly, we see again that reduction mod $\not{p}$ is injective on the entire set of poles. This suffices to prove that the rational function associated with $\sum_{v \in W} \omega^i(v)\, \lambda_i^* \circ (v)$ does not reduce to zero mod $\not{p}$.

Now, for $1 \leqslant i \leqslant p-2$, up to units in the Iwasawa algebra, $L_{\not{p},i}(s)$ is given by the $(i-1)$th gamma-transform of λ_i (see [1] for details), and $L_{\not{p},0}(s)$ is itself given by a unit in the Iwasawa algebra. Thus, applying the result of Theorem I in Section 2 permits us to conclude that the μ-invariants of the $L_{\not{p},i}(s)$ are zero for $0 \leqslant i \leqslant p-2$. This concludes the proof of Theorem IV.

References

1. D. Bernardi, C. Goldstein, and N. Stephens, Notes p-adiques sur les courbes elliptiques, *J. Reine Angew. Math.* **351** (1984), 129–170.
2. J. Coates and C. Goldstein, Some remarks on the main conjecture for elliptic curves with complex multiplication, *Amer. J. Math.* **103** (1983), 411–435.
3. J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977), 223–251.
4. J. Coates and A. Wiles, On p-adic L-functions and elliptic units, *J. Austral. Math. Soc. Ser. A* **26** (1978), 1–25.
5. R. Gillard, Transformation de Mellin–Leopoldt des fonctions elliptiques, Publication of the University of Geneva, to appear.
6. C. Goldstein and N. Schappacher, Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe, *J. Reine Angew. Math.* **327** (1981), 184–218.
7. R. Greenberg, On the structure of certain Galois groups, *Invent. Math.* **47** (1978), 85–99.
8. J. Lubin, One parameter formal Lie groups over p-adic integer rings, *Ann. of Math.* **80** (1964), 464–484.
9. W. Sinnott, On the μ-invariant of a rational function, *Invent. Math.* **75** (1984), 273–283.
10. R. Gillard, Unités elliptiques et fonctions L p-adiques, *Compositio Fascicule* **1** (1980), 57–88.