Available online at www.sciencedirect.com

ScienceDirect

C. R. Acad. Sci. Paris, Ser. I 346 (2008) 819–824

COMPTES RENDUS MATHEMATIQUE

http://france.elsevier.com/direct/CRASS1/

Number Theory/Algebraic Geometry

P-adic weight pairings on pro-Jacobians

Daniel Delbourgo

School of Mathematical Sciences, Monash University, Melbourne, Victoria 3800, Australia

Received 28 March 2008; accepted after revision 10 June 2008

Available online 21 July 2008

Presented by Christophe Soulé

Abstract

Let E denote an elliptic curve defined over the rational numbers. We outline a method of proving the statement

$$L(E,1)\neq 0 \quad \text{implies both} \quad \#E(\mathbb{Q})<\infty \quad \text{and} \quad \#\text{Ш}_E^{\mathrm{ord}}<\infty$$

using properties of p-adic modular forms, i.e. no Iwasawa theory whatsoever. The proof employs a version of Kato's zeta-elements with Λ-adic coefficients. ***To cite this article: D. Delbourgo, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Résumé

Accouplements de poids P-adiques sur les pro-jacobiennes. Soit E une courbe elliptique définie sur le corps des nombres rationnels. Nous proposons une méthode pour démontrer l'énoncé

$$L(E,1)\neq 0 \quad \text{implique} \quad \#E(\mathbb{Q})<\infty \quad \text{et} \quad \#\text{Ш}_E^{\mathrm{ord}}<\infty$$

en utilisant des formes modulaires p-adiques, c'est-à-dire sans la théorie d'Iwasawa. La démonstration utilise une version des éléments-zêta à coefficients Λ-adiques. ***Pour citer cet article : D. Delbourgo, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Version française abrégée

Depuis le travail fondamental de B. Mazur dans les années 1970, les propriétés arithmétiques des $\mathbb{Z}_p$-extensions se sont montrées être un outil puissant dans l'étude des courbes elliptiques. D'un point de vue tout à fait naïf, on peut penser que la théorie d'Iwasawa se réduit à une boîte noire donnant des informations sur le groupe de Selmer. Plus précisément, elle produit des données structurales inestimables le long de la ligne horizontale $k=2$ dans le plan (s,k), où s désignes la variable cyclotomique et k la variable poids.

Nous nous intéressons à la question de la robustesse de la méthode des systèmes d'Euler afin de démontrer des résultats de finitude, sans recours à la théorie d'Iwasawa. Comme défi, nous reproduisons quelques-uns des résultats de Kato et al., en étudiant le comportement des groupes de Selmer larges le long de la ligne verticale $s=1$ (éliminant ainsi la partie du raisonnement qui repose sur la théorie d'Iwasawa).

E-mail address: daniel.delbourgo@sci.monash.edu.au.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2008.06.005

La démonstration comporte deux volets principaux. La première étape consiste à écrire, de manière formelle, un « accouplement des poids » en utilisant des morphismes de degénerescence sur les courbes modulaires. L'étape finale évalue le discriminant du groupe de Mordell–Weil relatif au couplage p-adique précédent. Les propriétés algébriques des éléments-zêta à coefficients dans la représentation de Galois ambiante étayent ces idées (nous n'y ferons toutefois aucune référence dans la suite).

1. Introduction

The arithmetic properties of $\mathbb{Z}_p$-extensions have proven to be a powerful tool in the study of elliptic curves. From a naive perspective, one could interpret Iwasawa theory as a mysterious black-box churning out information about the Selmer group. More accurately, it yields invaluable structural data along the horizontal line $k=2$ in the (s,k)-plane, where s denotes the cyclotomic variable and k the weight.

We are interested in answering the following:

Question. Is the method of Euler systems now sufficiently robust, so that one can prove finiteness results without relying on Iwasawa's theory at all?

As a fun challenge, we shall reproduce *some* of the results of Kato and Rubin by instead studying the behaviour of big Selmer groups along the vertical line $s=1$ (thereby jettisoning the Iwasawa theory part of the argument).

The first step is to write down a formal 'weight pairing' using the degeneration maps on modular curves. The remaining step is to evaluate the discriminant of the Mordell–Weil group with respect to this p-adic pairing.

2. The construction of the pairing

Let $p>3$ be a prime number, and we shall fix some tame level $N \in \mathbb{N}$ coprime to p. For every integer $r \geqslant 1$ we shall set $J_r := \mathrm{Jac}\, X_1(Np^r)_{/\mathbb{Q}}$, and write $\mathrm{Ta}_p(J_r)$ for the Tate module $\varprojlim_m J_r[p^m]$ of each Jacobian. By its very construction in [6–8], the universal p-ordinary Galois representation

$$\rho_\infty^{\mathrm{univ}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}_{\mathcal{R}}(\mathbb{T}_\infty), \qquad \mathrm{rank}_{\mathcal{R}}(\mathbb{T}_\infty) = 2$$

is cut out of the big $G_{\mathbb{Q}}$-lattice $\varprojlim_r \mathrm{Ta}_p(J_r)^{\mathrm{ord}}$ using Hida's N-primitive projector. Here $\mathcal{R}$ denotes the image of the Hecke algebra inside the endomorphisms of $\mathbb{T}_\infty$, so $\mathcal{R}$ is of finite-type over the weight algebra $\Lambda^{\mathrm{wt}} = \mathbb{Z}_p[\![1+p\mathbb{Z}_p]\!]$. Under suitable hypotheses (e.g. residual irreducibility of $\rho_\infty^{\mathrm{univ}}$), one may assume that $\mathbb{T}_\infty$ is $\mathcal{R}$-free.

Remark. In a forthcoming work [2], we consider "refined" Selmer groups

$$\widetilde{H}^1_f\big(\mathbb{Q}, \mathrm{Ta}_p(J_r)^{\mathrm{ord}}\big) \quad \text{and} \quad \overline{H}^1_f\big(\mathbb{Q}, \mathbf{e}^*_{\mathrm{ord}} \cdot \mathrm{Ta}_p({}^{\mathbf{t}}J_r)\big)$$

which have slightly stricter local conditions than their Bloch–Kato cousins. Skipping the precise definitions, we now describe a p-adic pairing linking these two objects.

Suppose that G denotes either $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, or a decomposition group $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$. Then every one-cocycle $x_r \in H^1(G, \mathrm{Ta}_p(J_r)^{\mathrm{ord}})$ corresponds to an extension class

$$0 \longrightarrow \mathrm{Ta}_p(J_r)^{\mathrm{ord}} \longrightarrow \mathfrak{X}_{x_r} \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

of $\mathbb{Z}_p[G]$-modules; here the module $\mathfrak{X}_{x_r} = \mathrm{Ta}_p(J_r)^{\mathrm{ord}} \oplus \mathbb{Z}_p$ except that its Galois action is now twisted by

$$\sigma(t,z) := \big(\sigma(t) + z \times x_r(\sigma), z\big) \quad \text{for all } \sigma \in G \text{ and } (t,z) \in \mathfrak{X}_{x_r}.$$

Applying the functor $\mathrm{Hom}_{\mathbb{Z}_p}(-, \mathbb{Z}_p(1))$, we obtain a dual short exact sequence

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow \mathfrak{X}^*_{x_r}(1) \longrightarrow \mathbf{e}^*_{\mathrm{ord}} \cdot \mathrm{Ta}_p({}^{\mathbf{t}}J_r) \longrightarrow 0.$$

In order to construct canonical lifts, we now consider two maps π_1^* and $\frac{1}{p}\pi_{1*}$. The transition $\pi_1^* : J_r[p^\infty] \to J_{r+1}[p^\infty]$ is itself induced from the dual of the degeneration map $\pi_1 : X_1(Np^{r+1}) \to X_1(Np^r)$; secondly, Nekovář's [9] divided projections $\frac{1}{p}\pi_{1*} : \mathrm{Ta}_p(J_{r+1})^{\mathrm{ord}} \to \mathrm{Ta}_p(J_r)^{\mathrm{ord}}$ satisfy $\frac{1}{p}\pi_{1*} \circ \pi_1^* = [\times p]$.

Assume we are given a compatible system $(x_r)_{r\geqslant 1} \in \varprojlim_{\frac{1}{p}\pi_{1*}} H^1(G, \mathrm{Ta}_p(J_r)^{\mathrm{ord}})$. The following statement is shown in [2, §9.3]:

Lemma 1. *For each $n > 0$, there exist lifted cocycles $x'_{r+n} \in H^1(G, \mathrm{Ta}_p(J_{r+n})^{\mathrm{ord}})$ and a commutative diagram*

$$\begin{array}{ccccccccc} \cdots \longrightarrow & H^1(G, \mathbb{Z}_p(1)) & \longrightarrow & H^1(G, \mathfrak{X}^*_{x'_{r+n}}(1)) & \longrightarrow & H^1(G, \mathbf{e}^*_{\mathrm{ord}} \cdot \mathrm{Ta}_p({}^{\mathbf{t}}J_{r+n})) & \longrightarrow \cdots \\ & \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle \beta_n} & & \downarrow{\scriptstyle (\widehat{\pi_1^*}^n)} & \\ \cdots \longrightarrow & H^1(G, \mathbb{Z}_p(1)) & \longrightarrow & H^1(G, \mathfrak{X}^*_{x_r}(1)) & \longrightarrow & H^1(G, \mathbf{e}^*_{\mathrm{ord}} \cdot \mathrm{Ta}_p({}^{\mathbf{t}}J_r)) & \longrightarrow \cdots \end{array}$$

with the property that if $m \in \mathbb{N}$, for sufficiently large $n \gg m$ the image of the left-most arrow α_n lies in $p^m \cdot H^1(G, \mathbb{Z}_p(1))$.

Furthermore, we showed in [2, §9.3] whenever one has compatible families

$$(x_r)_{r\geqslant 1} \in \varprojlim_{\frac{1}{p}\pi_{1*}} H^1_f(\mathbb{Q}_l, \mathrm{Ta}_p(J_r)^{\mathrm{ord}}) \quad \text{and} \quad (y_r)_{r\geqslant 1} \in \varprojlim_{\widehat{\pi_1^*}} H^1_f(\mathbb{Q}_l, \mathbf{e}^*_{\mathrm{ord}} \cdot \mathrm{Ta}_p({}^{\mathbf{t}}J_r))$$

there exist lifts $\widetilde{y_{r+n}} \in H^1(\mathbb{Q}_l, \mathfrak{X}^*_{x'_{r+n}}(1))$ of the cocycle y_{r+n} for all integers $n > 0$, in other words $\widetilde{y_{r+n}} \mapsto y_{r+n}$ under $H^1(\mathbb{Q}_l, \mathfrak{X}^*_{x'_{r+n}}(1)) \to H^1(\mathbb{Q}_l, \mathbf{e}^*_{\mathrm{ord}} \cdot \mathrm{Ta}_p({}^{\mathbf{t}}J_{r+n}))$.

We now explain how to link together $\widetilde{H}^1_f$ and $\overline{H}^1_f$ via some standard local theory. Let $\chi_p : \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_p^\times$ be the cyclotomic character. For every prime l, one defines the composition

$$\ell_{\varrho,l} : \mathbb{Q}_l^\times \hookrightarrow \mathbb{A}_{\mathbb{Q}}^\times \xrightarrow{\text{rec.map}} \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\log_p \circ \chi_p} \mathbb{Q}_p$$

whose kernel comprises the group of universal norms for the cyclotomic p-extension. Moreover $\ell_{\varrho,l}$ naturally extends to $H^1(\mathbb{Q}_l, \mathbb{Z}_p(1)) \cong \mathbb{Q}_l^\times \widehat{\otimes} \mathbb{Z}_p$ by continuity.

Definition 2. Suppose $x_r \in \widetilde{H}^1_f(\mathbb{Q}, \mathrm{Ta}_p(J_r)^{\mathrm{ord}})$ and $y_r \in \overline{H}^1_f(\mathbb{Q}, \mathbf{e}^*_{\mathrm{ord}} \cdot \mathrm{Ta}_p({}^{\mathbf{t}}J_r))$. If $s_{\mathrm{glob}}(y_r)$ denotes any lift of y_r to $H^1(\mathbb{Q}_{\{Np\}}/\mathbb{Q}, \mathfrak{X}^*_{x_r}(1))$, then define

$$\langle x, y\rangle^{(r)}_{\mathbb{Q},p} := \sum_{\text{primes } l} \lim_{n\to\infty} \ell_{\varrho,l}\big(\mathrm{res}_l(s_{\mathrm{glob}}(y_r)) - \beta_n(\widetilde{\mathrm{res}_l(y_{r+n})})\big).$$

Of course, it is a non-trivial exercise to check that the resultant pairing

$$\langle -, -\rangle^{(r)}_{\mathbb{Q},p} : \widetilde{H}^1_f(\mathbb{Q}, \mathrm{Ta}_p(J_r)^{\mathrm{ord}}) \times \overline{H}^1_f(\mathbb{Q}, \mathbf{e}^*_{\mathrm{ord}} \cdot \mathrm{Ta}_p({}^{\mathbf{t}}J_r)) \longrightarrow \mathbb{Q}_p$$

is well-defined, and independent of the choice of lifts $s_{\mathrm{glob}}(y_r)$ and $\widetilde{\mathrm{res}_l(y_{r+n(m)})}$!

3. Applications to modular elliptic curves

The pairing just described (in Definition 2) has some very nice consequences for the arithmetic of elliptic curves. Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication, which is necessarily modular by the work of Wiles et al. Fix some prime number $p > 3$, and write N for the tame conductor of E over $\mathbb{Q}$. We now make four assumptions:

H1 E has either good ordinary or bad multiplicative reduction at p;
H2 There are no rational cyclic p-isogenies between E and another elliptic curve;
H3 The deformation ring $\mathcal{R}$ at level Np^∞ is isomorphic to Λ^{wt};
H4 The Galois representation $\rho_\infty^{\mathrm{univ}}$ is residually absolutely irreducible.

In fact none of hypotheses **H2**, **H3**, **H4** are really necessary, though they simplify the exposition considerably. For example, condition **H2** is true whenever $p > 37$, and **H3** holds if there is a single p-stabilised newform at level Np.

Remark. Let $A_{\mathbb{T}_\infty} = \mathrm{Hom}_{\mathrm{cont}}(\mathbb{T}_\infty, \mu_{p^\infty})$ be the χ_p-twisted discrete dual of $\mathbb{T}_\infty$. One can then define a Selmer group

$$\mathrm{Sel}_{\mathbb{Q}}(A_{\mathbb{T}_\infty}) \subset H^1\big(\mathbb{Q}_{\{Np\}}/\mathbb{Q}, A_{\mathbb{T}_\infty}\big)$$

consisting of those cocycles which are unramified away from p, and 'crystalline' in the sense of [4] at the prime p (it is easily checked to be of cofinite-type over Λ^{wt}).

Theorem 3. *The big Selmer group* $\mathrm{Sel}_{\mathbb{Q}}(A_{\mathbb{T}_\infty})$ *is a* Λ^{wt}*-cotorsion module.*

The proof uses non-vanishing of the L-values $L(f_k, 1)$ for all integers $k \geqslant 3$, where $f_k \in \mathcal{S}_k(\Gamma_0(Np), \omega^{2-k})$ are the members of the ordinary family lifting the newform associated to $E_{/\mathbb{Q}}$. The finiteness of each of the Bloch–Kato Selmer groups attached to $\{f_k\}_{k\geqslant 3}$ – in tandem with a weight-control theorem of P. Smith's – together implies that the Λ^{wt}-corank of big Selmer is zero.

Question. What is the connection between $\mathrm{Sel}_{\mathbb{Q}}(A_{\mathbb{T}_\infty})$ and the pairings $\langle -, -\rangle^{(r)}_{\mathbb{Q},p}$?

The curve E occurs as a subfactor of Jac $X_1(Np)$, so there are naturally inclusions

$$\mathbb{Q} \otimes \widetilde{H}^1_f\big(\mathbb{Q}, \mathrm{Ta}_p(J_1)^{\mathrm{ord}}\big) \hookleftarrow E(\mathbb{Q}) \mathbin{\widehat{\otimes}} \mathbb{Q}_p \hookrightarrow \mathbb{Q} \otimes \overline{H}^1_f\big(\mathbb{Q}, \mathbf{e}^*_{\mathrm{ord}} \cdot \mathrm{Ta}_p({}^{\mathbf{t}}J_1)\big)$$

under the strict proviso that the p-part of the Tate–Shafarevich group Ш_E is finite. One can then sensibly define

$$\langle -, -\rangle^{\mathrm{wt}}_{\mathbb{Q},p} : E(\mathbb{Q}) \mathbin{\widehat{\otimes}} \mathbb{Q}_p \times E(\mathbb{Q}) \mathbin{\widehat{\otimes}} \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$$

by the simple rule $(x, y) \mapsto p^{-n_1-n_2} \times \langle p^{n_1}x, p^{n_2}y\rangle^{(r)}_{\mathbb{Q},p}|_{r=1}$ for integers $n_1, n_2 \gg 0$.

Further, let us fix an isomorphism $\sigma : \mathbb{Z}_p[\![\Gamma^{\mathrm{wt}}]\!] \xrightarrow{\sim} \mathbb{Z}_p[\![X]\!]$ sending $\gamma_0 \mapsto 1 + X$. Given that $\mathbb{Z}_p[\![X]\!] \otimes_{\Lambda^{\mathrm{wt}},\sigma} \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Sel}_{\mathbb{Q}}(A_{\mathbb{T}_\infty}), \mathbb{Q}/\mathbb{Z})$ is a compact $\mathbb{Z}_p[\![X]\!]$-torsion module, we shall use $\mathbf{L}^{\mathrm{alg}}_p(X)$ to denote its characteristic power series.

Theorem 4. *If* $\langle -, -\rangle^{\mathrm{wt}}_{\mathbb{Q},p}$ *is non-degenerate on the product* $(E(\mathbb{Q}) \times E(\mathbb{Q})) \otimes \mathbb{Q}_p$ *and* $\text{Ш}_E[p^\infty]$ *is a finite group, then* $\mathrm{order}_{X=0}(\mathbf{L}^{\mathrm{alg}}_p(X)) = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{\mathbb{Q}}(E)[p^\infty]$. *Moreover, the quantity*

$$\mathcal{L}^{\mathrm{wt}}_p(E) \times \frac{\#\text{Ш}_E[p^\infty] \times \prod_{l\leqslant\infty}[E(\mathbb{Q}_l) : E_0(\mathbb{Q}_l)]}{\#E(\mathbb{Q})^2_{\mathrm{tors}}} \times \det\langle -, -\rangle^{\mathrm{wt}}_{\mathbb{Q},p}\big|_{E(\mathbb{Q})\times E(\mathbb{Q})}$$

divides into the leading term of $\mathbf{L}^{\mathrm{alg}}_p((1 + p)^{w-2} - 1)$ *at weight* $w = 2$, *where the* $\mathcal{L}^{\mathrm{wt}}$*-invariant equals* $\#\widetilde{E}(\mathbb{F}_p)[p^\infty]$ (*resp. equals* 1) *if* $p \nmid N_E$ (*resp. if* $p \| N_E$).

In fact, the above can be made into an equality after the introduction of certain Λ^{wt}-adic periods, Tamagawa factors, etc. but this takes too long to write out. We refer the reader to the manuscript [2, Thm 9.18] for these details.

The following summarises the main result of the work in progress [3]:

Theorem 5. *There exists a constant* $C = C(p, \mathbb{T}_\infty) \in \mathbb{Z}_p - \{0\}$ *such that*

$$\mathbb{Z}_p\langle\langle w\rangle\rangle \cdot \big(\mathbf{L}^{\mathrm{alg}}_p\big((1 + p)^{w-2} - 1\big)\big) \quad \textit{contains} \quad \mathbb{Z}_p\langle\langle w\rangle\rangle \cdot \big(C(p, \mathbb{T}_\infty) \times \mathbf{L}^{\mathrm{imp}}_p(w)\big)$$

where $\mathbf{L}^{\mathrm{imp}}_p(-)$ *denotes the improved* p*-adic* L*-function of Greenberg–Stevens.*

One should point out that the improved p-adic L-function in [5] interpolates

$$\mathbf{L}^{\mathrm{imp}}_p(k) = (\Lambda^{\mathrm{wt}}\text{-adic period})_k \times (\text{Euler factor})_k \times \frac{L(f_k, 1)}{\Omega^+_{f_k}} \quad \text{for all } k \geqslant 2,$$

and belongs to the affinoid algebra $\mathbb{Q}_p\langle\langle w\rangle\rangle$ of the unit disk. The constant $C(p,\mathbb{T}_\infty)$ à priori depends on the (lack of) surjectivity in the p-adic Galois representation, together with the indices of certain zeta-elements inside étale cohomology.

We proved in [1,2] the restriction map $\mathrm{Sel}_\mathbb{Q}(E)[p^\infty] \xrightarrow{\theta} H^0(\Gamma^{\mathrm{wt}}, \mathrm{Sel}_\mathbb{Q}(A_{\mathbb{T}_\infty}))$ has finite kernel and cokernel, in which case both groups share the same $\mathbb{Z}_p$-corank. Providing our weight pairing $\langle -,-\rangle^{\mathrm{wt}}_{\mathbb{Q},p}$ is non-degenerate, we deduce

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_\mathbb{Q}(E)[p^\infty] = \mathrm{order}_{w=2}\big(\mathbf{L}_p^{\mathrm{alg}}\big((1+p)^{w-2}-1\big)\big) \leqslant \mathrm{order}_{w=2}\big(\mathbf{L}_p^{\mathrm{imp}}(w)\big).$$

On the other hand let's suppose $L(E,1)\neq 0$, in which case one knows $\mathbf{L}_p^{\mathrm{imp}}(2)\neq 0$. The divisibility in Theorem 5 tells us the constant term of $\mathbf{L}_p^{\mathrm{alg}}(X)$ at $X=0$ is non-trivial, in which case the Γ^{wt}-invariants of $\mathrm{Sel}_\mathbb{Q}(A_{\mathbb{T}_\infty})$ must be a finite p-group. The fact $\theta:\mathrm{Sel}_\mathbb{Q}(E)[p^\infty]\to \mathrm{Sel}_\mathbb{Q}(A_{\mathbb{T}_\infty})^{\Gamma^{\mathrm{wt}}}$ is a quasi-isomorphism, then ensures that $E(\mathbb{Q})$ and $\text{Ш}_E[p^\infty]$ are both finite groups.

We conclude if the analytic rank is zero, then the conditions of Theorem 4 apply. Indeed the weight pairing $\langle -,-\rangle^{\mathrm{wt}}_{\mathbb{Q},p}: E(\mathbb{Q})\times E(\mathbb{Q})\to\mathbb{Q}_p$ trivialises in this situation, due to the finiteness of the classical p^∞-Selmer group for E.

Let $\delta_{p,\mathbb{T}_\infty}$ denote the p-adic order of the Λ^{wt}-adic period in $\mathbf{L}_p^{\mathrm{imp}}$ at weight two.

Conjecture 6.

(a) *At all bar finitely many ordinary $p\geqslant 5$, we have $\delta_{p,\mathbb{T}_\infty}=0$;*
(b) *There exists a constant $C_E^{\mathrm{glob}}\in\mathbb{Z}$ such that $\mathrm{ord}_p(C(p,\mathbb{T}_\infty))\leqslant \mathrm{ord}_p(C_E^{\mathrm{glob}})$ for all good ordinary or bad multiplicative primes $p\geqslant 5$.*

The first statement would follow if one could establish the freeness of the universal p-adic modular symbol (at almost all p), since the Λ^{wt}-adic periods would be units. Hopefully the second claim can be proven via a more careful study of the variation in $C(p,\mathbb{T}_\infty)$ over the Hida families occurring at the different primes p (as above).

Taking Theorems 4 and 5 in tandem, if $L(E,1)\neq 0$ then

$$\mathrm{ord}_p\big(\text{Ш}_E[p^\infty]\big)\leqslant \mathrm{ord}_p C(p,\mathbb{T}_\infty)+\delta_{p,\mathbb{T}_\infty}+\mathrm{ord}_p\left(\frac{\#E(\mathbb{Q})^2}{\mathrm{Tam}_\mathbb{Q}(E)}\times\frac{L(E,1)}{\Omega_E^+}\right).$$

If Conjecture 6 is to be believed, then for almost all the ordinary primes $p>3$ the right-hand side of the above inequality is equal to zero; it would therefore follow

$$\#\big(\text{Ш}_E^{\mathrm{ord}}\big)<\infty \quad \text{where } \text{Ш}_E^{\mathrm{ord}} := \prod_{p>3 \text{ with } a_p(E)\neq 0} \text{Ш}_E[p^\infty].$$

N.B. At no point does this argument require the Iwasawa theory of elliptic curves.

Acknowledgements

The author thanks Ivan Fesenko for his left of field insights, and is grateful to Kais Hamza for his French translation. He also thanks the referee for spotting a possible flaw in an earlier version of Lemma 1.

References

[1] D. Delbourgo, Λ-adic Euler characteristics of elliptic curves, Documenta Math. volume in honour of J.H. Coates' 60th birthday (2006) 301–323.
[2] D. Delbourgo, Elliptic Curves and Big Galois Representations, London Mathematical Society Lecture Note Series, vol. 356, Cambridge University Press, 2008.
[3] D. Delbourgo, On the divisibility of Selmer into the improved p-adic L-function, in preparation.
[4] D. Delbourgo, P. Smith, Kummer theory for big Galois representations, Math. Proc. Cambridge Philos. Soc. 142 (2007) 205–217.
[5] R. Greenberg, G. Stevens, p-adic L-functions and p-adic periods of modular forms, Invent. Math. 111 (1993) 401–447.

[6] H. Hida, Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, Invent. Math. 85 (1986) 545–613.
[7] H. Hida, Iwasawa modules attached to congruences of cusp forms, Ann. Sci. École Norm. Sup. (4) 19 (1986) 231–273.
[8] H. Hida, A p-adic measure attached to the zeta-functions associated with two elliptic modular forms I, Invent. Math. 79 (1985) 159–195.
[9] J. Nekovář, A. Plater, On the parity of ranks of Selmer groups, Asian J. Math. 4 (2) (2000) 437–497.