Compositio Mathematica **113:** 123–153, 1998.

Iwasawa theory for elliptic curves at unstable primes

DANIEL DELBOURGO*
University of Cambridge, Department of Pure Mathematics and Mathematical Statistics, 16 Mill Lane, Cambridge CB2 1SB, England

Received 25 November 1996; accepted in final form 22 April 1997

Abstract. In this paper we examine the Iwasawa theory of modular elliptic curves E defined over $\mathbb{Q}$ without semi-stable reduction at p. By constructing p-adic L-functions at primes of additive reduction, we formulate a 'Main Conjecture' linking this L-function with a certain Selmer group for E over the $\mathbb{Z}_p$-extension. Thus the leading term is expressible in terms of III_E, $E(\mathbb{Q})_{\mathrm{tors}}$ and a p-adic regulator term.

Mathematics Subject Classifications (1991): 11F67, 11F33, 11R23.

Key words: p-adic L-functions, Iwasawa theory, modular forms, elliptic curves.

Let E be a modular elliptic curve defined over $\mathbb{Q}$, and assume p denotes an odd rational prime. If $\mathbb{Q}(\mu_{p^\infty})$ denotes the field obtained by adjoining all p-power roots of unity to $\mathbb{Q}$, then $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \Gamma \times \Delta$ where $\Gamma \cong \mathbb{Z}_p$ and $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Write $\mathfrak{S}(E/\mathbb{Q}_\infty)$ for the Selmer group of E over $\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})^\Delta$, and let $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$ be the Iwasawa algebra of Γ.

The Iwasawa theory of E over $\mathbb{Q}_\infty$ is best understood when E has semi-stable ordinary reduction at p. On the analytic side, p-adic L-functions were constructed by Mazur and Swinnerton–Dyer [MSD] in the case of good ordinary reduction, and the method was further extended to include primes of (bad) multiplicative reduction in the paper of Mazur, Tate and Teitelbaum [MTT]. These L-functions are identified via a 'Main Conjecture' with the characteristic power series of the Pontrjagin dual $\mathfrak{S}(E/\mathbb{Q}_\infty)^\wedge$. It is conjectured that $\mathfrak{S}(E/\mathbb{Q}_\infty)^\wedge$ is Λ-torsion in the ordinary case, but this assertion has only been proved when E either has CM or trivial analytic rank.

A natural question to ask is what happens if p is an unstable prime for E. In this paper we construct a p-adic L-function for E under the assumption that E has bad additive reduction at p but possesses semi-stable reduction over a cyclotomic extension of $\mathbb{Q}_p$. If we view these L-functions as distributions on $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$, then they are bounded measures if p is potentially ordinary and 1-admissible measures if p is potentially supersingular.

When E has potential ordinary reduction at p, we formulate a Main Conjecture linking the characteristic power series of $\mathfrak{S}(E/\mathbb{Q}_\infty)^\wedge$ to our p-adic L-series. Fur-

* Supported by a C.C.T. scholarship; part of this author's PhD dissertation.

thermore if E has analytic rank zero, then we can prove that $\mathfrak{S}(E/\mathbb{Q}_\infty)^\wedge$ is indeed Λ-torsion and thus calculate the leading term of its characteristic power series.

Jones [Jon] has considered Iwasawa L-functions at additive primes in terms of the flat cohomology of the Néron model of elliptic curves defined over a general number field K. In our case $K = \mathbb{Q}$, the behaviour of the analytic p-adic L-function is in perfect agreement with his results. Once one makes a canonical choice of ℓ_p-invariant in the Main Conjecture, this conjecture implies the p-part of the Birch and Swinnerton–Dyer conjecture for the Hasse–Weil L-series of E at unstable primes.

1. The analytic side

In the first part of this paper we attach a p-adic L-function to modular elliptic curves with bad additive reduction at p. The method generalizes the construction in [MTT] to elliptic curves which have semi-stable reduction over a subfield of $\mathbb{Q}_p^{ab}$, the maximal abelian extension of $\mathbb{Q}_p$. This gives us a nice criterion for determining which elliptic curves satisfy the conditions of our construction. Examples of such curves are presented at the end.

1.1. Modular forms

We begin by recalling some standard definitions from the theory of modular forms. If

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}),$$

then the left action

$$\gamma z := \frac{az+b}{cz+d} \quad \text{for } z \in \mathfrak{H}, \qquad \gamma\infty := \frac{a}{c},$$

defines an automorphism of $\mathfrak{H} \cup \mathbb{R} \cup \{\infty\}$. For any $M \in \mathbb{N}$ define the congruence modular groups $\Gamma_0(M)$, $\Gamma_1(M)$ by

$$\Gamma_0(M) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0(M) \right\}.$$

and

$$\Gamma_1(M) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0(M), a \equiv d \equiv 1(M) \right\}.$$

Fix an integer $k \geqslant 2$. Let us denote by $\mathcal{S}_k(M)$ the space of holomorphic cusp forms of weight k on $\Gamma_1(M)$ with the standard action of $\mathrm{GL}_2(\mathbb{R})$, i.e.

$$F|\gamma := \left(\frac{\det\gamma^{1/2}}{cz+d}\right)^k F(\gamma z) \quad \text{for all } F \in \mathcal{S}_k(M).$$

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

Define the subspace of cusp forms of weight k, level M and character ψ by

$$\mathcal{S}_k(M,\psi) := \left\{ F \in \mathcal{S}_k(M) \,\middle|\, F \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \psi(d)F \quad \text{for all} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(M) \right\}.$$

We will write C_ψ for the conductor of ψ considered as a Dirichlet character.

The space $\mathcal{S}_k(M,\psi)$ is stable under the Hecke operators T_l, defined for *every* prime number l by

$$F|T_l := l^{(k/2)-1} \left(\sum_{u=0}^{l-1} F \middle| \begin{pmatrix} 1 & u \\ 0 & l \end{pmatrix} + \psi(l) F \middle| \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix} \right).$$

In particular, if $l \nmid M$ we have our usual Hecke operator at l; if $l|M$ we have the formula for U_l. Here ψ is identified with a Dirichlet character modulo M.

Decompose $M = QQ'$ into relatively prime factors Q and Q'. Then we may write $\psi = \psi_Q \psi_{Q'}$ where ψ_Q (resp. $\psi_{Q'}$) is a character modulo Q (resp. Q').

DEFINITION. We define the operator $w_Q\colon \mathcal{S}_k(M,\psi) \to \mathcal{S}_k(M, \overline{\psi_Q}\psi_{Q'})$ by

$$w_Q(F) := \psi_Q(y)\psi_{Q'}(x) F \middle| \begin{pmatrix} Qx & y \\ Mz & Qt \end{pmatrix},$$

where $x, y, z, t \in \mathbb{Z}$ are chosen such that $Qxt - Q'yz = 1$.

It is easy to verify that

$$w_Q^2(F) = (-1)^k \overline{\psi_{Q'}}(-Q) F$$

and

$$w_Q(F|T_l) = \psi_Q(l) w_Q(F)|T_l, \quad l \nmid M,$$

(see Atkin and Li [AtL]).

Finally if $F(z) = \Sigma_{n\geqslant 1} A_n q^n$ with $q = e^{2\pi i z}$, then the L-series of F is defined as the Mellin transform

$$L(F,s) := \sum_{n\geqslant 1} A_n n^{-s} = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty F(it) t^s \frac{\mathrm{d}t}{t}.$$

If F is a newform (i.e. a normalized simultaneous eigenform for the Hecke algebra), then the completed L-function $\Lambda(F,s)$ satisfies a functional equation and has analytic continuation to the whole s-plane. If ε is any Dirichlet character, then define the twist of F by ε as

$$F_\varepsilon := \sum_{n\geqslant 1} A_n \varepsilon(n) q^n.$$

Even though F_ε may not be a newform, there is always a newform $\widetilde{F} = \Sigma_{n\geqslant 1}\widetilde{A_n}q^n$ equivalent to F_ε, so that $\widetilde{A_n} = A_n\varepsilon(n)$ for all n prime to MC_ε.

1.2. ELLIPTIC CURVES WITH ADDITIVE REDUCTION

Let E be a modular elliptic curve defined over $\mathbb{Q}$ of conductor N, so there exists a non-constant $\mathbb{Q}$-rational map

$$\phi\colon X_0(N) \to E(\mathbb{C})$$

$$\infty \mapsto O.$$

Let $f = \Sigma_{n\geqslant 1}a_nq^n \in \mathcal{S}_2(N, \mathbf{1})$ be the (normalised) newform associated to the pull-back $\phi^*\omega_E$, where ω_E is the Néron differential associated to a minimal Weierstrass equation for E over $\mathbb{Z}$, with **1** denoting the trivial character.

Writing $G_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have a compatible system of l-adic representations $\Pi = \{\pi_l\}$,

$$\pi_l\colon G_\mathbb{Q} \to \mathrm{Aut}(T_lE \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}_l}), \quad \text{l prime},$$

coming from the action of $G_\mathbb{Q}$ on the Tate modules T_lE of E.

Let p be an *odd* prime number. If E has good reduction at p, p-adic L-functions were first defined by Mazur and Swinnerton–Dyer [MSD] and the construction was generalised to newforms of higher weight in the work of Manin [Man] and Vishik [Vis]. Mazur, Tate and Teitelbaum [MTT] further extended the method to allow primes of (bad) multiplicative reduction. (See [MTT] for a good overview.)

Roughly speaking, their construction uses congruences in p-adic distributions attached via the modular symbols of f. The key step in the proof lies in the fact that the Hasse–Weil L-series $L(E, s) = \Sigma_{n\geqslant 1}a_nn^{-s}$ of E has a non-trivial Euler factor at p. If $D_p \supset I_p$ denote a decomposition group for $G_\mathbb{Q}$ at p and its inertia subgroup, then this is equivalent to the l-adic realisation $H^1_l(E) = \mathrm{Hom}(T_lE \otimes_{\mathbb{Z}_l} \mathbb{Q}_l, \mathbb{Q}_l)$ possessing a non-trivial I_p-invariant subspace ($l \neq 2, p$).

Unfortunately this method breaks down if we have (bad) additive reduction at p, since the Euler factor is 1. To overcome this problem we consider the Hasse–Weil L-series of E as the L-function of our compatible system of l-adic representations $\Pi = \{\pi_l\}$. As we shall see, if I_p factors through $\mathrm{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p)$ then there is a twisted representation '$\Pi \otimes \varepsilon^{-1}$' whose L-function is the Mellin transform of a newform $\widetilde{f}$. Furthermore $L(\widetilde{f}, s)$ has a non-trivial Euler factor at p. Interpolating twists of $L(\widetilde{f}, 1)$ instead, the admissibility of our p-adic L-function depends solely on the Hecke polynomial of $\widetilde{f}$ at p.

1.3. POTENTIAL GOOD REDUCTION

Assume now that E has potential good reduction at p, so there exists a finite extension $L/\mathbb{Q}_p$ such that T_lE is unramified as a $\mathrm{Gal}(\overline{\mathbb{Q}_p}/L)$-representation ($l \neq$

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

$2, p$). Precise information is known about the action of I_p on $T_l E$ irrespective of whether E is modular or not.

For each integer $m \geqslant 3$ with $(m, p) = 1$, let Φ_p denote the inertial subgroup of $\mathbb{Q}_p(E_m)/\mathbb{Q}_p$, where $\mathbb{Q}_p(E_m)$ denotes the extension of $\mathbb{Q}_p$ obtained by adjoining the coordinates of the group of m-torsion points E_m on E. Then the action of I_p factors through Φ_p and this definition is independent of m (see [SeT]). In fact Φ_p is one of

$$1, \mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Z}/4, \mathbb{Z}/6,$$

or also $\mathbb{Z}/4 \ltimes \mathbb{Z}/3$ if $p = 3$. In fact, we shall only be interested in the case in which Φ_p is cyclic.

Let us consider the twisted representations $\Pi \otimes \varepsilon^{-1} = \{\pi_l \otimes \varepsilon^{-1}\}$ where ε is a Dirichlet character of p-power conductor. By a theorem of Carayol [Car] the representations

$$\pi_l \otimes \varepsilon^{-1}\colon G_{\mathbb{Q}} \to \mathrm{Aut}(T_l E \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}_l}),$$

correspond to a cusp form $\tilde{f} \in \mathcal{S}_2(\tilde{N}, \varepsilon^{-2})$, such that $\tilde{f}$ is the newform equivalent to $f_{\varepsilon^{-1}}$. Furthermore the level $\tilde{N}$ of $\tilde{f}$ is equal to $\mathrm{cond}(\Pi \otimes \varepsilon^{-1})$, the conductor of the l-adic system $\{\pi_l \otimes \varepsilon^{-1}\}$. Since ε is a character of p-power conductor, N and $\tilde{N}$ can only differ in the power of p dividing them. We shall write N_p for the p-part of N.

LEMMA. *Let $d = \#\Phi_p$. Assume that $p > 2$, $p \nmid d$ and Φ_p is cyclic. Then the following conditions are equivalent:*

(i) *The action of I_p on $T_l E$ factors through* $\mathrm{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p)$ *for all primes $l \neq 2, p$;*
(ii) *$\mathbb{Q}_p(E_l)/\mathbb{Q}_p$ is abelian for all primes $l \neq 2, p$;*
(iii) *There exists a character ε of p-power conductor such that if $\tilde{f} \in \mathcal{S}_2(\tilde{N}, \varepsilon^{-2})$ is the newform obtained from $\Pi \otimes \varepsilon^{-1}$, then $\tilde{N}_p = C_{\varepsilon^2}$;*
(iv) $p \equiv 1(d)$.

Proof. Since $\mathbb{Q}_p(E_{l^\infty})/\mathbb{Q}_p(E_l)$ is unramified, we note that $\mathbb{Q}_p(E_l)/\mathbb{Q}_p$ is abelian if and only if $\mathbb{Q}_p(E_{l^\infty})/\mathbb{Q}_p$ is abelian.

By the preceding remark, clearly (i) implies (ii). On the other hand, if $\mathbb{Q}_p(E_l)/\mathbb{Q}_p$ is abelian then the action of I_p factors through the inertia subgroup of $\mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)$, and so factors through the group $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$. But $p \nmid d$ and hence we know that $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p(\mu_p))$ acts trivially on $T_l E$. Hence conditions (i) and (ii) are equivalent.

We now show that (ii) implies (iii). Let us identify Φ_p with the inertial subgroup of $\mathbb{Q}_p^{nr}(E_l)$, and assume that $\Phi_p = \langle\tau\rangle$. If σ denotes any lift of the Frobenius element, then $\mathrm{Gal}(\mathbb{Q}_p^{nr}(E_l))$ is topologically generated by τ and σ.

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

By local class field theory, $L = \mathbb{Q}_p^{nr}(E_l)^{\sigma=1}$ corresponds to a character λ of $\mathbb{Z}_p^\times$ of finite order. Since $\pi_l|_{D_p}$ factors through $\mathrm{Gal}(\mathbb{Q}_p^{nr}(E_l)/\mathbb{Q}_p)$, and as π_l is injective on Φ_p and diagonalizes, we may assume

$$\pi_l(\tau) = \begin{pmatrix} \lambda(\tau) & \\ & \lambda(\tau)^{-1} \end{pmatrix}.$$

Hence $\pi_l \otimes \varepsilon$ and $\pi_l \otimes \varepsilon^{-1}$ are twists of minimal p-conductor (equal if $d = 1$ or 2), where ε is locally λ at p. Thus $\mathrm{cond}(\Pi \otimes \varepsilon^{\pm 1}) = C_{\varepsilon^2}$.

Conversely we can deduce (ii) from (iii). Because $\widetilde{N}_p = C_{\varepsilon^2}$, $H_l^1(E) \otimes \varepsilon^{\pm 1}$ possesses a non-trivial I_p-invariant subspace. By the Weil pairing there exist basis vectors $x, y \in T_l E \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}_l}$ such that $\tau(x) = \varepsilon(\tau)x$ and $\tau(y) = \overline{\varepsilon}(\tau)y$. Hence the totally ramified cyclic extension $L/\mathbb{Q}_p$ defined by ε is contained in $\mathbb{Q}_p(E_{l^\infty})$. As $\mathbb{Q}_p(E_{l^\infty})/L$ is unramified, $\mathbb{Q}_p(E_l)/\mathbb{Q}_p$ is abelian.

To see the equivalence of (ii) and (iv) first observe that all the field extensions we consider are tamely ramified since $p \nmid d$. Now if $\mathbb{Q}_p(E_l)/\mathbb{Q}_p$ is abelian then $\mathbb{Q}_p^{nr}(E_{l^\infty}) \subset \mathbb{Q}_p^{ab}$, so the ramification degree $d|(p-1)p^n$ for some $n \in \mathbb{N}_0$. But $p \nmid d$ so we must have $d|p-1$.

On the other hand there exists a unique tamely ramified extension $H/\mathbb{Q}_p^{nr}$ of degree d. If $d|p-1$ then $H = \mathbb{Q}_p^{nr}(E_{l^\infty}) \subset \mathbb{Q}_p^{nr}(\mu_p) \subset \mathbb{Q}_p^{ab}$ as required. The proof is complete.

It is straightforward to determine whether a particular E satisfies the conditions of this lemma. If E has j-invariant j_E and discriminant Δ_E, then E has potential good reduction if and only if $\mathrm{ord}_p j_E \geqslant 0$, whilst $d = \#\Phi_p$ can be read off from $\mathrm{ord}_p \Delta_E$ modulo 12 (see the paper of Serre [Ser] for a full description).

In fact one can show that if $d > 2$, $p \geqslant 5$ and $p \not\equiv 1(d)$, then E has potential supersingular reduction at p.

1.4. Measures Attached to Newforms

In this section we will briefly recall the method used to attach a p-adic distribution to a newform of weight 2. For the case of general weight $k \geqslant 2$ the reader should consult [MTT].

Let $J > 0$ be a fixed integer prime to p. Set

$$\mathbb{Z}_{p,J} := \varprojlim (\mathbb{Z}/p^n J\mathbb{Z}) = \mathbb{Z}_p \times (\mathbb{Z}/J\mathbb{Z})$$

and

$$\mathbb{Z}_{p,J}^\times := \varprojlim (\mathbb{Z}/p^n J\mathbb{Z})^\times = \mathbb{Z}_p^\times \times (\mathbb{Z}/J\mathbb{Z})^\times.$$

The p-adic analytic Lie group $\mathbb{Z}_{p,J}^\times$ is covered by open disks of the form

$$D(a, n) := a + p^n J\mathbb{Z}_{p,J} \subset \mathbb{Z}_{p,J}^\times,$$

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

where $n \in \mathbb{N}$ and $(a, pJ) = 1$. We embed once and for all $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$, with $\mathbb{C}_p$ denoting the Tate field.

Fix a newform $F \in \mathcal{S}_2(M, \psi)$ with the q-expansion $F = \sum_{n \geqslant 1} A_n q^n$. We factorize the (inverse) Hecke polynomial of F at p as

$$X^2 - A_p X + \psi(p)p = (X - \alpha_p)(X - \beta_p),$$

where we assume that $\mathrm{ord}_p \alpha_p \leqslant \mathrm{ord}_p \beta_p$ with at least α_p non-zero. One may consider p-adic L-functions attached to F as the (p-adic) Mellin transforms of distributions on $\mathbb{Z}_{p,J}^\times$. These distributions are determined by their integrals against the elements of $\mathrm{Hom}(\mathbb{Z}_{p,J}^\times, \overline{\mathbb{Q}}^\times)^{\mathrm{tors}}$ which we view as Dirichlet characters.

Now suppose that χ is a primitive Dirichlet character of conductor $C_\chi \in p^{\mathbb{N}_0} J$. Let $\Omega^\pm$ denote complex periods for F, so that

$$\frac{L(F, \overline{\chi}, 1)}{\Omega^{\mathrm{sign}(\chi)}} \in \overline{\mathbb{Q}} \quad \text{for all such } \chi.$$

DEFINITION. Define the p-adic distribution $\mu(F, \alpha_p)$ by

$$\int_{\mathbb{Z}_{p,J}^\times} \chi \, \mathrm{d}\mu(F, \alpha_p) := \frac{p^m J}{\alpha_p^m G(\overline{\chi})} \left(1 - \frac{\overline{\chi}(p)\psi(p)}{\alpha_p}\right) \left(1 - \frac{\chi(p)}{\alpha_p}\right) \times \frac{L(F, \overline{\chi}, 1)}{\Omega^{\mathrm{sign}(\chi)}},$$

for all $\chi \in \mathrm{Hom}(\mathbb{Z}_{p,J}^\times, \overline{\mathbb{Q}}^\times)^{\mathrm{tors}}$, $C_\chi = p^m J$ and $m \in \mathbb{N}_0$, where we denote by $G(\overline{\chi}) := \Sigma_{n=1}^{C_\chi} \overline{\chi}(n) e^{2\pi i n / C_\chi}$ the Gauss sum of $\overline{\chi}$.

Here it is important to remember that ψ is a character *modulo* M.

The p-adic boundedness of the distribution $\mu(F, \alpha_p)$ can be characterised in terms of 'h-admissibility'. It is a result due to Vishik [Vis] that $\mu(F, \alpha_p)$ is a 1-*admissible measure*, i.e.

$$\left| \int_{D(a,n)} \mathrm{d}\mu(F, \alpha_p) \right|_p = o\left(|p^n|_p^{-1}\right) \quad \text{for all } n \in \mathbb{N} \quad \text{and} \quad (a, pJ) = 1,$$

under our embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. As a consequence $\mu(F, \alpha_p)$ is uniquely determined by the integrals $\int_{\mathbb{Z}_{p,J}^\times} \chi \, \mathrm{d}\mu(F, \alpha_p)$ for all $\chi \in \mathrm{Hom}(\mathbb{Z}_{p,J}^\times, \overline{\mathbb{Q}}^\times)^{\mathrm{tors}}$. Furthermore if $\mathrm{ord}_p \alpha_p = 0$ (thus if A_p is a p-adic unit), then $\mu(F, \alpha_p)$ is a *bounded measure*, i.e.

$$\left| \int_{D(a,n)} \mathrm{d}\mu(F, \alpha_p) \right|_p \leqslant \text{a fixed constant},$$

for all $n \in \mathbb{N}$ and $(a, pJ) = 1$. (See [Vis] for the full details.)

Now as p is an odd prime, we can decompose $x \in \mathbb{Z}_p^\times$ via

$$x = \omega(x)\langle x \rangle,$$

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

where $\omega(x)$ is the Teichmüller representative of x and $\langle x\rangle \in 1+p\mathbb{Z}_p$. If we define Q to be the largest positive divisor of M prime to pJ, then write $M = QQ'$ as in Section 1.1 and assume that $Q'|p^m J$ for large enough m. The distribution $\mu(F, \alpha_p)$ satisfies the functional equation

$$\begin{aligned}&\int_{\mathbb{Z}_{p,J}^\times} \chi x_p^j \langle x\rangle^s \,\mathrm{d}\mu(F,\alpha_p)\\ &\quad = (-1)^{j+1}\psi_Q(-J)\psi_{Q'}(Q)\overline{\chi}(-Q)Q^{-j}\langle Q\rangle^{-s}\\ &\qquad \times \int_{\mathbb{Z}_{p,J}^\times} \psi_{Q'}\chi^{-1}x_p^{-j}\langle x\rangle^{-s}\,\mathrm{d}\mu\left(w_Q(F), \overline{\psi}_Q(p)\alpha_p\right),\end{aligned}$$

where $C_\chi \in p^{\mathbb{N}_0}J$, $s \in \mathbb{Z}_p$, $j \in \mathbb{Z}$ and $x_p : \mathbb{Z}_{p,J}^\times \twoheadrightarrow \mathbb{Z}_p^\times$ corresponds to the pth-cyclotomic character (see [MTT]). The functional equation for the p-adic L-function attached to E will be deduced from this relation in the next section.

1.5. The p-adic L-function

We are ready to attach a p-adic L-function to E. However we are forced to make the following assumption about the reduction.

HYPOTHESIS (G). E has potential good reduction at p and E possesses good reduction over a field $L \subset \mathbb{Q}_p(\mu_p)$ where $[L\colon \mathbb{Q}_p] = d$.

By the lemma of Section 1.3, (G) is equivalent to the existence of a newform $\widetilde{f} = \sum_{n\geqslant 1} \widetilde{a_n} q^n \in \mathcal{S}_2(\widetilde{N}, \varepsilon^{-2})$ with $\widetilde{N}_p = C_{\varepsilon^2}$ and $f = \widetilde{f}_\varepsilon$. It is an easy exercise to show that $p|\widetilde{N}$ if and only if $d = 3, 4$ or 6. In all cases the Euler factor

$$1 - \widetilde{a_p}p^{-s} + \overline{\varepsilon}^2(p)p^{1-2s},$$

of $L(\widetilde{f}, s)$ at p is non-trivial; this is exactly what we need.

Let α_p now denote a nonzero root of the polynomial

$$X^2 - \widetilde{a_p}X + \overline{\varepsilon}^2(p)p.$$

Without loss of generality we may assume that $\mathrm{ord}_p\alpha_p \leqslant \frac{1}{2}$ (if not twist $\Pi = \{\pi_l\}$ by ε instead of ε^{-1} since we know that $\alpha_p\overline{\alpha_p} = p$).

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

DEFINITION. We define the p-adic multiplier $\mathfrak{L}_p^{(G)}(X)$ by

$$\mathfrak{L}_p^{(G)}(X) := \begin{cases} \left(1-\frac{\overline{X}}{\alpha_p}\right)\left(1-\frac{X}{\alpha_p}\right) & \text{if } d=1,\\ \dfrac{\left(1-\frac{\overline{X}}{\alpha_p}\right)\left(1-\frac{X}{\alpha_p}\right)}{\left(1-\frac{\alpha_p\overline{X}}{p}\right)\left(1-\frac{\overline{\alpha_p X}}{p}\right)} & \text{if } d=2,\\ \dfrac{\left(1-\frac{X}{\alpha_p}\right)}{\left(1-\frac{\alpha_p\overline{X}}{p}\right)} & \text{if } d=3,4 \text{ or } 6. \end{cases}$$

(In fact if $d=2$ we clearly have

$$\frac{\left(1-\frac{\overline{X}}{\alpha_p}\right)\left(1-\frac{X}{\alpha_p}\right)}{\left(1-\frac{\alpha_p\overline{X}}{p}\right)\left(1-\frac{\overline{\alpha_p X}}{p}\right)} = \frac{\left(1-\frac{X}{\alpha_p}\right)}{\left(1-\frac{\alpha_p\overline{X}}{p}\right)},$$

but it actually makes more sense to write $\mathfrak{L}_p^{(G)}(X)$ without this cancellation.)

At first glance the definition of $\mathfrak{L}_p^{(G)}(X)$ seems rather arbitrary. The best justification for this strange multiplier is that it makes everything work!

THEOREM 1. *Assume E satisfies (G). Then there exists a unique 1-admissible measure μ_E such that*

$$\int_{\mathbb{Z}_{p,J}^{\times}} \chi\, \mathrm{d}\mu_E = \mathbf{L}_p(E,\chi) := \frac{p^m J}{\alpha_p^m G(\overline{\chi_\varepsilon})G(\overline{\varepsilon})}\mathfrak{L}_p^{(G)}(\chi_\varepsilon(p)) \times \frac{L(E,\chi^{-1},1)}{\Omega_E^{\mathrm{sign}(\chi)}},$$

where χ_ε is the primitive character associated to $\chi\varepsilon^{-1}$, $p^m J = C_{\chi_\varepsilon}$ and Ω_E^+ (resp. Ω_E^-) denotes the real (resp. imaginary) period of E.

Furthermore, if E has potential good ordinary reduction at p, μ_E is a bounded measure.

We remark that if $d=1$ (i.e. good reduction over $\mathbb{Q}_p$), then $\varepsilon = \mathbf{1}$, $\chi_\varepsilon = \chi$ and we retrieve the L-function of Mazur and Swinnerton–Dyer [MSD]. If $d>1$ then the denominator in $\mathfrak{L}_p^{(G)}(\chi_\varepsilon(p))$ puts back the 'missing Euler factor' that is lost by interpolating $L(E,\chi^{-1},1)$ instead of $L(\tilde{f}_{\overline{\chi_\varepsilon}},1)$.

The Functional Equation. Decomposing $\tilde{N} = QQ'$ with Q the largest positive divisor of $\tilde{N}$ prime to pJ, we have the p-adic functional relation

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

$$\int_{\mathbb{Z}_{p,J}^{\times}} \chi x_p^j \langle x\rangle^s \,\mathrm{d}\mu_E$$
$$= (-1)^{j+1}\overline{\varepsilon}(-Q)\widetilde{c_Q}\overline{\chi}(-Q)Q^{-j}\langle Q\rangle^{-s} \times \int_{\mathbb{Z}_{p,J}^{\times}} \chi^{-1}x_p^{-j}\langle x\rangle^{-s}\,\mathrm{d}\mu_E,$$

where $C_{\chi_\varepsilon} = p^m J$, $s \in \mathbb{Z}_p$, $j \in \mathbb{Z}$, and $w_Q(\widetilde{f}) = \widetilde{c_Q}\widetilde{f}$ with $\overline{\varepsilon}(-Q)\widetilde{c_Q} \in \{\pm 1\}$.

Proof. Consider the distribution $\mu(F, \alpha_p)$ of the previous section with $F = \widetilde{f}$, $\psi = \varepsilon^{-2}$ and $M = \widetilde{N}$. Defining μ_E to be the twist of $\mu(\widetilde{f}, \alpha_p)$ by ε^{-1}, i.e.

$$\mu_E(x) := \varepsilon^{-1}(x)\mu(\widetilde{f}, \alpha_p)(x),$$

we see immediately that

$$\int_{\mathbb{Z}_{p,J}^{\times}} \chi \,\mathrm{d}\mu_E = \int_{\mathbb{Z}_{p,J}^{\times}} \chi_\varepsilon \,\mathrm{d}\mu(\widetilde{f}, \alpha_p)$$
$$= \frac{p^m J}{\alpha_p^m G(\overline{\chi_\varepsilon})}\left(1 - \frac{\overline{\chi_\varepsilon}(p)\varepsilon^{-2}(p)}{\alpha_p}\right)\left(1 - \frac{\chi_\varepsilon(p)}{\alpha_p}\right) \times \frac{L(\widetilde{f}, \overline{\chi_\varepsilon}, 1)}{\Omega^{\mathrm{sign}(\chi_\varepsilon)}}$$

where $\Omega^{\pm} := G(\overline{\varepsilon})\Omega_E^{\pm \mathrm{sign}(\varepsilon)}$. But if $d > 1$ then

$$L(\widetilde{f}, \overline{\chi_\varepsilon}, 1) = \frac{L(f, \overline{\chi}, 1)}{(1 - \overline{\chi_\varepsilon}(p)\widetilde{a_p}p^{-1} + \overline{\chi_\varepsilon}^2(p)\varepsilon^{-2}(p)p^{-1})},$$

which explains the denominator term of $\mathfrak{L}_p^{(G)}(\chi_\varepsilon(p))$, and

$$\varepsilon^{-2}(p) = \begin{cases} 1 & \text{if } d = 1 \text{ or } 2, \\ 0 & \text{if } d = 3, 4 \text{ or } 6, \end{cases}$$

which explains the numerator term. The functional equation for μ_E is then a direct consequence of the functional equation

$$\int_{\mathbb{Z}_{p,J}^{\times}} \chi_\varepsilon x_p^j \langle x\rangle^s \,\mathrm{d}\mu(\widetilde{f}, \alpha_p)$$
$$= (-1)^{j+1}\varepsilon^{-2}(Q)\overline{\chi_\varepsilon}(-Q)Q^{-j}\langle Q\rangle^{-s}$$
$$\times \int_{\mathbb{Z}_{p,J}^{\times}} \varepsilon^{-2}(\chi_\varepsilon)^{-1}x_p^{-j}\langle x\rangle^{-s}\,\mathrm{d}\mu(w_Q(\widetilde{f}), \alpha_p)$$

and the fact that $w_Q(\widetilde{f}) = \widetilde{c_Q}\widetilde{f}$ for some $\widetilde{c_Q} \neq 0$, since $w_Q(\widetilde{f})|T_l = \widetilde{a_l}w_Q(\widetilde{f})$ for all l prime to $\widetilde{N}$. (In fact $w_Q^2(\widetilde{f}) = \widetilde{c_Q}^2\widetilde{f} = \varepsilon^2(-Q)\widetilde{f}$.)

All that remains to be proven is that if E has potential good ordinary reduction at p then $\mathrm{ord}_p\alpha_p = 0$. As L is totally ramified over $\mathbb{Q}_p$ its residue field is $\mathbb{F}_p$. Write $\mathfrak{F}$ for the reduction of E over L. If I_L denotes the inertial subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/L)$, we know that

$$\begin{aligned}\#\mathfrak{F}(\mathbb{F}_p) &= 1 - \mathrm{Tr}\,\widetilde{\sigma} + p \\ &= \det(1 - \sigma^{-1}|H^1_l(E)^{I_L}) \\ &= (1-\alpha_p)(1-\overline{\alpha_p}),\end{aligned}$$

where $\widetilde{\sigma}\colon x \mapsto x^p$ is the Frobenius automorphism on $\mathbb{F}_p$ and σ a lift to D_p.

But E has good ordinary reduction over L so the dual isogeny $\widehat{\widetilde{\sigma}}$ of $\widetilde{\sigma}$ cannot be inseparable. Since $[\mathrm{Tr}\,\widetilde{\sigma}] = \widetilde{\sigma} + \widehat{\widetilde{\sigma}}$ as an endomorphism of $\mathfrak{F}$, consequently $p \nmid \mathrm{Tr}\,\widetilde{\sigma}$. Hence $\mathrm{Tr}\,\widetilde{\sigma}$ is a p-adic unit and so α_p must be too. By Vishik's criteria [Vis], $\mu_E = \varepsilon^{-1}\mu(\widetilde{f}, \alpha_p)$ is bounded.

1.6. POTENTIAL MULTIPLICATIVE REDUCTION

We can apply the same ideas to all modular elliptic curves with potential multiplicative reduction at p. Assume now that $\mathrm{ord}_p j_E < 0$ so that E becomes isomorphic over a quadratic extension of $\mathbb{Q}_p$ to the Tate curve $E_q = \mathbb{G}_m/q_E^{\mathbb{Z}}$, where $q_E \in p\mathbb{Z}_p$ is given by the expansion

$$q_E = j_E^{-1} + 744 j_E^{-2} + 750420 j_E^{-3} + \cdots.$$

HYPOTHESIS (M). E has potential multiplicative reduction at p, and hence E possesses (bad) multiplicative reduction over a field $L \subset \mathbb{Q}_p(\mu_p)$ where $[L\colon \mathbb{Q}_p] =$ 1 or 2.

Denote by ε the non-trivial quadratic character of conductor p (resp. the trivial character $\mathbf{1}$) if $[L\colon \mathbb{Q}_p] = 2$ (resp. if $L = \mathbb{Q}_p$), so that $\mathrm{cond}(\Pi \otimes \varepsilon) = p$.

It is straightforward to deduce that (M) implies the existence of a newform $\widetilde{f} = \sum_{n\geqslant 1}\widetilde{a_n}q^n \in \mathcal{S}_2(\widetilde{N}, \mathbf{1})$ with $p\|\widetilde{N}$ and $f = \widetilde{f}_\varepsilon$. Furthermore the Euler factor of $L(\widetilde{f}, s)$ at p is

$$1 - \widetilde{a_p}p^{-s}.$$

Putting $\alpha_p = \widetilde{a_p}$, we know that $\alpha_p \in \{\pm 1\}$ since $\widetilde{a_p}^2 = 1$.

DEFINITION. We define the p-adic multiplier $\mathfrak{L}_p^{(M)}(X)$ by

$$\mathfrak{L}_p^{(M)}(X) := \begin{cases} \left(1 - \frac{X}{\alpha_p}\right) & \text{if } L = \mathbb{Q}_p, \\ \dfrac{\left(1 - \frac{X}{\alpha_p}\right)}{\left(1 - \frac{\alpha_p X}{p}\right)} & \text{if } [L\colon \mathbb{Q}_p] = 2. \end{cases}$$

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

THEOREM 2. *Assume E satisfies (M). Then there exists a unique bounded measure μ_E such that*

$$\int_{\mathbb{Z}_{p,J}^{\times}} \chi\, \mathrm{d}\mu_E = \mathbf{L}_p(E,\chi)$$

$$:= \frac{p^m J}{\alpha_p^m G(\overline{\chi_\varepsilon}) G(\overline{\varepsilon})} \mathfrak{L}_p^{(M)}(\chi_\varepsilon(p)) \times \frac{L(E,\chi^{-1},1)}{\Omega_E^{\mathrm{sign}(\chi)}},$$

where χ_ε is the primitive character associated to $\chi\varepsilon^{-1}$, $p^m J = C_{\chi_\varepsilon}$ and $\Omega_E^{\pm}$ are the periods of E.

The proof of this result runs along identical lines to that of Theorem 1. We simply remark that since $\alpha_p \in \{\pm 1\}$, μ_E will be bounded. Moreover μ_E satisfies exactly the functional equation given in the last section. Needless to say, if $L = \mathbb{Q}_p$, $\varepsilon = \mathbf{1}$ then we retrieve the L-function attached at multiplicative primes in Mazur, Tate and Teitelbaum [MTT].

It is interesting to observe that the p-adic multiplier $\mathfrak{L}_p^{(M)}(\chi_\varepsilon(p))$ vanishes if $\chi_\varepsilon(p) = \alpha_p$. This phenomenon was first noted for elliptic curves with split multiplicative reduction [MTT], and has no analogue in the case of potential good reduction. One expects this vanishing to be related to the extended Mordell–Weil group $E^\dagger$.

Without digressing too much, we remark that for a global number field K, $E^\dagger(K)$ sits inside the exact sequence

$$0 \to \mathbb{Z}^R \to E^\dagger(K) \to E(K) \to 0,$$

where R denotes the number of places ν dividing p such that the Néron model of E is split multiplicative at ν. There is a well-defined bilinear symmetric height pairing

$$\langle\cdot,\cdot\rangle_K^\dagger : E^\dagger(K) \otimes \mathbb{Q}_p \times E^\dagger(K) \otimes \mathbb{Q}_p \to \mathbb{Q}_p,$$

connected with Schneider's norm-adapted height [Sch], and it would be a useful exercise to follow the procedure in [MTT] and compute p-adic regulator data for some numerical examples of curves satisfying (M). However we do not pursue the idea any further here.

Greenberg [Gr2] has an alternative description of this vanishing for arbitrary *ordinary* representations. In our case we deduce that the p-adic L-function has a trivial zero if and only if the Frobenius element acting on the p-adic representation $V_pE \otimes \varepsilon$ has eigenvalues 1 or p. From the non-split exact sequence

$$0 \to \mathbb{Q}_p(1) \to V_pE_q \to \mathbb{Q}_p \to 0,$$

we see that this vanishing occurs if and only if $V_pE_q \cong V_pE \otimes \varepsilon$ as $G_{\mathbb{Q}_p}$-modules.

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

If E has additive reduction at $p \geqslant 5$ and $V_pE_q \cong V_pE \otimes \varepsilon$, then it is a simple consequence of the Greenberg–Stevens formula [GrS] that

$$\frac{\mathrm{d}}{\mathrm{d}s}\mathbf{L}_p(E, \varepsilon(x)\langle x\rangle^s)\Big|_{s=0} = \frac{\log_p q_E}{\mathrm{ord}_p q_E}\frac{p}{G(\varepsilon)(p-1)}\frac{L(E,\varepsilon)}{\Omega_E^{\mathrm{sign}(\varepsilon)}}.$$

Simply apply their formula to compute the derivative of the p-adic L-function attached to the Tate curve $E^{(\varepsilon)}$ which is the quadratic twist of E by ε.

1.7. Some numerical examples

Before we examine the algebraic part of the problem let us consider some modular elliptic curves defined over $\mathbb{Q}$ which satisfy the conditions of our construction. The examples all have analytic rank zero, and no complex multiplication.

EXAMPLE A. Consider the elliptic curve E_A defined by the minimal Weierstrass equation

$$E_A\colon y^2 + y = x^3 - 3x - 5.$$

It has conductor $99 = 3^2.11$ and potential good ordinary reduction at 3. Furthermore, $\#\Phi_3 = 2$ so $\varepsilon(\cdot) = \left(\frac{\cdot}{3}\right)$.

If f_A (resp. $\widetilde{f_A}$) denotes the newform obtained from E_A (resp. $\Pi \otimes \varepsilon^{-1}$), then

$$f_A = (\widetilde{f_A})_\varepsilon.$$

In fact $\widetilde{f_A}$ is the newform obtained from an elliptic curve $E_A^{(\varepsilon)}$ of conductor 11. As we shall see later, our twisted 3-adic L-function $L_3(E_A, (\frac{\cdot}{3}))$ evaluated at ε contains information about the arithmetic of $E_A^{(\varepsilon)}$ as well.

EXAMPLE B. Consider now the elliptic curve E_B defined by

$$E_B\colon y^2 + y = x^3 - x^2 - 2x - 1.$$

Its conductor is $147 = 3.7^2$ and it has bad additive reduction at 7. Since $\mathrm{ord}_7 j_{E_B} \geqslant 0$ and $\mathrm{ord}_7\Delta_{E_B} \equiv 2$ modulo 12, we see that E_B has potential good reduction and the size of inertia $\#\Phi_7 = 6$. But as $6|7-1$, E_B satisfies (G) and we may again apply our construction.

EXAMPLE C. Lastly consider the elliptic curve E_C defined by the equation

$$E_C\colon y^2 + xy = x^3 - x^2 + 9x.$$

It has conductor $63 = 3^2.7$ and thus bad additive reduction at 3. This time $\mathrm{ord}_3 j_{E_C} < 0$ so E_C has potential (split) multiplicative reduction.

If f_C is the newform obtained from E_C, then

$$f_C = (\widetilde{f_C})_\varepsilon,$$

where $\varepsilon(\cdot) = (\frac{\cdot}{3})$, and $\widetilde{f_C}$ corresponds to an elliptic curve $E_C^{(\varepsilon)}$ of conductor 21 with bad multiplicative reduction. In fact $E_C^{(\varepsilon)}$ over $\mathbb{Q}_3$ is a Tate curve and the reduction is split.

2. The algebraic side

The rest of this paper concerns the relationship between our p-adic L-functions and the characteristic power series of $\mathfrak{X}_\infty$, the Pontrjagin dual of the Selmer group of E over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We formulate a 'Main Conjecture' for E at odd primes p satisfying hypotheses (G) or (M), and by examining the case where E has analytic rank zero in detail, we predict the ℓ_p-invariant that enters into the conjecture at additive primes. As we shall see, this constant depends only on the reduction of E at p.

2.1. Selmer groups

Let us first recall the definition of Selmer groups for E in terms of Galois cohomology. We do not yet make any hypothesis about the modularity of E, nor about the nature of its reduction at $p \neq 2$.

Let $\mathbb{Q}_\infty$ denote the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, so that $\mathbb{Q}_\infty := \bigcup_{n\geqslant 0} \mathbb{Q}_n$ where $[\mathbb{Q}_n : \mathbb{Q}] = p^n$. If $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ then $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \Gamma \times \Delta$ where $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Fix a topological generator γ of Γ.

Throughout Σ will denote any finite set of non-archimedean primes of $\mathbb{Q}$, which is always assumed to contain p and the primes of bad reduction of E. Let $\mathbb{Q}_\Sigma$ be the maximal extension of $\mathbb{Q}$ unramified outside Σ and infinity, and put $G_\Sigma := \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$.

By our choice of Σ, clearly $\mathbb{Q}(E_{p^\infty}) \subset \mathbb{Q}_\Sigma$ and so we can regard E_{p^∞} as a G_Σ-module. We also put $G_{\infty,\Sigma} := \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$ and write Σ_∞ for the set of primes of $\mathbb{Q}_\infty$ lying over Σ. If ν denotes any finite place of $\mathbb{Q}_\infty$, we define $\mathbb{Q}_{\infty,\nu}$ to be the union of the completions at ν of the finite extensions of $\mathbb{Q}$ contained in $\mathbb{Q}_\infty$.

DEFINITION. We define the Selmer group $\mathfrak{S}(E/\mathbb{Q})$ for E at p by the exactness of the sequence

$$0 \to \mathfrak{S}(E/\mathbb{Q}) \to H^1(G_\Sigma, E_{p^\infty}) \xrightarrow{\text{res}} \bigoplus_{q\in\Sigma} H^1(\mathbb{Q}_q, E)(p).$$

Similarly we define the Selmer group $\mathfrak{S}(E/\mathbb{Q}_\infty)$ for E over $\mathbb{Q}_\infty$ by the exactness of

$$0 \to \mathfrak{S}(E/\mathbb{Q}_\infty) \to H^1(G_{\infty,\Sigma}, E_{p^\infty}) \xrightarrow{\text{res}} \bigoplus_{\nu\in\Sigma_\infty} H^1(\mathbb{Q}_{\infty,\nu}, E)(p).$$

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

As an immediate consequence of these definitions, we obtain the classical exact sequence

$$0 \to \mathfrak{S}(E/\mathbb{Q}) \to H^1(\mathbb{Q}, E_{p^\infty}) \xrightarrow{\text{res}} \bigoplus_q H^1(\mathbb{Q}_q, E)(p),$$

and both $\mathfrak{S}(E/\mathbb{Q})$ and $\mathfrak{S}(E/\mathbb{Q}_\infty)$ are clearly independent of the choice of Σ.

If M is any Abelian group we write $M\widehat{\otimes}\mathbb{Z}_p = \varprojlim M/p^n M$ for the p-adic completion of M. If M is a discrete p-primary Γ-module, let $M^\wedge := \mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ be its Pontrjagin dual, endowed with its natural Γ-action. This Γ-action extends by linearity and continuity to an action of the whole Iwasawa algebra $\Lambda := \mathbb{Z}_p[\![\Gamma]\!]$ on $M^\wedge$.

Now Γ acts by conjugation on $H^1(G_{\infty,\Sigma}, E_{p^\infty})$ and this action leaves $\mathfrak{S}(E/\mathbb{Q}_\infty)$ stable. It is well known that $H^1(G_{\infty,\Sigma}, E_{p^\infty})^\wedge$ is a finitely generated Λ-module (for example, see Greenberg's paper [Gr1]). We define the analytic rank r_E of E by

$$r_E := \mathrm{order}_{s=1} L(E, s).$$

If r_E is equal to 0 or 1 and E is modular, then $H^1(G_{\infty,\Sigma}, E_{p^\infty})^\wedge$ has Λ-rank 1 and possesses no finite non-zero Λ-submodules (see [CMc]).

Our primary object of study will be the Λ-module

$$\mathfrak{X}_\infty := \mathfrak{S}(E/\mathbb{Q}_\infty)^\wedge.$$

If p is potentially supersingular for E (i.e. there exists a finite extension K of $\mathbb{Q}$ such that E/K has good supersingular reduction at all places above p), then it is conjectured that $\mathrm{rank}_\Lambda\, \mathfrak{X}_\infty = 1$, and this can be proven when $r_E \leqslant 1$. On the other hand, if p is potentially ordinary for E (i.e. there exists a finite extension K of $\mathbb{Q}$ such that E/K has either multiplicative or good ordinary reduction at all places above p), it is conjectured that $\mathrm{rank}_\Lambda\, \mathfrak{X}_\infty = 0$, i.e. $\mathfrak{X}_\infty$ is Λ-torsion. It was Mazur who first observed that this conjecture can be proven if the Selmer group of E over $\mathbb{Q}$ is finite.

For the rest of this paper we consider the case where E is a modular elliptic curve of analytic rank zero and satisfies the hypotheses (G) or (M). If E is potentially ordinary at p we shall prove that $\mathfrak{X}_\infty$ is indeed Λ-torsion, by applying the deep results of Kolyvagin, Gross–Zagier and others on the finiteness of the Tate–Shafarevic group. We shall also calculate the leading term of the characteristic power series of $\mathfrak{X}_\infty$ in this case.

2.2. TAMAGAWA FACTORS

Let us consider the restriction map $\beta\colon H^1(G_\Sigma, E_{p^\infty}) \to H^1(G_{\infty,\Sigma}, E_{p^\infty})^\Gamma$. As Γ has cohomological dimension 1, we have the inflation-restriction exact sequence

$$0 \to H^1(\Gamma, E_{p^\infty}(\mathbb{Q}_\infty)) \to H^1(G_\Sigma, E_{p^\infty}) \xrightarrow{\beta} H^1(G_{\infty,\Sigma}, E_{p^\infty})^\Gamma \to 0.$$

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

Furthermore we know that the order of the kernel of β is equal to $\#E_{p^\infty}(\mathbb{Q})$ (use the fact that $E_{p^\infty}(\mathbb{Q}_\infty)$ is finite [Ima], whence we have $\#H^1(\Gamma, E_{p^\infty}(\mathbb{Q}_\infty)) = \#E_{p^\infty}(\mathbb{Q}_\infty)^\Gamma$).

The restriction maps give us the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{S}(E/\mathbb{Q}_\infty)^\Gamma \arrow[r] & H^1(G_{\infty,\Sigma}, E_{p^\infty})^\Gamma \arrow[r, "\lambda_\infty"] & \bigoplus_{\nu\in\Sigma_\infty} H^1(\mathbb{Q}_{\infty,\nu}, E)(p))^\Gamma \\
0 \arrow[r] & \mathfrak{S}(E/\mathbb{Q}) \arrow[r] \arrow[u, "\alpha"] & H^1(G_\Sigma, E_{p^\infty}) \arrow[r, "\lambda"] \arrow[u, "\beta"] & \bigoplus_{\nu\in\Sigma} H^1(\mathbb{Q}_q, E)(p) \arrow[u, "\delta"]
\end{tikzcd}$$

and since β is surjective we deduce from the snake lemma that we have an exact sequence

$$0 \to \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\beta) \to \mathrm{Ker}(\delta) \cap \mathrm{Im}(\lambda) \to \mathrm{Coker}(\alpha) \to 0.$$

Hence $\mathrm{Ker}(\alpha)$ is finite. Furthermore, $\mathrm{Coker}(\alpha)$ will be finite provided we can show that $\mathrm{Ker}(\delta)$ is finite. We devote the rest of this section to calculating $\#\mathrm{Ker}(\delta)$.

The inflation-restriction sequence shows that

$$\mathrm{Ker}(\delta) = \bigoplus_{\nu\in\Sigma} H^1(\mathbb{Q}_{\infty,\nu}/\mathbb{Q}_\nu, E(\mathbb{Q}_{\infty,\nu}))(p),$$

where we have fixed a prime of $\mathbb{Q}_\infty$ lying above ν. Hence it is sufficient to determine $\#H^1(\mathbb{Q}_{\infty,\nu}/\mathbb{Q}_\nu, E(\mathbb{Q}_{\infty,\nu}))(p)$.

LEMMA. *Assume that $\nu \neq p$. Then $\#H^1(\mathbb{Q}_{\infty,\nu}/\mathbb{Q}_\nu, E(\mathbb{Q}_{\infty,\nu}))(p)$ is the p-part of c_ν, where $c_\nu = [E(\mathbb{Q}_\nu) : E_0(\mathbb{Q}_\nu)]$ denotes the local Tamagawa factor at ν.*

Proof. Recall that $E_0(\mathbb{Q}_\nu)$ is the subgroup of $E(\mathbb{Q}_\nu)$ that maps to the non-singular points $\widetilde{E}_{ns}(\mathbb{F}_\nu)$, where $\widetilde{E}$ denotes the reduction of E over $\mathbb{Q}_\nu$. Since $\mathrm{Gal}(\mathbb{Q}_\nu^{nr}/\mathbb{Q}_\nu) \cong \widehat{\mathbb{Z}}$ and $\mathbb{Q}_{\infty,\nu}/\mathbb{Q}_\nu$ is unramified, we know that

$$H^1(\mathbb{Q}_{\infty,\nu}/\mathbb{Q}_\nu, E(\mathbb{Q}_{\infty,\nu}))(p) \cong H^1(\mathbb{Q}_\nu^{nr}/\mathbb{Q}_\nu, E(\mathbb{Q}_\nu^{nr}))(p).$$

But McCallum [McC] has shown that the exact orthogonal complement of $E_0(\mathbb{Q}_\nu)$ in the Tate pairing $E(\mathbb{Q}_\nu) \times H^1(\mathbb{Q}_\nu, E) \to \mathbb{Q}/\mathbb{Z}$ is the unramified cohomology $H^1(\mathbb{Q}_\nu^{nr}/\mathbb{Q}_\nu, E(\mathbb{Q}_\nu^{nr}))$, and so the lemma follows.

Now let $\mathfrak{p}$ be the unique prime of $\mathbb{Q}_\infty$ lying above p. Recall that p is totally ramified in $\mathbb{Q}_\infty$ and that $\mathrm{Gal}(\mathbb{Q}_{\infty,\mathfrak{p}}/\mathbb{Q}_p) \cong \Gamma$.

Assuming that E satisfies (G) or (M), let L be the smallest subfield of $\mathbb{Q}_p(\mu_p)$ where E has semi-stable reduction. We denote by $\mathfrak{F}$ the reduction of E over the field L, and we write $\mathfrak{R}$ for the reduction map. Recalling that L has residue field $\mathbb{F}_p$, the map

$$\mathfrak{R}\colon E(L) \to \mathfrak{F}(\mathbb{F}_p),$$

is clearly surjective.

LEMMA.

(i) *Assume that E has potential good ordinary reduction at p and satisfies (G). Then*

$$\#H^1(\mathbb{Q}_{\infty,\mathfrak{p}}/\mathbb{Q}_{\mathfrak{p}}, E(\mathbb{Q}_{\infty,\mathfrak{p}}))(p) = \#\mathfrak{F}(\mathbb{F}_p)(p)\#(\mathfrak{R}E(\mathbb{Q}_p))(p).$$

(ii) *Assume E satisfies (M) and does not have split multiplicative reduction over $\mathbb{Q}_p$. Then*

$$\#H^1(\mathbb{Q}_{\infty,\mathfrak{p}}/\mathbb{Q}_{\mathfrak{p}}, E(\mathbb{Q}_{\infty,\mathfrak{p}}))(p) = 1.$$

For example, if E has good ordinary reduction at p and $\widetilde{E}$ denotes the reduction of E over $\mathbb{Q}_p$, then $\mathfrak{R}\colon E(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p)$ surjects and $\#H^1(\mathbb{Q}_{\infty,\mathfrak{p}}/\mathbb{Q}_{\mathfrak{p}}, E(\mathbb{Q}_{\infty,\mathfrak{p}}))(p) = \#\widetilde{E}(\mathbb{F}_p)(p)^2$.

Proof. Let us begin with some general remarks. If $V = T_pE \otimes \mathbb{Q}_p$ then set W to be the $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-invariant $\mathbb{Q}_p$-subspace of V of minimal dimension, such that some subgroup of I_p of finite index acts trivially on the quotient V/W. Let C be the image of W under the map

$$V \to V/T_pE = E_{p^\infty},$$

so we know that C is $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-invariant. Put $h = \mathrm{corank}_{\mathbb{Z}_p} C$ and let $D = E_{p^\infty}/C$.

As Coates and Greenberg [CoG] point out we may identify C with $\mathcal{F}_{p^\infty}$, where $\mathcal{F}$ denotes the formal group of E defined over the ring of integers $\mathcal{O}_L$ of L. Consequently C is a connected p-divisible group over $\mathcal{O}_L$, and D is an étale p-divisible group over $\mathcal{O}_L$. Furthermore $h = 1$, since in our situation $\mathcal{F}$ has height 1.

In fact if E has potential good reduction then D can be identified with $\mathfrak{F}_{p^\infty}$, and we have the exact sequence

$$0 \to \mathcal{F}(\overline{\mathbb{Q}_p}) \to E(\overline{\mathbb{Q}_p}) \to \mathfrak{F}(\overline{\mathbb{F}_p}) \to 0.$$

As E is defined over $\mathbb{Q}_p$ this is an exact sequence of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-modules.

We dispose of (ii) first. Let $E^{(\psi)}$ denote a quadratic twist of E that has split multiplicative reduction over $\mathbb{Q}_p$, so $E \cong E^{(\psi)}$ over a quadratic extension F' of $\mathbb{Q}_p$. We set $\Gamma' := \mathrm{Gal}(F'_\infty/F')$ where F'_∞ is the $\mathbb{Z}_p$-extension of F'.

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

It is well known (for example see [Jon]) that we have a decomposition

$$\begin{aligned} H^1(\Gamma', E(F'_\infty)) &= H^1(\Gamma', E(F'_\infty))^+ \oplus H^1(\Gamma', E(F'_\infty))^- \\ &= H^1(\Gamma, E(\mathbb{Q}_{\infty,\mathfrak{p}})) \oplus H^1(\Gamma, E^{(\psi)}(\mathbb{Q}_{\infty,\mathfrak{p}})), \end{aligned}$$

as $p \neq 2$. By Tate local duality

$$H^1(\Gamma, E(\mathbb{Q}_{\infty,\mathfrak{p}})) \cong E(\mathbb{Q}_p)/\mathbf{N}_{\mathbb{Q}_p} E(\mathbb{Q}_{\infty,\mathfrak{p}}),$$

where

$$\mathbf{N}_{\mathbb{Q}_p} E(\mathbb{Q}_{\infty,\mathfrak{p}}) = \bigcap_{\mathbb{Q}_p \subset H \subset \mathbb{Q}_{\infty,\mathfrak{p}}} \mathbf{N}_{H/\mathbb{Q}_p} E(H),$$

denotes the group of universal norms of E from $\mathbb{Q}_{\infty,\mathfrak{p}}$ to $\mathbb{Q}_p$. Clearly it is sufficent to show the triviality of $E(\mathbb{Q}_p)/\mathbf{N}_{\mathbb{Q}_p} E(\mathbb{Q}_{\infty,\mathfrak{p}})$.

Now from our decomposition we see that

$$E(F')/\mathbf{N}_{F'} E(F'_\infty) \cong E(\mathbb{Q}_p)/\mathbf{N}_{\mathbb{Q}_p} E(\mathbb{Q}_{\infty,\mathfrak{p}}) \times E^{(\psi)}(\mathbb{Q}_p)/\mathbf{N}_{\mathbb{Q}_p} E^{(\psi)}(\mathbb{Q}_{\infty,\mathfrak{p}}).$$

There are two possibilities (see [CoG], p. 172).

Firstly, if the Tate period q_E is itself a universal norm from $\mathbb{Q}_{\infty,\mathfrak{p}}$ to $\mathbb{Q}_p$ then both $E(F')/\mathbf{N}_{F'} E(F'_\infty)$ and $E^{(\psi)}(\mathbb{Q}_p)/\mathbf{N}_{\mathbb{Q}_p} E^{(\psi)}(\mathbb{Q}_{\infty,\mathfrak{p}})$ are isomorphic to $\mathbb{Z}_p$, which implies $E(\mathbb{Q}_p)/\mathbf{N}_{\mathbb{Q}_p} E(\mathbb{Q}_{\infty,\mathfrak{p}})$ is trivial. Conversely, if q_E is not a universal norm then $E(F')/\mathbf{N}_{F'} E(F'_\infty)$ and $E^{(\psi)}(\mathbb{Q}_p)/\mathbf{N}_{\mathbb{Q}_p} E^{(\psi)}(\mathbb{Q}_{\infty,\mathfrak{p}})$ have finite order given by the index of the norm residue symbol of q_E for the extensions F'_∞/F' and $\mathbb{Q}_{\infty,\mathfrak{p}}/\mathbb{Q}_p$, respectively. Since these extensions are translates of each other by a group of order 2 and p is odd, again $E(\mathbb{Q}_p)/\mathbf{N}_{\mathbb{Q}_p} E(\mathbb{Q}_{\infty,\mathfrak{p}})$ must be trivial and assertion (ii) is proved.

The proof of (i) is trickier. Let $K = \mathbb{Q}_p(\mu_{p^\infty})$ and set $G_\infty := \mathrm{Gal}(K/\mathbb{Q}_p)$, so $G_\infty \cong \Gamma \times \Delta$. Taking G_∞-invariants of the exact sequence

$$0 \to \mathcal{F}(K) \to E(K) \xrightarrow{\mathfrak{R}} \mathfrak{F}(\mathbb{F}_p) \to 0,$$

we obtain the long exact sequence

$$\begin{aligned} E(\mathbb{Q}_p) &\xrightarrow{\mathfrak{R}} \mathfrak{F}(\mathbb{F}_p) \to H^1(G_\infty, \mathcal{F}) \to H^1(G_\infty, E) \\ &\longrightarrow H^1(G_\infty, \mathfrak{F}) \to H^2(G_\infty, \mathcal{F}). \end{aligned}$$

By inflation-restriction

$$0 \to H^1(\Gamma, E(\mathbb{Q}_{\infty,\mathfrak{p}})) \to H^1(G_\infty, E(K)) \to H^1(\Delta, E(K))^\Gamma$$

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

and since $p \nmid \#\Delta$ implies $H^1(\Delta, \cdot)(p) = 0$, it immediately follows that

$$H^1(\Gamma, E(\mathbb{Q}_{\infty,\mathfrak{p}}))(p) = H^1(G_\infty, E(K))(p).$$

We will first show that the $\mathbb{Z}_p$-corank of this group is zero, and then calculate its size. In order to do this we apply the important theorem that

$$H^i(K, \mathcal{F}) = 0 \quad \text{for all } i \geqslant 1,$$

since K over L has infinite conductor and so is a 'deeply ramified' extension of L in the sense of Coates and Greenberg [CoG]. As a corollary of their result, $H^1(G_\infty, \mathcal{F}(K)) = H^1(\mathbb{Q}_p, \mathcal{F})$ by inflation-restriction. From the Hochshild–Serre spectral sequence for $K/\mathbb{Q}_p$, we know that

$$0 = H^1(K, \mathcal{F})^{G_\infty} \to H^2(G_\infty, \mathcal{F}(K)) \to H^2(\mathbb{Q}_p, \mathcal{F}) \to H^2(K, \mathcal{F}) = 0$$

and hence $H^2(G_\infty, \mathcal{F}(K)) = H^2(\mathbb{Q}_p, \mathcal{F})$. Thus our long exact sequence becomes

$$\begin{aligned} 0 &\to \mathfrak{F}(\mathbb{F}_p)/\Re E(\mathbb{Q}_p) \to H^1(\mathbb{Q}_p, \mathcal{F}) \to H^1(G_\infty, E(K)) \\ &\to H^1(G_\infty, \mathfrak{F}(\mathbb{F}_p)) \to H^2(\mathbb{Q}_p, \mathcal{F}). \end{aligned}$$

In fact the proof of the lemma can now be deduced from the following three assertions, which we prove below:

(a) $H^1(G_\infty, \mathfrak{F}(\mathbb{F}_p))(p) = \mathfrak{F}(\mathbb{F}_p)(p)$;
(b) $H^1(\mathbb{Q}_p, \mathcal{F})$ is finite and $\#H^1(\mathbb{Q}_p, \mathcal{F})(p) = \#\mathfrak{F}(\mathbb{F}_p)(p)$;
(c) $H^2(\mathbb{Q}_p, \mathcal{F})(p) = 0$.

Consequently, $\operatorname{corank}_{\mathbb{Z}_p} H^1(G_\infty, E(K)) = 0$ since both groups $\mathfrak{F}(\mathbb{F}_p)/\Re E(\mathbb{Q}_p)$ and $H^1(G_\infty, \mathfrak{F}(\mathbb{F}_p))(p)$ are finite. Moreover

$$\#H^1(G_\infty, E(K))(p) = \frac{\#\mathfrak{F}(\mathbb{F}_p)(p)^2}{\#\left(\mathfrak{F}(\mathbb{F}_p)/\Re E(\mathbb{Q}_p)\right)(p)}$$

and hence the lemma as $H^1(\Gamma, E(\mathbb{Q}_{\infty,\mathfrak{p}}))(p) = H^1(G_\infty, E(K))(p)$. We spend the remainder of this section proving these three statements.

To deduce (a) we know that

$$0 \to H^1(\Gamma, \mathfrak{F}(\mathbb{F}_p)) \to H^1(G_\infty, \mathfrak{F}(\mathbb{F}_p)) \to H^1(\Delta, \mathfrak{F}(\mathbb{F}_p))^\Gamma,$$

so $H^1(G_\infty, \mathfrak{F}(\mathbb{F}_p))(p) = H^1(\Gamma, \mathfrak{F}(\mathbb{F}_p))(p)$ as $p \nmid \#\Delta$. But as Γ acts trivially on $\mathfrak{F}(\mathbb{F}_p)$, $H^1(\Gamma, \mathfrak{F}(\mathbb{F}_p)) = \mathfrak{F}(\mathbb{F}_p)(p)$ which is finite.

To prove (b) we start by computing $\mathbb{Z}_p$-coranks. By Kummer theory

$$0 \to \mathcal{F}(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(\mathbb{Q}_p, \mathcal{F}_{p^\infty}) \to H^1(\mathbb{Q}_p, \mathcal{F})(p) \to 0.$$

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

It follows from Mattuck's Theorem that $\mathcal{F}(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Q}_p/\mathbb{Z}_p$, and hence

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(\mathbb{Q}_p, \mathcal{F}) = \mathrm{corank}_{\mathbb{Z}_p} H^1(\mathbb{Q}_p, \mathcal{F}_{p^\infty}) - 1.$$

We use Tate's Euler characteristic theorem [Mil] to calculate $\mathrm{corank}_{\mathbb{Z}_p} H^1(\mathbb{Q}_p, \mathcal{F}_{p^\infty})$. If M is a finite $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-module of p-power order, denote its dual by $M^D = \mathrm{Hom}(M, \mu_{p^\infty})$. Then Tate's Theorem (in this case) states that

$$\frac{\#H^0(\mathbb{Q}_p, M)\#H^2(\mathbb{Q}_p, M)}{\#H^1(\mathbb{Q}_p, M)} = (\#M)^{-1}.$$

So for $M = \mathcal{F}_{p^n}$ we find that $\#H^1(\mathbb{Q}_p, \mathcal{F}_{p^n}) = p^n\#H^0(\mathbb{Q}_p, \mathcal{F}_{p^n})\#H^2(\mathbb{Q}_p, \mathcal{F}_{p^n})$ as $\mathrm{corank}_{\mathbb{Z}_p} C = 1$.

Now $\#H^0(\mathbb{Q}_p, \mathcal{F}_{p^n}) = 1$ as $\mathcal{F}(\mathbb{Q}_p)$ has trivial p-torsion. In fact $\mathcal{F}(L)$ has trivial p-torsion; suppose we have a point x of order p, and let $\mathcal{M}_L = (\wp_L)$ be the maximal ideal of $\mathcal{O}_L$. If v_L denotes the valuation on $\mathcal{O}_L$, then

$$v_L(x) \leqslant \frac{v_L(\wp_L)}{p-1} = \frac{1}{(p-1)}.$$

However $x \in \mathcal{M}_L$ so $v_L(x) \geqslant 1$. As $p > 2$ this cannot happen, and so $\#\mathcal{F}_{p^\infty}(L) = 1$.

On the other hand, the Weil pairing implies that $E_{p^n} \cong E_{p^n}^D$ and hence $\mathfrak{F}_{p^n} \cong \mathcal{F}_{p^n}^D$. Thus by Tate local duality

$$\#H^2(\mathbb{Q}_p, \mathcal{F}_{p^n}) = \#H^0(\mathbb{Q}_p, \mathfrak{F}_{p^n}) = \#\mathfrak{F}(\mathbb{F}_p)(p),$$

for large enough n. Therefore we know that $\#H^1(\mathbb{Q}_p, \mathcal{F}_{p^n}) = p^n\#\mathfrak{F}(\mathbb{F}_p)(p)$ for $n \gg 0$. Again by Kummer theory

$$0 \to \mathcal{F}_{p^\infty}(\mathbb{Q}_p)/p^n\mathcal{F}_{p^\infty}(\mathbb{Q}_p) \to H^1(\mathbb{Q}_p, \mathcal{F}_{p^n}) \to \left(H^1(\mathbb{Q}_p, \mathcal{F}_{p^\infty})\right)_{p^n} \to 0,$$

so consequently $\mathrm{corank}_{\mathbb{Z}_p} H^1(\mathbb{Q}_p, \mathcal{F}_{p^\infty}) = 1$ and $\#H^1(\mathbb{Q}_p, \mathcal{F})(p) = \#\mathfrak{F}(\mathbb{F}_p)(p)$.

Finally to show that (c) is true, choose p^n so large that it annihilates $\mathfrak{F}(\mathbb{F}_p)(p)$. Consider the exact sequence

$$H^1(\mathbb{Q}_p, \mathcal{F}) \xrightarrow{p^n} H^1(\mathbb{Q}_p, \mathcal{F}) \xrightarrow{\partial} H^2(\mathbb{Q}_p, \mathcal{F}_{p^n}) \to \left(H^2(\mathbb{Q}_p, \mathcal{F})\right)_{p^n} \to 0.$$

Because p^n kills $H^1(\mathbb{Q}_p, \mathcal{F})(p)$, thus $\partial\colon H^1(\mathbb{Q}_p, \mathcal{F})(p) \hookrightarrow H^2(\mathbb{Q}_p, \mathcal{F}_{p^n})$ is an injection. But by Tate duality $\#H^2(\mathbb{Q}_p, \mathcal{F}_{p^n}) = \#\mathfrak{F}(\mathbb{F}_p)(p)$, so $\partial: H^1(\mathbb{Q}_p, \mathcal{F})(p) \xrightarrow{\sim} H^2(\mathbb{Q}_p, \mathcal{F}_{p^n})$ is an isomorphism and $\mathrm{Ker}(\partial) = H^1(\mathbb{Q}_p, \mathcal{F})_{p\text{-div}}$, its p-divisible subgroup. Thus ∂ is surjective which implies that $(H^2(\mathbb{Q}_p, \mathcal{F}))_{p^n} = 0$. The proof is now complete.

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

2.3. CHARACTERISTIC POWER SERIES FOR $\mathfrak{X}_\infty$

Throughout this section we make the following assumption about E.

HYPOTHESIS (Kol). E is modular and its analytic rank r_E is zero.

It is important to note that (Kol) implies the finiteness of both $E(\mathbb{Q})$ and the Tate–Shafarevic group, as a consequence of Kolyvagin's deep results [Kol].

Let $\mathfrak{x}_p\colon \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_p^\times$ denote the pth-cyclotomic character. From the last section's work we have the following result.

THEOREM 3. *Assume that either E has potential good ordinary reduction at p and satisfies (G), or E satisfies (M) and does not have split multiplicative reduction at p. Moreover suppose that E satisfies the hypothesis* (Kol).

Then the module $\mathfrak{X}_\infty$ is Λ-torsion. If $\mathcal{G}_E$ denotes its characteristic power series then the leading term $\mathfrak{x}_p^0(\mathcal{G}_E) \neq 0$.

Proof. Recall that in the last section we showed that the map

$$\alpha\colon \mathfrak{S}(E/\mathbb{Q}) \to \mathfrak{S}(E/\mathbb{Q}_\infty)^\Gamma,$$

has finite kernel and cokernel. We will first prove that $\mathfrak{X}_\infty = \mathfrak{S}(E/\mathbb{Q}_\infty)^\wedge$ is a finitely generated Λ-module.

In fact all we need to show is that $(\mathfrak{X}_\infty)_\Gamma$ is finitely generated over $\mathbb{Z}_p$. Now $(\mathfrak{X}_\infty)_\Gamma$ is dual to $\mathfrak{S}(E/\mathbb{Q}_\infty)^\Gamma$ so it suffices to prove that

$$\mathfrak{S}(E/\mathbb{Q}) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r \oplus (\text{finite } p\text{-group}).$$

But this is a classical result for $\mathfrak{S}(E/\mathbb{Q})$ and so $\mathfrak{X}_\infty$ is finitely generated over Λ.

As a first application we must have

$$\mathfrak{X}_\infty \approx \Lambda^r \oplus \Lambda/(g_1) \oplus \cdots \oplus \Lambda/(g_k),$$

where $r = \mathrm{rank}_\Lambda\, \mathfrak{X}_\infty$ and $0 \neq g_i \in \Lambda$, $1 \leqslant i \leqslant k$, with $\approx$ denoting pseudo-isomorphism.

Let us recall that the Tate–Shafarevic group III_E is defined by the exactness of

$$0 \to \mathrm{III}_E \to H^1(\mathbb{Q}, E) \xrightarrow{\mathrm{res}} \bigoplus_\nu H^1(\mathbb{Q}_\nu, E),$$

where the sum is over *all* places of $\mathbb{Q}$. Remember that the hypothesis (Kol) implies that both $E(\mathbb{Q})$ and $\mathrm{III}_E(p)$ are finite [Kol]. Now

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathfrak{S}(E/\mathbb{Q}) \to \mathrm{III}_E(p) \to 0,$$

is exact, hence both $\mathfrak{S}(E/\mathbb{Q})$ and $\mathfrak{S}(E/\mathbb{Q}_\infty)^\Gamma$ are finite. But $\mathfrak{S}(E/\mathbb{Q}_\infty)^\Gamma$ is dual to $(\mathfrak{X}_\infty)_\Gamma$; therefore $\mathfrak{X}_\infty$ must be Λ-torsion, $\mathcal{G}_E = (g_1 \cdots g_k)$ and $\mathfrak{x}_p^0(\mathcal{G}_E) \neq 0$.

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

PROPOSITION 4. *Assume that either E has potential good ordinary reduction at p and satisfies (G), or E satisfies (M) and does not have split multiplicative reduction at p.*

Again suppose that E satisfies the hypothesis (Kol). *Then*

$$\mathfrak{r}_p^0(\mathcal{G}_E) \sim \frac{\#\text{III}_E(p)}{\#E(\mathbb{Q})^2} \# H^1(\mathbb{Q}_{\infty,\mathfrak{p}}/\mathbb{Q}_{\mathfrak{p}}, E(\mathbb{Q}_{\infty,\mathfrak{p}})) \prod_{\nu \neq p} c_\nu,$$

where III_E *is the Tate–Shafarevic group of E over $\mathbb{Q}$, with $\sim$ denoting equivalence up to a p-adic unit.*

Before we can begin the proof of Proposition 4, we need to examine the surjectivity of the restriction map over $\mathbb{Q}_\infty$. In fact we shall prove a stronger result than we need.

LEMMA. *If $H^2(G_{\infty,\Sigma}, E_{p^\infty}) = 0$, then the restriction map*

$$H^1(G_{\infty,\Sigma}, E_{p^\infty}) \to \bigoplus_{\nu \in \Sigma_\infty} H^1(\mathbb{Q}_{\infty,\nu}, E)(p),$$

is surjective.

Proof. We use the notation of Perrin–Riou [PeR], although most of the ideas are essentially due to Iwasawa. For $n, m \in \mathbb{N}$ put

$$S(E/\mathbb{Q}_n; p^m) = \text{Ker}\left(H^1(\mathbb{Q}_n, E_{p^m}) \xrightarrow{\text{res}} \bigoplus_\nu H^1(\mathbb{Q}_{n,\nu}, E)(p)\right),$$

where $\mathbb{Q}_n$ denotes the nth-layer of the $\mathbb{Z}_p$-extension. We define the usual Selmer groups $H^1_f(\cdot, E_{p^\infty})$ as

$$H^1_f(\mathbb{Q}_n, E_{p^\infty}) := \varinjlim S(E/\mathbb{Q}_n; p^m).$$

We also define compact Selmer groups $H^1_f(\mathbb{Q}_n, T_pE) \subset H^1(\mathbb{Q}_n, T_pE)$ by

$$H^1_f(\mathbb{Q}_n, T_pE) := \varprojlim S(E/\mathbb{Q}_n; p^m).$$

Lastly set

$$Z^1_{\infty,f} := \varprojlim H^1_f(\mathbb{Q}_n, T_pE), \qquad H^1_f(\mathbb{Q}_\infty, E_{p^\infty}) := \varinjlim H^1_f(\mathbb{Q}_n, E_{p^\infty}).$$

In order to prove our lemma it is sufficient to show that $Z^1_{\infty,f} = 0$, since by the Cassels–Poitou–Tate exact sequence over $\mathbb{Q}_\infty$, we have

$$0 \longrightarrow H^1_f(\mathbb{Q}_\infty, E_{p^\infty}) \to H^1(G_{\infty,\Sigma}, E_{p^\infty}) \xrightarrow{\text{res}} \bigoplus_{\nu \in \Sigma_\infty} H^1(\mathbb{Q}_{\infty,\nu}, E)(p) \to (Z^1_{\infty,f})^\wedge \to 0,$$

as $H^2(G_{\infty,\Sigma}, E_{p^\infty}) = 0$ by [CMc].

We shall now construct a map

$$Z^1_{\infty,f} \to \mathrm{Hom}_\Lambda(H^1_f(\mathbb{Q}_\infty, E_{p^\infty})^\wedge, \Lambda)^\bullet,$$

where $^\bullet$ indicates that the natural Γ-action has been inverted.

In fact we will prove the following two assertions:

(a) The map $Z^1_{\infty,f} \to \mathrm{Hom}_\Lambda(H^1_f(\mathbb{Q}_\infty, E_{p^\infty})^\wedge, \Lambda)^\bullet$ is an embedding;
(b) The module $Z^1_{\infty,f}$ is Λ-torsion.

The triviality of $Z^1_{\infty,f}$ then follows immediately, since $\mathrm{Hom}_\Lambda(X, \Lambda)$ is Λ-free if X is finitely generated as a Λ-module, and $H^1_f(\mathbb{Q}_\infty, E_{p^\infty})^\wedge$ is none other than $\mathfrak{X}_\infty$.

In order to deduce (a), by a basic property of continuous cohomology we can identify $H^1_f(\mathbb{Q}_n, T_pE) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ with the maximal divisible subgroup of $H^1_f(\mathbb{Q}_n, E_{p^\infty})$. This gives us an exact sequence

$$0 \to H^1_f(\mathbb{Q}_n, T_pE) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1_f(\mathbb{Q}_n, E_{p^\infty}) \to M,$$

where M is torsion and not divisible. Taking Pontrjagin duals, we obtain another exact sequence

$$M^\wedge \to H^1_f(\mathbb{Q}_n, E_{p^\infty})^\wedge \to \mathrm{Hom}_{\mathbb{Z}_p}(H^1_f(\mathbb{Q}_n, T_pE), \mathbb{Z}_p) \to 0.$$

Applying the functor $\mathrm{Hom}_{\mathbb{Z}_p}(\cdot, \mathbb{Z}_p)$ to our finitely generated $\mathbb{Z}_p$-modules, we have a canonical injection

$$H^1_f(\mathbb{Q}_n, T_pE)/H^1_f(\mathbb{Q}_n, T_pE)_{\mathrm{tors}} \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(H^1_f(\mathbb{Q}_n, E_{p^\infty})^\wedge, \mathbb{Z}_p),$$

since $\mathrm{Hom}_{\mathbb{Z}_p}(M^\wedge, \mathbb{Z}_p) = 0$ as $M^\wedge$ is $\mathbb{Z}_p$-torsion.

Writing $\Gamma^n = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n)$, the natural map $H^1_f(\mathbb{Q}_n, E_{p^\infty}) \to H^1_f(\mathbb{Q}_\infty, E_{p^\infty})^{\Gamma^n}$ certainly has finite kernel, whence we obtain the dual map $(H^1_f(\mathbb{Q}_\infty, E_{p^\infty})^\wedge)_{\Gamma^n} \to H^1_f(\mathbb{Q}_n, E_{p^\infty})^\wedge$ with finite cokernel. Again applying $\mathrm{Hom}_{\mathbb{Z}_p}(\cdot, \mathbb{Z}_p)$ yields an injection

$$\mathrm{Hom}_{\mathbb{Z}_p}(H^1_f(\mathbb{Q}_n, E_{p^\infty})^\wedge, \mathbb{Z}_p) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_p}((H^1_f(\mathbb{Q}_\infty, E_{p^\infty})^\wedge)_{\Gamma^n}, \mathbb{Z}_p),$$

and from there a canonical embedding

$$H^1_f(\mathbb{Q}_n, T_pE)/H^1_f(\mathbb{Q}_n, T_pE)_{\mathrm{tors}} \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_p}((H^1_f(\mathbb{Q}_\infty, E_{p^\infty})^\wedge)_{\Gamma^n}, \mathbb{Z}_p).$$

But $E(\mathbb{Q}_\infty)_{\mathrm{tors}}$ is finite, so $\varprojlim H^1_f(\mathbb{Q}_n, T_pE)_{\mathrm{tors}} = 0$ because $H^1_f(\mathbb{Q}_n, T_pE)_{\mathrm{tors}} = E_{p^\infty}(\mathbb{Q}_n)$. Hence passing to the projective limit we have shown statement (a),

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

as it is a standard fact that for any finitely generated Λ-module X, the limit $\varprojlim \mathrm{Hom}_{\mathbb{Z}_p}(X_{\Gamma^n}, \mathbb{Z}_p) = \mathrm{Hom}_\Lambda(X, \Lambda)^\bullet$.

To prove that (b) is true, we do a simple calculation of Λ-coranks. Again from the Cassels–Poitou–Tate sequence, we know that

$$\begin{aligned}&\mathrm{rank}_\Lambda Z^1_{\infty,f}\\ &\quad= \sum_{\nu\in\Sigma_\infty} \mathrm{corank}_\Lambda H^1(\mathbb{Q}_{\infty,\nu}, E)(p) - \mathrm{corank}_\Lambda H^1(G_{\infty,\Sigma}, E_{p^\infty}) + \mathrm{rank}_\Lambda \mathfrak{X}_\infty.\end{aligned}$$

Let h denote the stable height of E at p, so $h = 1$ if p is potentially ordinary and $h = 2$ if p is potentially supersingular. Now, $\mathrm{corank}_\Lambda H^1(G_{\infty,\Sigma}, E_{p^\infty}) = 1$. Furthermore, if $\nu \nmid p$ then $H^1(\mathbb{Q}_{\infty,\nu}, E)(p)$ is dual to $T_pE^{\mathrm{Gal}(\overline{\mathbb{Q}_\nu}/\mathbb{Q}_{\infty,\nu})}$, and so is definitely Λ-cotorsion. On the other hand by [CoG], Proposition 4.9, the Λ-rank of $H^1(\mathbb{Q}_{\infty,\mathfrak{p}}, E)(p)$ is equal to $2 - h$. Since $\mathrm{rank}_\Lambda\, \mathfrak{X}_\infty = h - 1$, we have shown that $\mathrm{rank}_\Lambda Z^1_{\infty,f} = 0$ and the lemma follows.

Proof of Proposition 4. Recall in our commutative diagram

$$\begin{array}{ccccccc}
0 \longrightarrow & \mathfrak{S}(E/\mathbb{Q}_\infty)^\Gamma & \longrightarrow & H^1(G_{\infty,\Sigma}, E_{p^\infty})^\Gamma & \xrightarrow{\lambda_\infty} & \bigoplus_{\nu\in\Sigma_\infty} (H^1(\mathbb{Q}_{\infty,\nu}, E)(p))^\Gamma \\
& \uparrow{\scriptstyle\alpha} & & \uparrow{\scriptstyle\beta} & & \uparrow{\scriptstyle\delta} \\
0 \longrightarrow & \mathfrak{S}(E/\mathbb{Q}) & \longrightarrow & H^1(G_\Sigma, E_{p^\infty}) & \xrightarrow{\lambda} & \bigoplus_{q\in\Sigma} H^1(\mathbb{Q}_q, E)(p),
\end{array}$$

all the vertical maps have finite kernel and cokernel. Hence $\mathrm{Coker}(\lambda_\infty)$ is finite, since $\mathrm{Coker}(\lambda) = (E(\mathbb{Q})\widehat{\otimes}\mathbb{Z}_p)^\wedge$ and $E(\mathbb{Q})$ is finite.

By a standard lemma on finitely generated Λ-torsion modules

$$\mathfrak{r}^0_p(\mathcal{G}_E) \sim \frac{\#(\mathfrak{X}_\infty)_\Gamma}{\#(\mathfrak{X}_\infty)^\Gamma}.$$

Our previous lemma implies that $H^1(G_{\infty,\Sigma}, E_{p^\infty}) \to \bigoplus_{\nu\in\Sigma_\infty} H^1(\mathbb{Q}_{\infty,\nu}, E)(p)$ is surjective, so taking Γ-invariants we obtain the exact sequence

$$\begin{aligned}\cdots \to H^1(G_{\infty,\Sigma}, E_{p^\infty})^\Gamma &\xrightarrow{\lambda_\infty} \bigoplus_{\nu\in\Sigma_\infty} (H^1(\mathbb{Q}_{\infty,\nu}, E)(p))^\Gamma\\ &\to H^1(\Gamma, \mathfrak{S}(E/\mathbb{Q}_\infty)) \to 0,\end{aligned}$$

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

as $H^1(\Gamma, H^1(G_{\infty,\Sigma}, E_{p^\infty})) = 0$ by [CMc], Theorem 2. Consequently $\#(\mathfrak{X}_\infty)^\Gamma = \#\mathfrak{S}(E/\mathbb{Q}_\infty)_\Gamma = \#\,\mathrm{Coker}(\lambda_\infty)$, and

$$\begin{array}{ccccccc}
H^1(G_{\infty,\Sigma}, E_{p^\infty})^\Gamma & \xrightarrow{\lambda_\infty} & \bigoplus_{\nu\in\Sigma_\infty} (H^1(\mathbb{Q}_{\infty,\nu}, E)(p))^\Gamma & \longrightarrow & \mathrm{Coker}(\lambda_\infty) & \longrightarrow & 0 \\
\uparrow{\scriptstyle\beta} & & \uparrow{\scriptstyle\delta} & & \uparrow & & \\
H^1(G_\Sigma, E_{p^\infty}) & \xrightarrow{\lambda} & \bigoplus_{q\in\Sigma} H^1(\mathbb{Q}_q, E)(p) & \longrightarrow & (E(\mathbb{Q})\widehat{\otimes}\mathbb{Z}_p)^\wedge & \longrightarrow & 0,
\end{array}$$

by the Cassels–Poitou–Tate sequence.

We know (i) β is surjective, (ii) $\mathrm{Ker}(\beta)$ is finite with $\#\mathrm{Ker}(\beta) \sim \#E(\mathbb{Q})$, and (iii) $\mathrm{Ker}(\delta)$ is finite with $\#\mathrm{Ker}(\delta) \sim \#H^1(\mathbb{Q}_{\infty,\mathfrak{p}}/\mathbb{Q}_{\mathfrak{p}}, E(\mathbb{Q}_{\infty,\mathfrak{p}}))\prod_{\nu\neq p} c_\nu$. By the snake lemma

$$0 \to \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\beta) \xrightarrow{j} \mathrm{Ker}(\delta) \cap \mathrm{Im}(\lambda) \to \mathrm{Coker}(\alpha) \to 0$$

and computing orders

$$\begin{aligned}
\#\mathfrak{S}(E/\mathbb{Q}_\infty)^\Gamma &= \#\mathrm{Coker}(\alpha)\#\mathrm{Im}(\alpha) \\
&= \frac{\#\mathrm{Coker}(\alpha)\#\mathfrak{S}(E/\mathbb{Q})\#\mathrm{Im}(j)}{\#\mathrm{Ker}(\beta)} \\
&= \frac{\#\mathfrak{S}(E/\mathbb{Q})\#\mathrm{Ker}(\delta)}{\#\mathrm{Ker}(\beta)[\mathrm{Ker}(\delta) : \mathrm{Ker}(\delta)\cap\mathrm{Im}(\lambda)]}.
\end{aligned}$$

Thus our theorem holds if $[\mathrm{Ker}(\delta) : \mathrm{Ker}(\delta)\cap\mathrm{Im}(\lambda)] \sim \#E(\mathbb{Q})/\#\mathrm{Coker}(\lambda_\infty)$, since $\#\mathfrak{S}(E/\mathbb{Q}) \sim \#\text{Ш}_E(p)$. The rest of the section will be used to show this equivalence.

As before the Cassels–Poitou–Tate sequence implies $\mathrm{Coker}(\lambda) = (E(\mathbb{Q})\widehat{\otimes}\mathbb{Z}_p)^\wedge$, hence

$$\mathrm{Coker}(\lambda) \sim \#E(\mathbb{Q}).$$

Considering the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Ker}(\delta) & \longrightarrow & \bigoplus_{\nu\in\Sigma} H^1(\mathbb{Q}_\nu, E)(p) & \xrightarrow{\delta} & \mathrm{Im}(\delta) & \longrightarrow & 0 \\
& & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathrm{Ker}(\delta)\cap\mathrm{Im}(\lambda) & \longrightarrow & \mathrm{Im}(\lambda) & \longrightarrow & \delta(\mathrm{Im}(\lambda)) & \longrightarrow & 0,
\end{array}$$

we see that $[\mathrm{Ker}(\delta) : \mathrm{Ker}(\delta)\cap\mathrm{Im}(\lambda)] \sim \#E(\mathbb{Q})/\mathrm{Coker}(\lambda_\infty)$ if δ is surjective, for then $\delta(\mathrm{Im}(\lambda)) = \mathrm{Im}(\lambda_\infty)$. The theorem then follows immediately.

In order to prove that δ surjects, it is sufficient to verify that

$$H^2(\mathbb{Q}_{\infty,\nu}/\mathbb{Q}_\nu, E(\mathbb{Q}_{\infty,\nu}))(p) = 0,$$

for all places $\nu \in \Sigma_\infty$. Let $\widehat{E}_{(\nu)}$ be the formal group of E over $\mathbb{Q}_\nu$, so for each $n \geqslant 0$ we have an exact sequence

$$0 \to \widehat{E}_{(\nu)}(\mathbb{Q}_{n,\nu}) \to E(\mathbb{Q}_{n,\nu}) \to B_{n,\nu} \to 0,$$

where $B_{n,\nu}$ is a torsion group. Taking the direct limit

$$0 \to \widehat{E}_{(\nu)}(\mathbb{Q}_{\infty,\nu}) \to E(\mathbb{Q}_{\infty,\nu}) \to B_{\infty,\nu} \to 0,$$

where again $B_{\infty,\nu} = \varinjlim B_{n,\nu}$ is torsion. Applying cohomology

$$\begin{aligned} H^2(\mathbb{Q}_{\infty,\nu}/\mathbb{Q}_\nu, \widehat{E}_{(\nu)}(\mathbb{Q}_{\infty,\nu})) \;&\to\; H^2(\mathbb{Q}_{\infty,\nu}/\mathbb{Q}_\nu, E(\mathbb{Q}_{\infty,\nu})) \\ &\to\; H^2(\mathbb{Q}_{\infty,\nu}/\mathbb{Q}_\nu, B_{\infty,\nu}) \end{aligned}$$

and this last group is zero as Γ has cohomological dimension 1. It suffices to prove that

$$H^2(\mathbb{Q}_{\infty,\nu}/\mathbb{Q}_\nu, \widehat{E}_{(\nu)}(\mathbb{Q}_{\infty,\nu}))(p) = 0.$$

If $\nu \nmid p$ this is obvious because p is a unit in $\mathbb{Z}_q$ where $\nu | q$. If $\nu = \mathfrak{p}$, then it is an easy consequence of the proof of our lemma in Section 2.2 and the fact that $\mathbb{Q}_{\infty,\mathfrak{p}}/\mathbb{Q}_p$ is deeply ramified, that

$$H^2(\Gamma, \widehat{E}_{(\mathfrak{p})}(\mathbb{Q}_{\infty,\mathfrak{p}}))(p) = H^2(\mathbb{Q}_p, \widehat{E}_{(\mathfrak{p})})(p) = 0.$$

Thus δ surjects and the proof is now complete.

2.4. Comparison of Leading Terms

For the moment we assume that E has potential good ordinary reduction at p and satisfies hypotheses (G) and (Kol). So by Proposition 4

$$\mathfrak{x}_p^0(\mathcal{G}_E) \sim \frac{\#\text{Ш}_E(p)}{\#E(\mathbb{Q})^2} \#\mathfrak{F}(\mathbb{F}_p) \#\mathfrak{R}E(\mathbb{Q}_p) \prod_{\nu \neq p} c_\nu,$$

where $\mathfrak{F}$ denotes the reduction over the field $L/\mathbb{Q}_p$ of good reduction and $\mathfrak{R}$ the reduction map over L.

DEFINITION. We define the constant $\kappa_E \in \mathbb{Q}^\times$ by

$$\kappa_E := \frac{\#\mathfrak{F}(\mathbb{F}_p)\#\mathfrak{R}E(\mathbb{Q}_p)}{[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]}.$$

Note that κ_E contains information solely about the reduction of E at p.

Let us further assume that E has bad additive reduction at p, so $d = \#\Phi_p > 1$. Then the p-adic L-function defined in Section 1.5 is a bounded measure on $\mathbb{Z}_p^\times$, and has leading term

$$\begin{aligned}\mathbf{L}_p(E, \mathbf{1}) = \int_{\mathbb{Z}_p^\times} \mathrm{d}\mu_E &= \frac{p}{\alpha_p G(\varepsilon)G(\overline{\varepsilon})}\mathfrak{L}_p^{(G)}(0) \times \frac{L(E,1)}{\Omega_E^+}\\ &\sim \frac{L(E,1)}{\Omega_E^+},\end{aligned}$$

as $C_\varepsilon = p$ and α_p is a p-adic unit.

(In the case of good reduction we would have

$$\mathbf{L}_p(E, \mathbf{1}) = \left(1 - \frac{1}{\alpha_p}\right)^2 \frac{L(E,1)}{\Omega_E^+} \sim \#\widetilde{E}(\mathbb{F}_p)^2 \frac{L(E,1)}{\Omega_E^+},$$

instead, as $(1 - \frac{1}{\alpha_p}) \sim 1 - a_p + p = \#\widetilde{E}(\mathbb{F}_p)$).

Anyhow, it follows from our definition that

$$\mathfrak{r}_p^0(\mathcal{G}_E) \sim \left\{ \frac{\#\text{III}_E(p)}{\#E(\mathbb{Q})^2} \prod_\nu c_\nu \left(\frac{L(E,1)}{\Omega_E^+}\right)^{-1} \right\} \times \kappa_E\, \mathbf{L}_p(E, \mathbf{1}).$$

It is reasonable to conjecture that the term $\{\cdot\}$ above equals 1. (Indeed the Birch and Swinnerton–Dyer conjecture for elliptic curves of analytic rank zero would imply this equality.)

Recall Examples A, B and C from Section 1.7. Considering first the elliptic curve E_A of conductor 99 with potential good ordinary reduction at 3, we have

$$\frac{L(E_A,1)}{\Omega_{E_A}^+} = 1, \quad \#E_A(\mathbb{Q}) = 1, \quad c_3 = c_5 = 1,$$

$$\text{III}_{E_A}(3) = 1 \quad \text{and} \quad \kappa_{E_A} \sim 1,$$

as $\#\mathfrak{F}_A(\mathbb{F}_3) \sim \#\widetilde{E}_A^{(\varepsilon)}(\mathbb{F}_3) = 5$. Thus

$$\mathfrak{r}_p^0(\mathcal{G}_{E_A}) \sim \mathbf{L}_3(E_A, \mathbf{1}).$$

Recall that $\widetilde{f_A}$ was the newform obtained from the elliptic curve $E_A^{(\varepsilon)}$ of conductor 11. As ε is an odd quadratic character, $\Omega^+_{E_A^{(\varepsilon)}} \sim \sqrt{3}\Omega^-_{E_A}$ so

$$\mathbf{L}_3(E_A, \varepsilon) \sim \#\widetilde{E_A^{(\varepsilon)}}(\mathbb{F}_3)^2 \frac{L(E_A^{(\varepsilon)},1)}{\Omega^+_{E_A^{(\varepsilon)}}},$$

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

since $L(E_A,\varepsilon)/1-\widetilde{a_3}3^{-1}+3^{-1}=L(E_A^{(\varepsilon)},1)$ and $G(\overline{\varepsilon})\sim\sqrt{3}$. In fact one might even conjecture that the 3-adic Mellin transform $\int_{x\in 1+3\mathbb{Z}_3}\varepsilon(x)(1+T)^x\mu_{E_A}$ is the characteristic power series $\mathcal{G}_{E_A^{(\varepsilon)}}(T)$ of $\mathfrak{S}(E_A^{(\varepsilon)}/\mathbb{Q}_\infty)^\wedge$ by identification with the ε-eigenspace of the module $\mathfrak{S}(E_A/\mathbb{Q}(\mu_{3^\infty}))^\wedge$ under the action of Δ, where $\mathfrak{S}(E_A/\mathbb{Q}(\mu_{3^\infty}))$ is the Selmer group of E_A over $\mathbb{Q}(\mu_{3^\infty})$.

Recall the definition of the elliptic curve E_B of conductor 147 with potential good ordinary reduction at 7, where the size of inertia $\#\Phi_7$ is 6. Here

$$\frac{L(E_B,1)}{\Omega^+_{E_B}}=1,\quad \#E_B(\mathbb{Q})=1,\quad c_3=c_7=1,\quad \text{and}\quad \text{III}_{E_B}(7)=1.$$

However the character ε is now of order 6 and it seems that $\int_{x\in\mathbb{Z}_7^\times}\varepsilon(x)(1+T)^x\mu_{E_B}$ no longer relates to the arithmetic of an elliptic curve, but rather a piece of $\mathrm{Jac}(X_1(147))$.

Dropping the proviso of potential good ordinary reduction, consider the elliptic curve E_C of conductor 63 which has potential multiplicative reduction at 3. Again

$$\frac{L(E_C,1)}{\Omega^+_{E_C}}=\tfrac{1}{2},\quad \#E_C(\mathbb{Q})=2,\quad c_3=2,\quad c_7=1,$$

$$\text{III}_{E_C}(3)=1\quad\text{and}\quad \alpha_3=1.$$

Interestingly $\mathbf{L}_3(E_C,\varepsilon)=0$ but $L(E_C,\varepsilon)/1-\frac{1}{3}=L(E_C^{(\varepsilon)},1)\neq 0$, so this zero is a purely p-adic phenomenon. As explained at the end of Section 1.6, it is related to the fact that $E_C^{(\varepsilon)}$ over $\mathbb{Q}_3$ is a Tate curve with split multiplicative reduction, so its extended Mordell–Weil group $E_C^{(\varepsilon)\dagger}(\mathbb{Q})$ has rank 1 whilst $E_C^{(\varepsilon)}(\mathbb{Q})$ only has rank 0. One can even compute the derivative by using the variant of the Greenberg–Stevens formula [GrS] given earlier.

2.5. The Main Conjecture

From now on we make the following two assumptions:

(i) E is modular;
(ii) E has bad additive reduction at p.

Bearing in mind our analysis in the $r_E=0$ case, we formulate a Main Conjecture for elliptic curves with bad additive reduction. We then conjecture a relationship between the order of vanishing of our p-adic L-function and the analytic rank r_E of E. Furthermore, assuming the existence of a non-degenerate p-adic height pairing on E, we make a p-adic Birch and Swinnerton–Dyer type conjecture about the leading term.

Define the ℓ_p-invariant of E by

$$\ell_p(E) := \begin{cases} \dfrac{\#\mathfrak{F}(\mathbb{F}_p)\#\mathfrak{R}E(\mathbb{Q}_p)}{[E(\mathbb{Q}_p)\colon E_0(\mathbb{Q}_p)]} & \text{if } E \text{ has potential good ordinary} \\ & \text{reduction and satisfies}(G), \\ \dfrac{1}{[E(\mathbb{Q}_p)\colon E_0(\mathbb{Q}_p)]} & \text{if } E \text{ satisfies}(M). \end{cases}$$

Of course if $p > 3$ then $c_p = [E(\mathbb{Q}_p)\colon E_0(\mathbb{Q}_p)]$ is a p-adic unit anyway.

Recall that Λ was the Iwasawa algebra of Γ. We identify Λ with the power series ring $\mathbb{Z}_p[\![T]\!]$ via the topological isomorphism $\gamma \mapsto 1 + T$.

MAIN CONJECTURE. *Assume that E is potentially ordinary at p and satisfies hypothesis (G) or (M). Then $\mathfrak{X}_\infty = \mathfrak{S}(E/\mathbb{Q}_\infty)^\wedge$ is Λ-torsion. If $\mathcal{G}_E$ denotes its characteristic power series, then*

$$\lambda(T)\mathcal{G}_E(T) = \ell_p(E)\int_{g\in\Gamma}(1+T)^{\mathfrak{x}_p(g)}\,\mathrm{d}\mu_E,$$

for some $\lambda \in \Lambda^\times$, with $\int_{g\in\Gamma}(1+T)^{\mathfrak{x}_p(g)}\,\mathrm{d}\mu_E$ the p-adic Mellin transform of μ_E.

Defining the p-adic height pairing is more difficult than in the semi-stable case. Assume that K is a Galois extension of $\mathbb{Q}$ where E has good or multiplicative reduction at all primes above p. If $\langle\cdot,\cdot\rangle_K$ denotes the analytic p-adic height pairing on $E(K)\times E(K)$, then define $\langle\cdot,\cdot\rangle_{\mathbb{Q}}\colon E(\mathbb{Q})\times E(\mathbb{Q}) \to \mathbb{Q}_p$ by

$$\langle P, Q\rangle_{\mathbb{Q}} := \frac{1}{[K:\mathbb{Q}]}\langle P, Q\rangle_K\,,$$

for all $P, Q \in E(\mathbb{Q})$. This pairing is well-defined regardless of how we vary the field K [Jon]. Denote the p-adic regulator associated to this height pairing by $\mathrm{Reg}_p(E)$, so that

$$\mathrm{Reg}_p(E) := \det(\langle P_i, P_j\rangle_{\mathbb{Q}})_{1\leqslant i,j\leqslant r_E},$$

where $\{P_i | 1 \leqslant i \leqslant r_E\}$ form a linearly independent basis for the free part of $E(\mathbb{Q})$.

BS-D(p) CONJECTURE. *Assume that E satisfies either (G) or (M), so that $\mathbf{L}_p(E,\cdot)$ is defined.*

(i) *The order of vanishing of $\mathbf{L}_p(E,\cdot)$ should be given by*

$$\mathrm{order}_{s=0}\mathbf{L}_p(E, \langle x\rangle^s) = r_E,$$

where r_E is the order of the zero of the Hasse–Weil L-series of E.

https://doi.org/10.1023/A:1000408925932 Published online by Cambridge University Press

(ii) *The leading term of* $\mathbf{L}_p(E,\cdot)$ *should satisfy the equivalence*

$$\frac{1}{r_E!}\frac{\mathrm{d}^{r_E}}{\mathrm{d}s^{r_E}}\mathbf{L}_p(E,\langle x\rangle^s)\Big|_{s=0} \sim \frac{\#\text{III}_E(p)\ \prod_\nu c_\nu\ \mathrm{Reg}_p(E)}{\#E(\mathbb{Q})^2_{\mathrm{tors}}}.$$

We remark that in the case of good ordinary reduction there is no ℓ_p-invariant entering into the Main Conjecture, but it instead turns up in the BS-D(p) Conjecture. Indeed this arises because we were forced to interpolate the Galois representations $\Pi\otimes\varepsilon^{-1}$ rather than Π, so we lost information about the reduction of E at p as a side-effect. In fact this information appears in $\mathbf{L}_p(E,\varepsilon)$ rather than $\mathbf{L}_p(E,\mathbf{1})$. When we have good reduction, $\varepsilon=\mathbf{1}$ and the terms coincide.

In the case of split multiplicative reduction, Mazur, Tate and Teitelbaum [MTT] define $\ell_p(E)$ to be $\log_p q_E/\mathrm{ord}_p\, q_E$ where q_E is the Tate period of E. The order of vanishing in this situation should be r_E+1, and the sign in the functional equation changes parity.

For elliptic curves with good ordinary reduction, Perrin–Riou calculates the leading term of $\mathcal{G}_E$ under the assumption that $\mathfrak{X}_\infty$ is Λ-torsion. In our case of bad additive reduction it should be possible to do the same sort of procedure. When $r_E=0$ and E satisfies (G) or (M) this is Proposition 4.

A natural question to ask is what happens if E is potentially supersingular at p. Then $\mathfrak{X}_\infty$ will have Λ-rank 1. On the analytic side, we will have two p-adic L-functions instead of one (c.f. the case of good supersingular reduction), but these power series won't lie in $\Lambda\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ anymore. However it should still be feasible to calculate their leading terms.

More generally, what can we say if E doesn't satisfy (G)? Twisting Π by one-dimensional representations will not give us any inertia invariant subspace at p, so the method presented here cannot cope with these sort of curves. However there would be much interest in finding such a construction.

Acknowledgement

The author thanks John Coates for his advice and encouragement during the preparation of this paper.

References

[AtL] Atkin, A. and Li, W.: Twists of newforms and pseudo-eigenvalues of W-operators, *Invent. Math.* 48 (1978) 221–243.

[Car] Carayol, H.: Courbes de Shimura, formes automorphes et représentations galoisiennes, Thése, Paris 1984.

[CMc] Coates, J. and McConnell, G.: Iwasawa theory of modular elliptic curves of analytic rank at most 1, *Jour. of the London Math. Soc.* 2 (1994) 243–264.

[CoG] Coates, J. and Greenberg, R.: Kummer theory for abelian varieties over local fields, *Invent. Math.* 124 (1996) 129–174.

[Gr1] Greenberg, R.: Iwasawa theory for p-adic representations, in: *Advanced Studies in Pure Math.* 17 (1989) 97–137.

[Gr2] Greenberg, R: Trivial zeros of p-adic L-functions, in: p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture, Contemp. Math. 165 (1994) 149–181.
[GrS] Greenberg, R. and Stevens, G.: p-adic L-functions and p-adic periods of modular forms, *Invent. Math.* 111 (1993) 401–447.
[Ima] Imai, H.: A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_l$-extensions, *Proc. Japan Acad. Ser. A Math. Sci.* 51 (1975) 12–16.
[Jon] Jones, J.: Iwasawa L-functions of elliptic curves with additive reduction, *Journal of Number Theory* 51 (1995) 103–117.
[Kol] Kolyvagin, V.: Euler systems, Grothendieck Festchrift II, *Progress in Mathematics* 87 (Birkhäuser, Boston, 1990) 435–483.
[Man] Manin, J.: Parabolic points and zeta functions of modular curves, *Izv. Akad. Nauk SSSR* (AMS translation) 6 (1972) 19–64.
[MSD] Mazur, B. and Swinnerton–Dyer, P.: Arithmetic of Weil curves, *Invent. Math.* 25 (1974) 1–61.
[MTT] Mazur, B., Tate, J. and Teitelbaum, J.: On p-adic analogues of the conjectures of Birch and Swinnerton–Dyer, *Invent. Math.* 84 (1986) 1–48.
[McC] McCallum, W.: Tate duality and wild ramification, *Math. Ann.* 288 (1990) 553–558.
[Mil] Milne, J. S.: Arithmetic duality theorems, *Perspectives in Mathematics I* (Academic Press, Boston, 1986).
[PeR] Perrin-Riou, B.: Théorie d'Iwasawa et hauteurs p-adiques, *Invent. Math.* 109 (1992) 137–185.
[Ser] Serre, J. P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972) 259–331.
[SeT] Serre, J. P. and Tate, J.: Good reduction of abelian varieties, *Ann. Math.* 88 (1968) 492–517.
[Sch] Schneider, P.: p-adic heights, *Invent. Math.* 69 (1982) 401–409.
[Vis] Vishik, M. M.: Nonarchimedean measures connected with Dirichlet series, *Math. USSR Sbornik* 28 (1976) 216–228.