Links Between Cyclotomic and GL_2 Iwasawa Theory

John Coates, Peter Schneider, Ramdorai Sujatha

Received: September 26, 2002
Revised: February 26, 2003

Vying with the light
Of the heaven-coursing sun,
Oh, let me search,
That I find it once again,
The Way that was so pure.

Dedicated to Kazuya Kato

Abstract. We study, in the case of ordinary primes, some connections between the GL_2 and cyclotomic Iwasawa theory of an elliptic curve without complex multiplication.

2000 Mathematics Subject Classification: 11G05; 11R23.
Keywords and Phrases: Iwasawa theory, elliptic curves.

1 Introduction

Let F be a finite extension of $\mathbb{Q}$, E an elliptic curve defined over F, and p a prime number such that E has good ordinary reduction at all primes v of F dividing p. Let F^{cyc} denote the cyclotomic $\mathbb{Z}_p$-extension of F, and put $\Gamma = G(F^{cyc}/F)$. A very well known conjecture due to Mazur [15] asserts that the dual of the Selmer group of E over F^{cyc} is a torsion module over the Iwasawa algebra $\Lambda(\Gamma)$ of Γ (the best result in the direction of this conjecture is due to Kato [13], who proves it when E is defined over $\mathbb{Q}$, and F is an abelian

extension of $\mathbb{Q}$). Now let F_∞ denote a Galois extension of F containing F^{cyc} whose Galois group G over F is a p-adic Lie group of dimension > 1. This paper will make some modest observations about the following general problem. To what extent, and in what way, does the arithmetic of E over F^{cyc} influence the arithmetic of E over the much larger p-adic Lie extension F_∞? For example, assuming that G is pro-p and has no element of order p, and that Mazur's conjecture is true for E over F^{cyc}, can one deduce that the dual of the Selmer group of E over F_∞ is a torsion module over the Iwasawa algebra $\Lambda(G)$ of G? In their paper [12] in this volume, Hachimori and Venjakob prove the surprising result that the answer is yes for a wide class of non-abelian extensions F_∞ of F in which G has dimension 2. In the first two sections of this paper, we study the different case in which $F_\infty = F(E_{p^\infty})$ is the field obtained by adjoining to F the coordinates of all p-power division points on E. We assume that E has no complex multiplication, so that G is open in $GL_2(\mathbb{Z}_p)$ by a well known theorem of Serre. In [4], it was shown that, in this case, the dual of the Selmer group of E over F_∞ is $\Lambda(G)$-torsion provided Mazur's conjecture for E over F^{cyc} is true, and, in addition, the μ-invariant of the dual of Selmer of E over F^{cyc} is zero. Although we can do no better than this result as far as showing the dual of E over F_∞ is $\Lambda(G)$-torsion, we do prove some related results which were not known earlier. The main result of this paper is Theorem 3.1, relating the truncated G-Euler characteristic of the Selmer group of E over F_∞ with the Γ-Euler characteristic of E over F^{cyc} (only a slightly weaker form of this result was shown in [4] under the more restrictive assumption that the Selmer group of E over F is finite). We also establish a relation between the μ-invariant of the dual of the Selmer group of E over F_∞ and the μ-invariant of the dual of the Selmer group of E overF^{cyc} (see Propositions 3.12 and 3.13). The proof of this relationship between μ-invariants led us to study in §4 a new invariant attached to a wide class of finitely generated torsion modules for the Iwasawa algebra of any pro-p p-adic Lie group G, which has no element of order p, and which has a closed normal subgroup H such that $\Gamma = G/H$ is isomorphic to $\mathbb{Z}_p$. This new invariant is a refinement of the G-Euler characteristic of such modules, and, in particular, we investigate its behaviour on pseudo-null modules.
Added in proof: Since this paper was written, O. Venjakob, in his Heidelberg Habilitation thesis, has made use of our invariant to prove the existence of an analogue of the characteristic power series of commutative Iwasawa theory for any module in the category $\mathfrak{M}_H(G)$ which is defined at the beginning of §4.

Notation

Let p be a fixed prime number. If A is an abelian group, $A(p)$ will always denote its p-primary subgroup. Throughout G will denote a compact p-adic Lie group, and we write

$$\Lambda(G) = \varprojlim_{U} \mathbb{Z}_p\,[G/U],$$

where U runs over all open normal subgroups of G, for the Iwasawa algebra of G. All modules we consider will be left modules for $\Lambda(G)$. If W is a compact $\Lambda(G)$-module, we write $\widehat{W} = \mathrm{Hom}_{\mathbb{Z}_p}(W, \mathbb{Q}_p/\mathbb{Z}_p)$ for its Pontrjagin dual. It is a discrete p-primary abelian group, endowed with its natural structure of a left $\Lambda(G)$-module. We shall write $H_i(G, W)$ for the homology groups of W. If W is a finitely generated $\Lambda(G)$-module, then it is well known that, for each $i \geqslant 0$, $H_i(G, W)$ has as its Pontrjagin dual the cohomology group $H^i(G, \widehat{W})$, which is defined with continuous cochains.

When K is a field, $\overline{K}$ will denote a fixed separable closure of K, and G_K will denote the Galois group of $\overline{K}$ over K. We write $G(L/K)$ for the Galois group of a Galois extension L over K. If A is a discrete G_K-module, $H^i(K, A)$ will denote the usual Galois cohomology groups. Throughout, F will denote a finite extension of $\mathbb{Q}$, and E an elliptic curve defined over F, which will always be assumed to have $\mathrm{End}_{\overline{F}}(E) = \mathbb{Z}$. We impose throughout sections 2 and 3 of this paper the hypothesis that E has good ordinary reduction at all primes v of F dividing p. We let S denote any fixed set of places of F such that S contains all primes of F dividing p, and all primes of F where E has bad reduction. We write F_S for the maximal extension of F which is unramified outside S and the archimedean primes of F. For each intermediate field L with $F \subset L \subset F_S$, we put $G_S(L) = G(F_S/L)$. Finally, we shall always assume that our prime p satisfies $p \geq 5$.

2 The fundamental exact sequence

We recall that we always assume that E has good ordinary reduction at all primes v of F dividing p. Let F^{cyc} denote the cyclotomic $\mathbb{Z}_p$-extension of F, and put $\Gamma = G(F^{\mathrm{cyc}}/F)$. By a basic conjecture of Mazur [15], the dual of the Selmer group of E over F^{cyc} is a torsion $\Lambda(\Gamma)$-module. The aim of this section is to analyse the consequences of this conjecture for the study of the Selmer group of E over the field generated by all the p-power division points on E.

If L is any intermediate field with $F \subset L \subset F_S$, we recall that the Selmer group $\mathcal{S}(E/L)$ is defined by

$$\mathcal{S}(E/L) = \mathrm{Ker}(H^1(L, E_{p^\infty}) \to \prod_w H^1(L_w, E(\overline{L}_w))),$$

where E_{p^∞} denotes the Galois module of all p-power division points on E. Here w runs over all non-archimedean valuations of L, and L_w denotes the union of the completions at w of all finite extensions of $\mathbb{Q}$ contained in L. As usual, it is more convenient to view $\mathcal{S}(E/L)$ as a subgroup of $H^1(G_S(L), E_{p^\infty})$. For $v \in S$, we define $J_v(L) = \varinjlim J_v(K)$, where the inductive limit is taken with respect to the restriction maps as K ranges over all finite extensions of F contained in L, and where, for such a finite extension K of F, we define

$$J_v(K) = \bigoplus_{w|v} H^1(K_w, E(\overline{K}_w))(p).$$

Since $L \subset F_S$, we then have $\mathcal{S}(E/L) = \mathrm{Ker}\ \lambda_S(L)$, where

$$\lambda_S(L) \ :\ H^1(G_S(L), E_{p^\infty}) \to \bigoplus_{v\in S} J_v(L) \tag{1}$$

denotes the evident localization map. We shall see that, when L is an infinite extension of F, the question of the surjectivity of $\lambda_S(L)$ is a basic one. We write

$$X(E/L) = \mathrm{Hom}(\mathcal{S}(E/L), \mathbb{Q}_p/\mathbb{Z}_p) \tag{2}$$

for the compact Pontrjagin dual of the discrete module $\mathcal{S}(E/L)$. We shall be primarily concerned with the case in which L is Galois over F, in which case both $\mathcal{S}(E/L)$ and $X(E/L)$ have a natural left action of $G(L/F)$, which extends to a left action of the whole Iwasawa algebra $\Lambda(G(L/F))$. It is easy to see that $X(E/L)$ is a finitely generated $\Lambda(G(L/F))$-module.
We are going to exploit the following well-known lemma (see [17, Lemmas 4 and 5] and also [12, §7] for an account of the proof in a more general setting).

Lemma 2.1 *Assume that $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. Then the localization map $\lambda_S(F^{\mathrm{cyc}})$ is surjective, i.e. we have the exact sequence of Γ-modules*

$$0 \to \mathcal{S}(E/F^{\mathrm{cyc}}) \to H^1(G_S(F^{\mathrm{cyc}}), E_{p^\infty}) \xrightarrow{\lambda_S(F^{\mathrm{cyc}})} \bigoplus_{v\in S} J_v(F^{\mathrm{cyc}}) \to 0. \tag{3}$$

Moreover, we also have

$$H^2(G_S(F^{\mathrm{cyc}}), E_{p^\infty}) = 0. \tag{4}$$

We now consider the field $F_\infty = F(E_{p^\infty})$, which always contains F^{cyc} by the Weil pairing. We write

$$G = G(F_\infty/F), \quad H = G(F_\infty/F^{\mathrm{cyc}}), \tag{5}$$

so that $G/H = \Gamma$. By Serre's theorem, G is an open subgroup of $\mathrm{Aut}(T_p(E)) = GL_2(\mathbb{Z}_p)$, where, as usual, $T_p(E) = \varprojlim E_{p^n}$. The following is the principal result of this section.

Theorem 2.2 *Assume that (i) $p \geq 5$, (ii) E has good ordinary reduction at all primes v of F dividing p, and (iii) $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. Then we have the exact sequence*

$$0 \to \mathcal{S}(E/F_\infty)^G \to W_\infty^G \to \bigoplus_{v\in S} J_v(F_\infty)^G \to H^1(G, \mathcal{S}(E/F_\infty)) \to H^1(G, W_\infty) \to 0, \tag{6}$$

where $W_\infty = H^1(G_S(F_\infty), E_{p^\infty})$.

In fact, we expect $\lambda_S(F_\infty)$ to be surjective for all prime numbers p. If $p \geq 5$, it is shown in [4] that $H^i(G, W_\infty) = 0$ for all $i \geq 2$, and that $H^i(G, J_v(F_\infty)) = 0$ for all $i \geq 1$ and all $v \in S$. Thus if $\lambda_S(F_\infty)$ is surjective for a prime number $p \geq 5$, the exact sequence (6) follows. However, what is surprising about Theorem 2.2 is that we can establish it without knowing the surjectivity of $\lambda_S(F_\infty)$ (in our present state of knowledge [4], to prove the surjectivity of $\lambda_S(F_\infty)$ we must assume hypotheses *(i)* and *(ii)* of Theorem 2.2, replace *(iii)* by the stronger hypothesis that $X(E/F^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module, and, in addition, assume that G is pro-p). Finally, we mention that if hypotheses *(i)* and *(ii)* of Theorem 2.2 hold, and if also G is pro-p, then $X(E/F_\infty)$ is $\Lambda(G)$-torsion if and only if $\lambda_S(F_\infty)$ is surjective.
We now proceed to establish Theorem 2.2 via a series of lemmas. For these lemmas, we assume that the hypotheses *(i), (ii)* and *(iii)* of Theorem 2.2 are valid.

Lemma 2.3 *We have the exact sequence*

$$0 \to \mathcal{S}(E/F_\infty)^H \to H^1(G_S(F_\infty), E_{p^\infty})^H \overset{\rho_S(F_\infty)}{\to} \bigoplus_{v\in S} J_v(F_\infty)^H \to 0,$$

where $\rho_S(F_\infty)$ is induced by the localization map $\lambda_S(F_\infty)$.

Proof All we have to show is that $\rho_S(F_\infty)$ is surjective. We clearly have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{S}(E/F_\infty)^H \arrow[r] & H^1(G_S(F_\infty), E_{p^\infty})^H \arrow[r, "\rho_S(F_\infty)"'] & \bigoplus_{v\in S} J_v(F_\infty)^H & \\
0 \arrow[r] & \mathcal{S}(E/F^{\mathrm{cyc}}) \arrow[r] \arrow[u] & H^1(G_S(F^{\mathrm{cyc}}), E_{p^\infty}) \arrow[r, "\lambda_S(F^{\mathrm{cyc}})"'] \arrow[u] & \bigoplus_{v\in S} J_v(F^{\mathrm{cyc}}) \arrow[r] \arrow[u, "\gamma_S(F^{\mathrm{cyc}})"'] & 0,
\end{tikzcd}$$

where $\gamma_S(F^{\mathrm{cyc}})$ is induced by restriction, and where the surjectivity of $\lambda_S(F^{\mathrm{cyc}})$ is given by Lemma 2.1, thanks to our assumption that $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. Hence it suffices to prove the surjectivity of $\gamma_S(F^{\mathrm{cyc}})$. This is essentially contained in the proof of [4, Lemma 6.7], but we give the detailed proof as it is only shown there that $\gamma_S(F^{\mathrm{cyc}})$ has finite cokernel. As is well known and easy to see, there are only finitely many primes of F^{cyc} above each non-archimedean prime of F. Hence we have

$$\mathrm{Coker}(\gamma_S(F^{\mathrm{cyc}})) = \bigoplus_{w|S} \mathrm{Coker}(\gamma_w(F^{\mathrm{cyc}})),$$

where w runs over all primes of F^{cyc} lying above primes in S, and where, as $H^2(F_{\infty,w}, E) = 0$,

$$\mathrm{Coker}(\gamma_w(F^{\mathrm{cyc}})) = H^2(\Omega_w, E(F_{\infty,w}))(p);$$

here Ω_w denotes the decomposition group in H of some fixed prime of F_∞ lying above w. Now Ω_w is a p-adic Lie group with no elements of order p as $p \geq 5$, and so Ω_w has finite p-cohomological dimension equal to its dimension as a p-adic Lie group. Moreover, a simple local analysis (see [2] or [4]) shows that Ω_w has dimension at most 1 when w does not divide p, and dimension 2 when w does divide p. We claim that we always have

$$H^2(\Omega_w, E_{p^\infty}) = 0. \tag{7}$$

This is plain from the above remarks when v does not divide p. When v divides p, Ω_w has p-cohomological dimension equal to 2, and, thus $H^2(\Omega_w, E_{p^\infty})$ is a divisible group. On the other hand, as E has good reduction at w, it is well-known (see [4] for a direct argument, or [8] for a general result) that $H^2(\Omega_w, E_{p^\infty})$ is finite, whence (7) follows. We now finish the proof using (7). Assume first that w does not divide p. Then (see [2, Lemma 3.7]) we have

$$\mathrm{Coker}(\gamma_w(F^{\mathrm{cyc}})) = H^2(\Omega_w, E_{p^\infty}),$$

and so we obtain the surjectivity of $\gamma_w(F^{\mathrm{cyc}})$ from (7). Suppose now that w does divide p. Then it follows from the results of [3] that

$$\mathrm{Coker}(\gamma_w(F^{\mathrm{cyc}})) = H^2(\Omega_w, \tilde{E}_{w,p^\infty}),$$

where $\tilde{E}_{w,p^\infty}$ denotes the image of E_{p^∞} under reduction modulo w. But as Ω_w has p-cohomological dimension equal to 2, the vanishing of $H^2(\Omega_w, \tilde{E}_{w,p^\infty})$ is an immediate consequence of (7). This completes the proof of Lemma 2.3. $\square$

Lemma 2.4 *We have $H^i(H, H^1(G_S(F_\infty), E_{p^\infty})) = 0$ for all $i \geq 1$.*

Proof We have

$$H^m(G_S(F_\infty), E_{p^\infty}) = 0, \quad (m \geq 2). \tag{8}$$

Indeed, (8) is obvious for $m > 2$ as $G_S(F_\infty)$ has p-cohomological dimension equal to 2, and it is a consequence of Iwasawa's work on the cyclotomic $\mathbb{Z}_p$-extension of number fields when $m = 2$ (see [2, Theorem 2.10]). In view of (8), the Hochschild-Serre spectral sequence gives

$$H^{i+1}(G_S(F^{\mathrm{cyc}}), E_{p^\infty}) \to H^i(H, H^1(G_S(F_\infty), E_{p^\infty})) \to H^{i+2}(H, E_{p^\infty}). \tag{9}$$

The group on the left of (9) vanishes (for $i = 1$, we use Lemma 2.1). Now H has p-cohomological dimension 3, and so $H^{i+2}(H, E_{p^\infty})$ is zero for $i > 1$, and divisible for $i = 1$. On the other hand, it is known [6] that $H^k(H, E_{p^\infty})$ is finite for all $k \geq 0$, whence, in particular, we must have $H^3(H, E_{p^\infty}) = 0$. Thus (9) gives Lemma 2.4 as required. $\square$

Lemma 2.5 *We have $H^1(H, \mathcal{S}(E/F_\infty)) = 0$.*

PROOF Let A_∞ denote the image of $\lambda_S(F_\infty)$. Hence, in view of Lemma 2.4 with $i = 1$, we have the exact sequence

$$0 \to \mathcal{S}(E/F_\infty)^H \to H^1(G_S(F_\infty), E_{p^\infty})^H \to A_\infty^H \to H^1(H, \mathcal{S}(E/F_\infty)) \to 0.$$

But the surjectivity of $\rho_S(F_\infty)$ in Lemma 2.3 shows that

$$A_\infty^H = \bigoplus_{v \in S} J_v(F_\infty)^H,$$

whence it is clear that $H^1(H, \mathcal{S}(E/F_\infty)) = 0$, as required. □

REMARK 2.6 By a similar argument to that given in the proof of [2, Theorem 3.2], we see that $H^i(H, J_v(F_\infty)) = 0$ for all $i \geq 1$, for all primes $p \geq 5$, and all finite places v of F. Thus we deduce from Lemma 2.4 that the surjectivity of $\lambda_S(F_\infty)$ implies that $H^i(H, \mathcal{S}(E/F_\infty)) = 0$ for all $i \geq 1$. Unfortunately, we cannot at present prove the surjectivity of $\lambda_S(F_\infty)$ assuming only the hypotheses *(i), (ii)* and *(iii)* of Theorem 2.2.

LEMMA 2.7 *We have isomorphisms*

$$H^1(\Gamma, H^1(G_S(F_\infty), E_{p^\infty})^H) \simeq H^1(G, H^1(G_S(F_\infty), E_{p^\infty}))$$
$$H^1(\Gamma, \mathcal{S}(E/F_\infty)^H) \simeq H^1(G, \mathcal{S}(E/F_\infty)).$$

PROOF This is immediate from Lemmas 2.4 and 2.5, and the usual inflation-restriction exact sequence for H^1. □

LEMMA 2.8 *We have* $H^1(\Gamma, \bigoplus_{v \in S} J_v(F_\infty)^H) = 0$.

PROOF To simplify notation, let us put $K = F^{\mathrm{cyc}}$. Since the map

$$\gamma_S(K) \;:\; \bigoplus_{v \in S} J_v(K) \to \bigoplus_{v \in S} J_v(F_\infty)^H$$

is surjective by Lemma 2.3, and since Γ has p-cohomological dimension equal to 1, it suffices to show that

$$H^1(\Gamma, \bigoplus_{v \in S} J_v(K)) = 0. \tag{10}$$

It is well-known that (10) is valid, but we sketch a proof now for completeness. For each place v of F, let w be a fixed place of K above v, and let $\Gamma_v \subset \Gamma$ denote the decomposition group of w over v, which is an open subgroup of Γ. As usual, it follows from Shapiro's lemma that

$$H^1(\Gamma, J_v(K)) \simeq H^1(\Gamma_v, H^1(K_w, E)(p)),$$

and so we must prove that

$$H^1(\Gamma_v, H^1(K_w, E)(p)) = 0. \tag{11}$$

We begin by noting that, for each algebraic extension L of F_v, we have

$$H^2(L, E_{p^\infty}) = 0. \tag{12}$$

When L is a finite extension of F_v, Tate local duality shows that $H^2(L, E_{p^\infty})$ is dual to $H^0(L, T_p(E))$, and this latter group is zero because the torsion subgroup of $E(L)$ is finite. Clearly (12) is now true for all algebraic extensions L of F_v by passing to the inductive limit over all finite extensions of F_v contained in L. Suppose now that v does not divide p. Then

$$H^1(K_w, E_{p^\infty}) \simeq H^1(K_w, E)(p).$$

In view of (12), the Hochschild-Serre spectral sequence for K_w/F_v shows that we have the exact sequence

$$H^2(F_v, E_{p^\infty}) \to H^1(\Gamma_v, H^1(K_w, E_{p^\infty})) \to H^3(\Gamma_v, E_{p^\infty}(K_v)).$$

But the group on the left is zero again by (12), and the group on the right is zero because Γ_v has p-cohomological dimension equal to 1. This proves (11) in this case. Suppose next that v divides p. As K_w is a deeply ramified p-adic field, it follows from [3] that

$$H^1(K_w, E)(p) \simeq H^1(K_w, \tilde{E}_{w,p^\infty}),$$

where $\tilde{E}_{w,p^\infty}$ denotes the image of E_{p^∞} under reduction modulo w. As $\tilde{E}_{w,p^\infty}$ is a quotient of E_{p^∞}, and as the Galois group of $\overline{F_v}$ over K_w has p-cohomological dimension at most 2, we conclude from (12) that

$$H^2(K_w, \tilde{E}_{w,p^\infty}) = 0. \tag{13}$$

In fact, the Galois group of $\overline{F}_v$ over K_w has p-cohomological dimension 1, so that (13) also follows directly from this fact. In view of (13), the Hochschild-Serre spectral sequence for K_w/F_v yields the exact sequence

$$H^2(F_v, \tilde{E}_{w,p^\infty}) \to H^1(\Gamma_v, H^1(K_w, \tilde{E}_{w,p^\infty}) \to H^3(\Gamma_v, \tilde{E}_{w,p^\infty}).$$

The group on the right is zero because Γ_v has p-cohomological dimension equal to 1. By Tate local duality, the dual of the group on the left is $H^0(F_v, T_p(\hat{E}_w))$, where $T_p(\hat{E}_w) \varprojlim \hat{E}_{w,p^n}$, and $\hat{E}_{w,p^n}$ denotes the kernel of multiplication by p^n on the formal group $\hat{E}_w$ of E at w. But again $H^0(F_v, T_p(\hat{E}_w)) = 0$ because the torsion subgroup of $E(F_v)$ is finite, and so we have proven (11) in this case. This completes the proof of Lemma 2.8. □

Proof of Theorem 2.2 We can now prove Theorem 2.2. Put $W_\infty = H^1(G_S(F_\infty), E_{p^\infty})$. Taking Γ-cohomology of the exact sequence of Lemma 2.3, and using Lemma 2.8, we obtain the long exact sequence

$$0 \to \mathcal{S}(E/F_\infty)^G \to W_\infty^G \to \bigoplus_{v \in S} J_v(F_\infty)^G \to$$
$$\to H^1(\Gamma, \mathcal{S}(E/F_\infty)^H) \to H^1(\Gamma, W_\infty^H) \to 0.$$

Theorem 2.2 now follows immediately from Lemma 2.7. $\square$

The following is a curious consequence of the arguments in this section, and we have included it because a parallel result has a striking application to the work of Hachimori and Venjakob [12].

Proposition 2.9 *Assume that (i) $p \geq 5$, (ii) E has good ordinary reduction at all primes v of F dividing p, (iii) $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$ -torsion, and (iv) G is pro-p. Then $X(E/F_\infty)$ is $\Lambda(G)$-torsion if and only if $H^2(H, \mathcal{S}(E/F_\infty)) = 0$.*

Proof Since G is pro-p, it is well-known (see for example, Theorem 4.12 of [2]) that $X(E/F_\infty)$ is $\Lambda(G)$-torsion if and only if $\lambda_S(F_\infty)$ is surjective. We have already observed in Remark 2.6 that the surjectivity of $\lambda_S(F_\infty)$ implies that $H^i(H, \mathcal{S}(E/F_\infty)) = 0$ for all $i \geq 1$. Conversely, assume that $H^2(H, \mathcal{S}(E/F_\infty)) = 0$. As in the proof of Lemma 2.5, let A_∞ denote the image of $\lambda_S(F_\infty)$. Taking the H-cohomology of the exact sequence

$$0 \to \mathcal{S}(E/F_\infty) \to H^1(G_S(F_\infty), E_{p^\infty}) \to A_\infty \to 0,$$

we conclude from Lemma 2.4 that

$$H^1(H, A_\infty) \simeq H^2(H, \mathcal{S}(E/F_\infty)).$$

Hence our hypothesis implies that $H^1(H, A_\infty) = 0$. Now let $B_\infty = \mathrm{Coker}(\lambda_S(F_\infty))$. Taking H-cohomology of the exact sequence

$$0 \to A_\infty \to \bigoplus_{v \in S} J_v(F_\infty) \to B_\infty \to 0,$$

and using Lemma 2.3 and the fact mentioned in Remark 2.6 that $H^1(H, J_v(F_\infty)) = 0$ for all $v \in S$, we conclude that

$$B_\infty^H = H^1(H, A_\infty).$$

Hence $B_\infty^H = 0$. But as H is pro-p and B_∞ is a p-primary discrete H-module, it follows that $B_\infty = 0$. Thus $\lambda_S(F_\infty)$ is surjective, and this completes the proof of Proposition 2.5. $\square$

We conclude this section by proving a result relating the so-called μ-invariants of the $\Lambda(G)$-module $X(E/F_\infty)$ and the $\Lambda(\Gamma)$-module $X(E/F^{\mathrm{cyc}})$. Let us assume for the rest of this section that G is pro-p. Let W be any finitely generated

$\Lambda(G)$-module. We write $W(p)$ for the submodule of all elements of W which are annihilated by some power of p, and we then define

$$W_f = W/W(p). \tag{14}$$

We recall that the homology groups $H_i(G, W)$ are the Pontrjagin duals of the cohomology groups $H^i(G, \widehat{W})$, where $\widehat{W} = \mathrm{Hom}_{\mathbb{Z}_p}(W, \mathbb{Q}_p/\mathbb{Z}_p)$ is the discrete p-primary Pontrjagin dual of W (see [11]). As is explained in [11], the $H^i(G, W)$ are finitely generated $\mathbb{Z}_p$-modules, and thus the $H_i(G, W(p))$ are finite groups for all $i \geq 0$. Now the μ-invariant of W, which we shall denote by $\mu_G(W)$, can be defined in various equivalent fashions (see [22], [11]) in terms of the structure theory of the $\Lambda(G)$-module $W(p)$. However, for us it will be more convenient to use the description of $\mu_G(W)$ in terms of the Euler characteristics which is proven in [11], namely

$$p^{\mu_G(W)} = \prod_{i \geq 0} \#(H_i(G, W(p)))^{(-1)^i}. \tag{15}$$

As usual, we shall denote the right hand side of (15) by $\chi(G, W(p))$. We shall use the analogous notation and results for the μ-invariants of finitely generated $\Lambda(\Gamma)$-modules. For the remainder of this section, we always assume the hypotheses (i)-(iv) of Proposition 2.9.

Lemma 2.10 *Both $H_0(H, X(E/F_\infty)_f)$ and $H_1(H, X(E/F_\infty)_f)$ are finitely generated torsion $\Lambda(\Gamma)$-modules, and $H_1(H, X(E/F_\infty)_f)$ is annihilated by some power of p.*

Proof For simplicity, put $X = X(E/F_\infty)$. By duality, the restriction map on cohomology induces a Γ-homomorphism

$$\alpha : X_H = H_0(H, X) \to X(E/F^{\mathrm{cyc}}). \tag{16}$$

Thanks to the basic results of [5], it is shown in [4, Lemma 6.7], that $\mathrm{Ker}(\alpha)$ is a finitely generated $\mathbb{Z}_p$-module, and that $\mathrm{Coker}(\alpha)$ is finite. As $X(E/F^{\mathrm{cyc}})$ is assumed to be $\Lambda(\Gamma)$-torsion, it follows that $H_0(H, X)$ is a finitely generated torsion $\Lambda(\Gamma)$-module. Now if we take H-cohomology of the exact sequence

$$0 \to X(p) \to X \to X_f \to 0, \tag{17}$$

and recall that $H_1(H, X) = 0$ by Lemma 2.5, we obtain the exact sequence of $\Lambda(\Gamma)$-modules

$$0 \to H_1(H, X_f) \to H_0(H, X(p)) \to H_0(H, X) \to H_0(H, X_f) \to 0. \tag{18}$$

The right hand end of (18) shows that $H_0(H, X_f)$ is $\Lambda(\Gamma)$-torsion, and the left hand end shows that $H_1(H, X_f)$ is finitely generated over $\Lambda(\Gamma)$ and annihilated by a power of p, because these two properties clearly hold for $H_0(H, X(p))$. This completes the proof of Lemma 2.10. $\square$

REMARK 2.11 Put $X = X(E/F_\infty)$, and continue to assume that hypotheses (i)-(iv) of Proposition 2.9 hold. As H is pro-p, Nakayama's lemma also shows that $X_f = X/X(p)$ is finitely generated as a $\Lambda(H)$-module if and only if $(X_f)_H = H_0(H, X_f)$ is a finitely generated $\mathbb{Z}_p$-module. As $H_0(H, X_f)$ is a finitely generated torsion $\Lambda(\Gamma)$-module, it follows that X_f is finitely generated as a $\Lambda(H)$-module if and only if $\mu_\Gamma(H_0(H, X_f)) = 0$.

PROPOSITION 2.12 *Assume that (i) $p \geq 5$, (ii) E has good ordinary reduction at all primes v of F dividing p (iii) G is pro-p, and (iv) $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. Then we have*

$$\mu_G(X(E/F_\infty)) = \mu_\Gamma(X(E/F^{\mathrm{cyc}})) + \delta + \epsilon, \tag{19}$$

where, writing $X = X(E/F_\infty)$,

$$\delta = \Sigma_{i=0}^{1} (-1)^{i+1} \mu_\Gamma(H_i(H, X_f)), \quad \epsilon = \Sigma_{i=1}^{3} (-1)^i \mu_\Gamma(H_i(H, X(p))). \tag{20}$$

PROOF As each module in the exact sequence (18) is $\Lambda(\Gamma)$-torsion, it follows (see [11, Prop. 1.9]) that the alternating sum of the μ_Γ-invariants taken along (18) is zero. Moreover, the μ_Γ-invariants of the two middle terms in (18) can be calculated as follows. Firstly, as $\mathrm{Ker}(\alpha)$ and $\mathrm{Coker}(\alpha)$ are finitely generated $\mathbb{Z}_p$-modules, it follows from (16) that

$$\mu_\Gamma(H_0(H, X)) = \mu_\Gamma(X(E/F^{\mathrm{cyc}})). \tag{21}$$

Secondly, for $i = 1, 2, 3, 4$, the Hochschild-Serre spectral sequence yields the short exact sequence

$$0 \to H_0(\Gamma, H_i(H, X(p))) \to H_i(G, X(p)) \to H_1(\Gamma, H_{i-1}(H, X(p))) \to 0. \tag{22}$$

Also, we have $H_4(H, X(p)) = 0$ because H has p-homological dimension equal to 3. It follows easily that

$$\chi(G, X(p)) = \prod_{i=0}^{3} \chi(\Gamma, H_i(H, X(p)))^{(-1)^i}, \tag{23}$$

whence by (15) for both the group G and the group Γ, we obtain

$$\mu_G(X) = \Sigma_{i=0}^{3} (-1)^i \mu_\Gamma(H_i(H, X(p))). \tag{24}$$

Proposition 2.12 now follows immediately (21) and (24) and from the fact that the alternating sum of the μ_Γ-invariants along (18) is 0. $\square$

We now give a stronger form of (19) when we impose the additional hypothesis that $X(E/F_\infty)$ is $\Lambda(G)$-torsion.

PROPOSITION 2.13 *Assume that (i) $p \geq 5$, (ii) E has good ordinary reduction at all primes v of F dividing p, (iii) G is pro-p, (iv) $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion, and (v) $X(E/F_\infty)$ is $\Lambda(G)$-torsion. Then $H_i(H, X_f)$ $(i = 1, 2)$, where*

$X_f = X(E/F_\infty)/X(E/F_\infty)(p)$, is a finitely generated $\Lambda(\Gamma)$-module which is killed by a power of p. Moreover,

$$\mu_G(X(E/F_\infty)) = \mu_\Gamma(X(E/F^{\mathrm{cyc}})) + \Sigma_{i=0}^{2}\ (-1)^{i+1}\mu_\Gamma(H_i(H, X_f)). \tag{25}$$

Corollary 2.14 *Assume hypotheses (i)-(iv) of Proposition 2.13 and replace (v) by the hypothesis that $X(E/F_\infty)/X(E/F_\infty)(p)$ is finitely generated over $\Lambda(H)$. Then*

$$\mu_G(X(E/F_\infty)) = \mu_\Gamma(X(E/F^{\mathrm{cyc}})). \tag{26}$$

To deduce the corollary, we first note that the hypothesis that X_f is finitely generated over $\Lambda(H)$ implies that X_f is $\Lambda(G)$-torsion, whence X is also $\Lambda(G)$-torsion. Secondly, the $H_i(H, X_f)$ are finitely generated $\mathbb{Z}_p$-modules once X_f is finitely generated over $\Lambda(H)$, and hence their μ_Γ-invariants are zero. Thus (26) then follows from (25). We remark that, in all cases known to date in which we can prove $X(E/F_\infty)$ is $\Lambda(G)$-torsion, one can show that X_f is finitely generated over $\Lambda(H)$, but we have no idea at present of how to prove this latter assertion in general.

Proof of Proposition 2.13 Again put $X = X(E/F_\infty)$. Since we are now assuming that X is $\Lambda(G)$-torsion, or equivalently that $\lambda_S(F_\infty)$ is surjective, we have already remarked (see Remark 2.6) that

$$H_i(H, X) = 0 \text{ for all } i \geq 1. \tag{27}$$

We next claim that

$$H_3(H, X_f) = 0. \tag{28}$$

Indeed, as H has p-cohomological dimension 3, and multiplication by p is injective on X_f, it follows that multiplication by p must also be injective on $H_3(H, X_f)$. On the other hand, taking H-homology of the exact sequence (17), we see that $H_3(H, X_f)$ injects into the torsion group $H_2(H, X(p))$ because $H_3(H, X) = 0$. Thus (28) follows. Moreover, using (27) and (28), we conclude from the long exact sequence of H-cohomology of (17) that

$$H_1(H, X(p)) = H_2(H, X_f), \quad H_i(H, X(p)) = 0\ (i = 2, 3). \tag{29}$$

Thus (25) now follows from (19), completing the proof of Proposition 2.13. $\square$

3 The truncated Euler characteristic

We assume throughout this section our three standard hypotheses: (i) $p \geq 5$, (ii) E has good ordinary reduction at all primes v of F dividing p, and (iii) $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. Since G has dimension 4 as a p-adic Lie group and has no element of order p, G has p-cohomological dimension equal to

4. We begin by defining the notion of the truncated G-Euler characteristic $\chi_t(G, A)$ of a discrete p-primary G-module A. The main aim of this section is to compute the truncated G-Euler characteristic of $\mathcal{S}(E/F_\infty)$ in terms of the Γ-Euler characteristic of $\mathcal{S}(E/F^{\mathrm{cyc}})$. A Birch-Swinnerton-Dyer type formula for the latter Euler characteristic is well-known (see Schneider [19], Perrin-Riou [18]), and we shall recall this at the end of this section.
If D is a discrete p-primary Γ-module, we have

$$H^0(\Gamma, D) = D^\Gamma, \quad H^1(\Gamma, D) \cong D_\Gamma,$$

and hence there is the obvious map

$$\phi_D \ : \ H^0(\Gamma, D) \to H^1(\Gamma, D) \tag{30}$$

given by $\phi_D(x) =$ residue class of x in D_Γ. If f is any homomorphism of abelian groups, we define

$$q(f) = \#(\mathrm{Ker}(f))/\#(\mathrm{Coker}(f)), \tag{31}$$

saying $q(f)$ is finite if both $\mathrm{Ker}(f)$ and $\mathrm{Coker}(f)$ are finite. We say D has finite Γ-Euler characteristic if $q(\phi_D)$ is finite, and we then define $\chi(\Gamma, D) = q(\phi_D)$.
Suppose now that A is a discrete p-primary G-module. As in the previous section, we write $H = G(F_\infty/F^{\mathrm{cyc}})$, so that H is a closed normal subgroup of G with $G/H = \Gamma$. Parallel to (30), we define a map

$$\xi_A \ : \ H^0(G, A) \to H^1(G, A) \tag{32}$$

by $\xi_A = \eta \circ \phi_{A^H}$, where η is the inflation map from $H^1(\Gamma, A^H)$ to $H^1(G, A)$. We say that A has *finite truncated G-Euler characteristic* if $q(\xi_A)$ is finite, and we then define the truncated G-Euler characteristic of A by

$$\chi_t(G, A) = q(\xi_A). \tag{33}$$

Of course, if the $H^i(G, A)$ are finite for all $i \geqslant 0$, and zero for $i \geqslant 2$, then the truncated G-Euler characteristic of A coincides with the usual G-Euler characteristic of A. However, we shall be interested in G-modules A, which arise naturally in arithmetic, and for which we can often show that the truncated Euler characteristic is finite and compute it, without being able to prove anything about the $H^i(G, A)$ for $i \geqslant 2$. In fact (see the remarks immediately after Theorem 2.2), it is conjectured that in the arithmetic example we consider when $A = S(E/F_\infty)$, we always have $H^i(G, A) = 0$ for $i \geqslant 2$.
If v is a finite prime of F, we write $L_v(E, s)$ for the Euler factor at v of the complex L-function of E over F. In particular, when E has bad reduction (the only case we shall need) $L_v(E, s)$ is 1, $(1 - (Nv)^{-s})^{-1}$, and $(1 + (Nv)^{-s})^{-1}$, according as E has additive, split multiplicative, or non-split multiplicative reduction at v. Also, if u and v are non-zero elements of $\mathbb{Q}_p$, $u \sim v$ means that u/v is a p-adic unit. The following is the main result of this section. As usual, j_E denotes the j-invariant of the elliptic curve E.

Theorem 3.1 *Assume that (i) $p \geq 5$, (ii) E has good ordinary reduction at all places v of F dividing p, and (iii) $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. Then $\chi_t(G, \mathcal{S}(E/F_\infty))$ is finite if and only if $\chi(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}}))$ is finite. Moreover, when $\chi(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}}))$ is finite, we have*

$$\chi_t(G, \mathcal{S}(E/F_\infty)) \sim \chi(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}})) \times \prod_{v \in \mathcal{M}} L_v(E,1)^{-1},$$

where $\mathcal{M}$ consists of all places v of F where the j-invariant of E is non-integral,

The following is a special case of Theorem 3.1 (see [2, Theorem 1.15] for a weaker result in this direction). Assuming hypotheses (i) and (ii) of Theorem 3.1, it is well-known (see [6] or Greenberg [10]) that both $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion and $\chi(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}}))$ is finite when $\mathcal{S}(E/F)$ is finite.

Corollary 3.2 *Assume that (i) $p \geq 5$, (ii) E has good ordinary reduction at all places v of F dividing p, and (iii) $\mathcal{S}(E/F)$ is finite. Then $\chi_t(G, \mathcal{S}(E/F_\infty))$ is finite and*

$$\chi_t(G, \mathcal{S}(E/F_\infty)) \sim \chi(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}})) \times \prod_{v \in \mathcal{M}} L_v(E,1)^{-1},$$

We now give the proof of Theorem 3.1 via a series of lemmas. For these lemmas, we assume that hypotheses (i), (ii) and (iii) of Theorem 3.1 are valid. We let S' be the subset of S consisting of all places v of F such that $\mathrm{ord}_v(j_E) < 0$. We then define

$$\mathcal{S}'(E/F^{\mathrm{cyc}}) = \mathrm{Ker}(H^1(G_S(F^{\mathrm{cyc}}), E_{p^\infty}) \to \bigoplus_{v \in S \setminus S'} J_v(F^{\mathrm{cyc}})). \tag{34}$$

We remark that we could also define $\mathcal{S}'(E/F_\infty)$ analogously, but in fact $\mathcal{S}'(E/F_\infty) = \mathcal{S}(E/F_\infty)$ as $J_v(F_\infty) = 0$ for v in S' (see [2, Lemma 3.3]).

Lemma 3.3 *We have the exact sequence of Γ-modules*

$$0 \to \mathcal{S}(E/F^{\mathrm{cyc}}) \to \mathcal{S}'(E/F^{\mathrm{cyc}}) \to \bigoplus_{v \in S'} J_v(F^{\mathrm{cyc}}) \to 0.$$

Proof This is clear from the commutative diagram with exact rows (cf. Lemma 2.1)

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{S}(E/F^{\mathrm{cyc}}) \arrow[r] \arrow[d] & H^1(G_S(F^{\mathrm{cyc}}), E_{p^\infty}) \arrow[r, "\lambda_S(F^{\mathrm{cyc}})"] \arrow[d] & \bigoplus_{v \in S} J_v(F^{\mathrm{cyc}}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{S}'(E/F^{\mathrm{cyc}}) \arrow[r] & H^1(G_S(F^{\mathrm{cyc}}), E_{p^\infty}) \arrow[r] & \bigoplus_{v \in S \setminus S'} J_v(F^{\mathrm{cyc}}) \arrow[r] & 0
\end{tikzcd}$$

where all the vertical arrows are the natural maps, the first is the natural inclusion, the middle map is the identity and the right vertical map is the natural projection. $\square$

LEMMA 3.4 *We have that* $\chi(\Gamma, \mathcal{S}'(E/F^{\mathrm{cyc}}))$ *is finite if and only if* $\chi(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}}))$ *is finite. Moreover, when* $\chi(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}}))$ *is finite, we have*

$$\chi(\Gamma, \mathcal{S}'(E/F^{\mathrm{cyc}})) \sim \chi(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}})) \times \prod_{v \in \mathcal{M}} L_v(E,1)^{-1}$$

and $\mathcal{M}$ *is the set of places with non-integral* j*-invariant as before.*

PROOF The lemma is very well known (see, for example, [4, Lemma 5.6 and Corollary 5.8] for a special case), and so we only sketch the proof. Indeed, by the multiplicativity of the Euler characteristic in exact sequences, we see that all follows from Lemma 3.3 and the fact that

$$\chi(\Gamma, \bigoplus_{v \in S'} J_v(F^{\mathrm{cyc}})) \sim \prod_{v \in \mathcal{M}} L_v(E,1)^{-1},$$

(see [4, Lemmas 5.6 and 5.11]). □

LEMMA 3.5 *Let* $f : A \to B$ *be a homomorphism of* p*-primary* Γ*-modules with both* $\mathrm{Ker}(f)$ *and* $\mathrm{Coker}(f)$ *finite. If*

$$g \ : \ A^{\Gamma} \to B^{\Gamma}, \quad h \ : \ A_{\Gamma} \to B_{\Gamma}$$

denote the two maps induced by f*, then* $q(g)$ *and* $q(h)$ *are finite, and* $q(g) = q(h)$.

PROOF This follows easily from breaking up the commutative diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & A^{\Gamma} & \longrightarrow & A & \xrightarrow{\gamma-1} & A & \longrightarrow & A_{\Gamma} & \longrightarrow & 0 \\ & & {\scriptstyle g}\downarrow & & {\scriptstyle f}\downarrow & & {\scriptstyle f}\downarrow & & {\scriptstyle h}\downarrow & & \\ 0 & \longrightarrow & B^{\Gamma} & \longrightarrow & B & \xrightarrow{\gamma-1} & B & \longrightarrow & B_{\Gamma} & \longrightarrow & 0, \end{array}$$

where γ is a topological generator of Γ, into two commutative diagrams of short exact sequences and applying the snake lemma to each of these diagrams. □

The heart of the proof of Theorem 3.1 is to apply Lemma 3.5 to the map

$$f \ : \ \mathcal{S}'(E/F^{\mathrm{cyc}}) \to \mathcal{S}(E/F_{\infty})^{H} \tag{35}$$

given by the restriction. We therefore need

LEMMA 3.6 *If* f *is given by* (35)*, both* $\mathrm{Ker}(f)$ *and* $\mathrm{Coker}(f)$ *are finite.*

PROOF Put $S'' = S \setminus S'$. As $J_v(F_{\infty}) = 0$ for $v \in S'$, we have the commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 \longrightarrow & \mathcal{S}(E/F_\infty)^H & \longrightarrow & H^1(G_S(F_\infty), E_{p^\infty})^H & \longrightarrow & \bigoplus_{v\in S''} J_v(F_\infty)^H & \\ & {\scriptstyle f}\uparrow & & \uparrow & & {\scriptstyle \gamma''_S(F^{\rm cyc})}\uparrow & \\ 0 \longrightarrow & \mathcal{S}'(E/F^{\rm cyc}) & \longrightarrow & H^1(G_S(F^{\rm cyc}), E_{p^\infty}) & \longrightarrow & \bigoplus_{v\in S''} J_v(F^{\rm cyc}) & \longrightarrow 0. \end{array}$$

Now it is known that $H^i(H, E_{p^\infty})$ is finite for all $i \geq 0$ (see [6, Appendix A.2.6]). Hence Lemma 3.6 will follow from this diagram provided we show that the kernel of $\gamma_{S''}(F^{\rm cyc})$ is finite (it is here that we will use the fact that S'' contains no place of potential multiplicative reduction for E). Now

$$\mathrm{Ker}(\gamma_{S''}(F^{\rm cyc})) = \bigoplus_w \mathrm{Ker}(\gamma_w(F^{\rm cyc})),$$

where

$$\mathrm{Ker}(\gamma_w(F^{\rm cyc})) = H^1(\Omega_w, E(F_{\infty,w}))(p);$$

here w runs over all primes of $F^{\rm cyc}$ lying above primes in S'', and Ω_w denotes the decomposition group in H of some fixed prime of F_∞ above w. Then (see [2, Lemma 3.7]) we have

$$\mathrm{Ker}(\gamma_w(F^{\rm cyc})) = H^1(\Omega_w, E_{p^\infty}). \tag{36}$$

But E has potential good reduction at w, and $F_w^{\rm cyc}$ contains the unique unramified $\mathbb{Z}_p$ extension of F_w. Hence, as $p \geq 5$, it follows from Serre-Tate [20] that Ω_w must be a finite group of order prime to p, and thus (36) shows that $\gamma_w(F^{\rm cyc})$ is injective in this case. Suppose next that w does divide p. Then it follows from the results of [3] that

$$\mathrm{Ker}(\gamma_w(F^{\rm cyc})) = H^1(\Omega_w, \tilde{E}_{w,p^\infty}), \tag{37}$$

where $\tilde{E}_{w,p^\infty}$ denotes the image of E_{p^∞} under reduction modulo w. But it is known (see either [8] or [4, Lemma 5.25]) that the cohomology groups $H^i(\Omega_w, \tilde{E}_{w,p^\infty})$ are finite for all $i \geq 0$. Hence $\mathrm{Ker}(\gamma_w(F^{\rm cyc}))$ is finite, and the proof of Lemma 3.6 is complete. □

We can now finish the proof of Theorem 3.1. Consider the Γ-modules

$$A = \mathcal{S}'(E/F^{\rm cyc}), \quad B = \mathcal{S}(E/F_\infty)^H,$$

and the map given by (35). By Lemma 2.7, we have

$$H^0(\Gamma, B) = H^0(G, \mathcal{S}(E/F_\infty)), \quad H^1(\Gamma, B) = H^1(G, \mathcal{S}(E/F_\infty)),$$

and we clearly have the commutative diagram

$$\begin{array}{ccc} H^0(\Gamma, A) & \xrightarrow{g} & H^0(\Gamma, B) = H^0(G, \mathcal{S}(E/F_\infty)) \\ {\scriptstyle \phi_A}\downarrow & & {\scriptstyle \xi_B}\downarrow \\ H^1(\Gamma, A) & \xrightarrow{h} & H^1(\Gamma, B) = H^1(G, \mathcal{S}(E/F_\infty)), \end{array}$$

here g and h are induced by f, and ϕ_A and ξ_B are defined by (30) and (32), respectively. By Lemmas 3.5 and 3.6, we know that $q(g)$ and $q(h)$ are finite, whence it is plain from the diagram that $q(\phi_A)$ is finite if and only if $q(\xi_B)$ is finite. Now it is a basic property of the q-function, that q of a composition of two maps is the product of the $q's$ of the individual maps. Hence, as $\xi_B \circ g = \phi_A \circ h$, we conclude that $q(\xi_B)q(g) = q(\phi_A)q(h)$, when $q(\phi_A)$ or equivalently $q(\xi_B)$ is finite. But $q(g) = q(h)$ by Lemma 3.5, and so $q(\phi_A) = q(\xi_B)$. Applying Lemma 3.4 to compute $q(\phi_A)$ in terms of $\chi(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}}))$, the proof of Theorem 3.1 is now complete. □

We now briefly recall the value of $\chi(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}}))$ determined by Perrin-Riou [18] and Schneider [19], and use Theorem 3.1 to discuss several numerical examples. We need the following notation. If A is an abelian group, $A(p)$ will denote its p-primary subgroup. If w is any finite prime of F, we put $c_w = [E(F_w) : E_0(F_w)]$, where $E_0(F_w)$ denotes the subgroup of points in $E(F_w)$ with non-singular reduction modulo w. Put

$$\tau_p(E) = |\Pi_w c_w|_p^{-1},$$

where the p-adic valuation is normalized so that $|p|_p = p^{-1}$. For each place v of F dividing p, let k_v be the residue field of v, and let $\widetilde{E}_v$ over k_v be the reduction of E modulo v. We say that a prime v of F dividing p is *anomalous* if $\widetilde{E}_v(k_v)(p) \neq 0$. We always continue to assume that $p \geqslant 5$, and that E has good ordinary reduction at all primes v of F dividing p. Write $\text{Ш}(E/F)$ for the Tate-Shafarevich group of E over F.

CASE 1. We assume that $E(F)$ is finite, and $\text{Ш}(E/F)(p)$ is finite, or equivalently $\mathcal{S}(E/F)$ is finite. Then it is shown in [18], [19] that $H^i(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}}))$ $(i = 0, 1)$ is finite, and

$$\chi(\Gamma, \mathcal{S}(E/F^{\mathrm{cyc}})) = \frac{\#(\text{Ш}(E/F)(p))}{\#(E(F)(p))^2} \times \tau_p(E) \times \prod_{v|p} \#(\widetilde{E_v}\ (k_v)(p))^2.$$

EXAMPLE 1. Take $F = \mathbb{Q}$ and let E be the elliptic curve

$$X_1(11) : y^2 + y = x^3 - x^2.$$

Kolyvagin's theorem tells us that both $E(\mathbb{Q})$ and $\text{Ш}(E/\mathbb{Q})$ are finite, since the complex L-function of E does not vanish at $s1$. The conjecture of Birch and Swinnerton-Dyer predicts that $\text{Ш}(E/\mathbb{Q}) = 0$, but the numerical verification of this via Heegner points does not seem to exist in the literature. Now it is well known that $\mathcal{S}(E/\mathbb{Q}^{\mathrm{cyc}}) = 0$ for $p = 5$, and that $\mathcal{S}(E/\mathbb{Q}^{\mathrm{cyc}}) = 0$ for a good ordinary prime $p > 5$ provided $\text{Ш}(E/\mathbb{Q})(p) = 0$ (see [6]). Hence, assuming $\text{Ш}(E/\mathbb{Q})(p) = 0$ when $p > 5$, we conclude that

$$\chi(\Gamma, \mathcal{S}(E/\mathbb{Q}^{\mathrm{cyc}})) = 1$$

for all good ordinary primes $p \geqslant 5$. Our knowledge of $X(E/F_\infty)$ is extremely limited. We know (see [2]) that $X(E/F_\infty)\bigotimes_{\mathbb{Z}_p} \mathbb{Q}_p$ has infinite dimension over $\mathbb{Q}_p$ for all primes $p \geqslant 5$. Take $S\{p, 11\}$, and note that 11 is the only prime where E has non-integral j-invariant and $L_{11}(E, S) = (1 - 11^{-s})^{-1}$. First, assume that $p = 5$. Theorem 3.1 then tells us that

$$\chi_t(G, \mathcal{S}(E/F_\infty)) = 5.$$

But it is shown in [4] that the map $\lambda_S(G_\infty)$ is surjective when $p = 5$. Hence we have also $H^i(G, \mathcal{S}(E/F_\infty)) = 0$ for $i = 2, 3, 4$ and so we have the stronger result that $\mathcal{S}(E/F_\infty)$ has finite G-Euler characteristic, and $\chi(G, \mathcal{S}(E/F_\infty)) = 5$. Next assume that p is a good ordinary prime > 5, and that $\text{Ш}(E/\mathbb{Q})(p) = 0$. Then Theorem 3.1 gives

$$\chi_t(G, \mathcal{S}(E/F_\infty)) = 1.$$

However, it has not been proven yet that $\lambda_S(F_\infty)$ is surjective for a single good ordinary prime $p > 5$, and so we know nothing about the $H^i(G, \mathcal{S}(E/F_\infty))$ for $i = 2, 3, 4$. But we can deduce a little more from the above evaluation of the truncated Euler characteristic. For $E = X_1(11)$, Serre has shown that $GGL_2(\mathbb{Z}_p)$ for all $p \geqslant 7$, whence it follows by a well known argument that $H^i(G, E_{p^\infty}) = 0$ for all $i \geqslant 1$. But it is proven in [2] (see Lemmas 4.8 and 4.9) that the order of $H^1(G, \mathcal{S}(E/F_\infty))$ must divide the order of $H^3(G, E_{p^\infty})$. Hence finally we conclude that

$$H^0(G, \mathcal{S}(E/F_\infty)) = H^1(G, \mathcal{S}(E/F_\infty)) = 0$$

for all good ordinary primes $p > 5$ such that $\text{Ш}(E/\mathbb{Q})(p) = 0$.

Case 2. We assume now that $E(F)$ has rank $g \geq 1$, and that $\text{Ш}(E/F)(p)$ is finite. We write

$$< \ , \ >_{F,p} \colon E(F) \times E(F) \to \mathbb{Q}_p$$

for the canonical p-adic height pairing (see [16], [18], [19]), which exists because of our hypotheses that E has good ordinary reduction at all places v of F dividing p. If $P_1, \cdots, P_g$ denote a basis of $E(F)$ modulo torsion, we define

$$R_p(E/F) = \det < P_i, P_j > .$$

It is conjectured that we always have $R_p(E/F) \neq 0$, but this is unknown. Recalling that we are assuming that $\text{Ш}(E/F)(p)$ is finite, the principal result of [18], [19] is that firstly $\chi(\Gamma, \mathcal{S}(E/F^{\text{cyc}}))$ is finite if and only if $R_p(E/F) \neq 0$, and secondly, when $R_p(E/F) \neq 0$, we have

$$\chi(\Gamma, \mathcal{S}(E/F^{\text{cyc}})) = p^{-g} \mid \rho_p \mid_p^{-1} .$$

where

$$\rho_p = \frac{R_p(E/F) \times \#(\text{Ш}(E/F)(p))}{\sharp(E(F)(p))^2} \times \tau_p(E) \times \prod_{v|p} \#(\widetilde{E_v}(k_v)(p))^2.$$

The work of Mazur and Tate [16] gives a very efficient numerical method for calculating $R_p(E/F)$ up to a p-adic unit, and so the right hand side of this formula can be easily computed in simple examples, provided we know the order of $Ш(E/F)(p)$.

Example 2. Take $F = \mathbb{Q}$, and let E be the elliptic curve of conductor 37.

$$E \;:\; y^2 + y = x^3 - x.$$

It is well-known that $E(\mathbb{Q})$ is a free abelian group of rank 1 generated by $P = (0, 0)$. Moreover, the complex L-function of E over $\mathbb{Q}$ has a simple zero at $s = 1$, and so $Ш(E/\mathbb{Q})$ is finite by Kolyvagin's theorem. In fact, the conjecture of Birch and Swinnerton-Dyer predicts that $Ш(E/\mathbb{Q}) = 0$, but again the numerical verification of this via Heegner points does not seem to exist in the literature. We put $h_p(P) =< P, P >_{\mathbb{Q},p}$. The supersingular primes for E less than 500 are 2, 3, 17, 19, 257, 311. The ordinary primes for E less than 500 which are anamolous are 53, 127, 443. The following values for $h_p(P)$ for p ordinary with $p < 500$ have been calculated by C. Wuthrich. We have

$$\mid h_p(P) \mid_p = p^{-2} \text{ for } p = 13,\ 67 \text{ and } \mid h_p(P) \mid_p = p \text{ for } p = 53,\ 127,\ 443,$$

and $\mid h_p(P) \mid_p = p^{-1}$ for the remaining primes. As $c_{37} = 1$, we conclude from the above formula that $\chi(\Gamma, \mathcal{S}(E/\mathbb{Q}^{\mathrm{cyc}})) = 1$ for all ordinary primes $p < 500$, with the exception of $p = 13,\ 67$, where we have $\chi(\Gamma, \mathcal{S}(E/\mathbb{Q}^{\mathrm{cyc}})) = p$; here we are assuming that $Ш(E/\mathbb{Q})(p) = 0$. Now 37 is the only prime where the j-invariant of E is non-integral, and $L_{37}(E, s) = (1+37^{-s})^{-1}$. Hence we conclude from Theorem 3.1 that $\chi_t(G, \mathcal{S}(E/F_\infty))$ is finite and

$$\chi_t(G, \mathcal{S}(E/F_\infty)) = \chi(\Gamma, \mathcal{S}(E/\mathbb{Q}^{\mathrm{cyc}})).$$

We point out that we do not know that $\lambda_S(F_\infty)$ is surjective for a single ordinary prime p for this curve.

4 An algebraic invariant

In this last section, we attach a new invariant to a wide class of modules over the Iwasawa algebra of a compact p-adic Lie group G satisfying the following conditions: (i) G is pro-p, (ii) G has no element of order p, and (iii) G has a closed normal subgroup H such that G/H is isomorphic to $\mathbb{Z}_p$. We always put

$$\Gamma = G/H, \tag{38}$$

and write $Q(\Gamma)$ for the quotient field of the Iwasawa algebra $\Lambda(\Gamma)$ of Γ. We assume that G satisfies these hypotheses for the rest of this section. By [14], G has finite p-cohomological dimension, which is equal to the dimension d of

G as a p-adic Lie group. We are interested in the following full subcategory of the category of all finitely generated torsion $\Lambda(G)$-modules. Let $\mathfrak{M}_H(G)$ denote the category whose objects are all $\Lambda(G)$-modules which are finitely generated over $\Lambda(H)$ (such modules are automatically torsion $\Lambda(G)$-modules, because $\Lambda(G)$ is not finitely generated as a $\Lambda(H)$-module). Perhaps somewhat unexpectedly, it is shown in [4] that many $\Lambda(G)$-modules which arise in the GL_2-Iwasawa theory of elliptic curves belong to $\mathfrak{M}_H(G)$ (specifically, in the notation of §2, $X(E/F_\infty)$ is a $\Lambda(G)$-module in $\mathfrak{M}_H(G)$ when we assume that (i) $p \geqslant 5$, (ii) E has good ordinary reduction at all primes v of F dividing p, (iii) G is pro-p, and (iv) $X(E/F^{cyc})$ is a finitely generated $\mathbb{Z}_p$-module; here $H = G(F_\infty/F^{cyc})$).

If f and g are any two non-zero elements of $Q(\Gamma)$, we write $f \sim g$ if fg^{-1} is a unit in $\Lambda(\Gamma)$. To each M is $\mathfrak{M}_H(G)$, we now attach a non-zero element f_M of $Q(\Gamma)$, which is canonical in the sense that it is well-defined up to the equivalence relation $\sim$. As M is a finitely generated $\Lambda(H)$-module, all of the homology groups

$$H_i(H, M) \qquad (i \geqslant 0) \tag{39}$$

are finitely generated $\mathbb{Z}_p$-modules. On the other hand, as M is a $\Lambda(G)$-module, these homology groups have a natural structure as $\Lambda(\Gamma)$-modules, and they must therefore be torsion $\Lambda(\Gamma)$-modules. Let g_i in $\Lambda(\Gamma)$ be a characteristic power series for the $\Lambda(\Gamma)$-module $H_i(H, M)$, and define

$$f_M = \prod_{i \geqslant 0} g_i^{(-1)^i}. \tag{40}$$

This product is, of course, finite because $H_i(H, M) = 0$ for $i \geqslant d$, and it is well defined up to $\sim$, because each g_i is well defined up to multiplication by a unit in $\Lambda(\Gamma)$.

Lemma 4.1 *(i) If $M(p)$ denotes the submodule of M in $\mathfrak{M}_H(G)$ consisting of all elements of p-power order, then $f_M \sim f_{M/M(p)}$; (ii) If we have an exact sequence of modules in $\mathfrak{M}_H(G)$,*

$$0 \to M_1 \to M_2 \to M_3 \to 0, \tag{41}$$

then $f_{M_2} \sim f_{M_1} \cdot f_{M_3}$.

Proof (i) is plain from the long exact sequence of H-homology derived from the exact sequence

$$0 \to M(p) \to M \to M/M(p) \to 0,$$

and the fact that the $H_i(H, M(p))(i \geqslant 0)$ are killed by any power of p which annihilates $M(p)$, and are therefore finite. Similarly, (ii) follows from the exact sequence of H-homology derived from (41), and the classical fact that the $\Lambda(\Gamma)$-characteristic series is multiplicative in exact sequences. □

One of the main reasons we are interested in the invariant f_M is its link with the G-Euler characteristic of M. If g is any element of $\Lambda(\Gamma)$, we write $g(0)$ as usual for the image of g under the augmentation map from $\Lambda(\Gamma)$ to $\mathbb{Z}_p$. Similarly, if g is any non-zero element of $Q(\Gamma)$, then the fact that $\Lambda(\Gamma)$ is a unique factorization domain allows us to write $g = h_1/h_2$, where h_1 and h_2 are relatively prime elements of $\Lambda(\Gamma)$. We say that $g(0)$ is defined if $h_2(0) \neq 0$, and then put $g(0) = h_1(0)/h_2(0)$. If $M \in \mathfrak{M}_H(G)$, we say that M has finite G-Euler characteristic if the $H_i(G, M)$ are finite for all $i \geqslant 0$, and, when this is the case, we define

$$\chi(G, M) = \prod_{i \geqslant 0} \#(H_i(G, M))^{(-1)^i}. \tag{42}$$

Lemma 4.2 *Assume that M in $\mathfrak{M}_H(G)$ has finite G-Euler characteristic. Then $f_M(0)$ is defined and non-zero, and we have*

$$\chi(G, M) = |f_M(0)|_p^{-1}. \tag{43}$$

Proof As Γ has cohomological dimension 1, for all $i \geqslant 1$ the Hochschild-Serre spectral sequence yields an exact sequence

$$0 \to H_0(\Gamma, H_i(H, M)) \to H_i(G, M) \to H_1(\Gamma, H_{i-1}(H, M)) \to 0. \tag{44}$$

The finiteness of the $H_i(G, M)$ ($i \geqslant 0$) therefore implies that, for all $i \geqslant 0$, we have $g_i(0) \neq 0$, where, as above, g_i denotes a characteristic power series for $H_i(H, M)$. Moreover, by a classical formula for $\Lambda(\Gamma)$-modules, we then have

$$|g_i(0)|_p^{-1} = \frac{\#(H_0(\Gamma, H_i(H, M)))}{\#(H_1(\Gamma, H_i(H, M)))} \tag{45}$$

for all $i \geqslant 0$. The formula (43) is now plain from (44) and (45), and the proof of the lemma is complete. □

Let

$$\pi_\Gamma : \Lambda(G) \to \Lambda(\Gamma) \tag{46}$$

be the natural ring homomorphism.

Lemma 4.3 *Let g be a non-zero element of $\Lambda(G)$ such that $N = \Lambda(G)/\Lambda(G)g$ belongs to $\mathfrak{M}_H(G)$. Then $H_i(H, N) = 0$ for all $i > 0$. Moreover, $f_N \sim \pi_\Gamma(g)$ lies in $\Lambda(\Gamma)$, and $f_N(0) \neq 0$ if and only if N has finite G-Euler characteristic.*

Proof We have the exact sequence of $\Lambda(G)$-modules

$$(47) \qquad 0 \to \Lambda(G) \xrightarrow{\cdot g} \Lambda(G) \to N \to 0,$$

where $\cdot g$ denotes multiplication on the right by g. Since $H_i(G, \Lambda(G)) = 0$ for $i \geqslant 1$, we conclude that $H_i(G, N) = 0$ for $i > 1$. But, for any compact $\Lambda(G)$-module R, the Hochschild-Serre spectral sequence provides an injection of $H_0(\Gamma, H_i(H, R))$ into $H_i(G, R)$, and so the vanishing of $H_i(G, R)$ implies the vanishing of the compact Γ-module $H_i(H, R)$. It follows that $H_i(H, \Lambda(G)) = 0$ for $i \geqslant 1$, and that $H_i(H, N) = 0$ for $i > 1$. Put $h = \pi_\Gamma(g)$. Taking H-homology of (47). we obtain the exact sequence of $\Lambda(\Gamma)$-modules

$$(48) \qquad 0 \to H_1(H, N) \to \Lambda(\Gamma) \xrightarrow{\cdot h} \Lambda(\Gamma) \to H_0(H, N) \to 0,$$

where $\cdot h$ now denotes right multiplication by h. Note that $H_0(H, N)$ is $\Lambda(\Gamma)$-torsion as N is in $\mathfrak{M}_H(G)$, and so we must have $h \neq 0$. But then multiplication by h in $\Lambda(\Gamma)$ is injective, and so $H_1(H, N) = 0$, and it is then clear than $f_N \sim h$. Finally, returning to the G-homology of (47), we obtain the exact sequence

$$(49) \qquad 0 \to H_1(G, N) \to \mathbb{Z}_p \xrightarrow{\cdot h(0)} \mathbb{Z}_p \to H_0(G, N) \to 0,$$

and so N has finite G-Euler characteristic if and only if $h(0) \neq 0$. This completes the proof of Lemma 4.3. $\square$

We recall (see [22]) that a finitely generated torsion $\Lambda(G)$-module M is defined to be *pseudo-null* if $\mathrm{Ext}^1_{\Lambda(G)}(M, \Lambda(G)) = 0$. If M lies in $\mathfrak{M}_H(G)$, it is an important fact that M is pseudo-null as a $\Lambda(G)$-module if and only if M is $\Lambda(H)$-torsion. Since G as an extension of Γ by H necessarily splits, and hence is a semi-direct product, this is proven in [23, Prop. 5.4] provided H is uniform. However, by a well-known argument [22, Prop. 2.7], it then follows in general for our G, since H must always contain an open subgroup which is uniform.

Lemma 4.4 *Let M be a module in $\mathfrak{M}_H(G)$. If G is isomorphic to $\mathbb{Z}_p^r$, for some integer $r \geqslant 1$, then $f_M \sim 1$ if and only if M is pseudo-null as a $\Lambda(G)$-module.*

Proof We assume $r \geq 2$, since pseudo-null modules are finite when $r = 1$. Let M be a $\Lambda(H)$-torsion module in $\mathfrak{M}_H(G)$. We recall that $f_M = \prod_{i \geqslant 0} g_i^{(-1)^i}$, where g_i in $\Lambda(\Gamma)$ is a characteristic power series for the torsion $\Lambda(\Gamma)$-module $H_i(H, M)$. By (i) of Lemma 4.1, we may assume that M has no p-torsion. Thus the assumptions of Lemma 2 of [9] when applied to M as a $\Lambda(H)$-module are satisfied, and we conclude that there exists a closed subgroup J of H such that $H/J \xrightarrow{\sim} \mathbb{Z}_p$ and M is finitely generated as a $\Lambda(J)$-module. Analogously to (44), the Hochschild-Serre spectral sequence gives rise to the exact sequences of finitely generated torsion $\Lambda(\Gamma)$-modules, for all $i \geqslant 1$,

$$(50) \quad 0 \to H_0(H/J, H_i(J, M)) \to H_i(H, M) \to H_1(H/J, H_{i-1}(J, M)) \to 0.$$

Hence, if $g_{j,i}$ denotes the characteristic power series of $H_j(H/J, H_i(J,M))$ as a torsion $\Lambda(\Gamma)$-module, we obtain

$$g_0 \sim g_{0,0}, \quad g_i \sim g_{1,i-1} \cdot g_{0,i} \quad (i \geqslant 1).$$

Thus

$$f_M \sim g_{0,0} \times \prod_{i \geqslant 1} (g_{1,i-1} \cdot g_{0,i})^{(-1)^i} \sim \prod_{i \geqslant o} (g_{0,i}/g_{1,i})^{(-1)^i}.$$

On the other hand, letting $\overline{h}$ denote a topological generator of H/J, we have the exact sequence of $\Lambda(C)$-modules

$$0 \to H_1(H/J, H_i(J,M)) \to H_i(J,M) \xrightarrow{\overline{h}-1} H_i(J,M) \to H_0(H/J, H_i(J,M)) \to 0.$$

But $H_i(J,M)$ is a finitely generated $\mathbb{Z}_p$-module, because J was chosen so that M is a finitely generated $\Lambda(J)$-module. Hence the above exact sequence is in fact an exact sequence of finitely generated torsion $\Lambda(C)$-modules. By the multiplicativity of the characteristic power series along exact sequences, it follows that $g_{0,i} \sim g_{1,i}$.

Conversely, let $f_M \sim 1$. Under our hypotheses on G, the Iwasawa algebra $\Lambda(G)$ is a commutative regular local ring. By the classical structure theorem for finitely generated modules, M is pseudo-isomorphic to $\mathfrak{E}(M)$ where

$$\mathfrak{E}(M) = \bigoplus_{i=1}^{m} \Lambda(G)/\Lambda(G)g_i$$

with g_i non-zero for $i = 1, \cdots, m$. By Lemma 4.3 and the first part of the proof above, we see that $f_M \sim \pi_\Gamma(g_1 \cdots g_m)$. As f_M is assumed to be a unit in $\Lambda(\Gamma)$, we conclude that $\pi_\Gamma(g_1 \cdots g_m)$ is also a unit in $\Lambda(\Gamma)$, and hence $\pi_\Gamma(g_1 \cdots g_m)$ does not belong to the maximal ideal of $\Lambda(G)$. But, as the residue field of $\Lambda(G)$ is $\mathbb{F}_p$, and $\Lambda(G)$ is local, we see that $g_1 \cdots g_m$ is a unit in $\Lambda(G)$ and hence so is each g_1 $(i = 1, \cdots, m)$. Thus $\mathfrak{E}(M)$ is zero and M is pseudo-null, thereby completing the proof of the lemma. □

LEMMA 4.5 *Assume that G is a direct product $C \times H$, where C is isomorphic to Γ and H has dimension ≥ 1. Suppose that M in $\mathfrak{M}_H(G)$ is finitely generated as a $\mathbb{Z}_p$-module, then $f_M \sim 1$.*

PROOF We remark that a finitely generated $\mathbb{Z}_p$-module M in $\mathfrak{M}_H(G)$ is necessarily pseudo-null since H has dimension ≥ 1.

We fix a topological generator c of C end let $g_i(T)$ denote the characteristic polynomial of $c-1$ on the finite dimensional vector space $H_i(H,M) \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p$. We will show that

$$\prod_{i \geqslant 0} g_i^{(-1)^{(i)}} = 1.$$

Note first of all that, because M is finitely generated as a $\mathbb{Z}_p$-module, it is $\Lambda(H)$-torsion, and so we have (see [11])

$$\sum_{i\geqslant 0}(-1)^i \deg(g_i) = 0.$$

We now choose a finite extension $L/\mathbb{Q}_p$ which is a splitting field for all the polynomials g_i. Then g_i also can be viewed as the characteristic polynomial of $c-1$ on the L-vector space

$$H_i(H,M)\otimes_{\mathbb{Z}_p} L = H_i(H, M\otimes_{\mathbb{Z}_p} L).$$

Since our assertion is multiplicative in short exact sequences we may argue by induction with respect to the dimension of $M \underset{\mathbb{Z}_p}{\otimes} L$. As the H-action and the C-action commute, the H-action preserves all C-eigenspaces. This reduces us to the case where c acts on $M \underset{\mathbb{Z}_p}{\otimes} L$ by a single eigenvalue λ. Then c certainly acts on each $H_i(H,M) \underset{\mathbb{Z}_p}{\otimes} L$ by the same eigenvalue λ, and we obtain

$$\prod_{i\geqslant 0} g_i^{(-1)^{(i)}} = (T-\lambda)^{\sum (-1)^i \deg(g_i)} = (T-\lambda)^0 = 1.$$

□

When M is a finitely generated $\mathbb{Z}_p$-module which has finite G-Euler characteristic, then Lemmas 4.4 and 4.5 prove that $\chi(G,M)=1$. This is a slightly stronger version of the main theorem of [21] for a group $G = C\times H$ as in Lemma 4.5.

The previous two results might lead one to believe that the invariant f_M is a unit for all pseudo-null modules M in $\mathfrak{M}_H(G)$. However, the following two examples illustrate that this is not the case.

Example 3 (see [8], §5). Let K be any finite extension of $\mathbb{Q}_p$ which contains μ_p if p is odd and μ_4 if $p=2$. Take E to be any Tate elliptic curve over K, and write

$$G = G(K(E_{p^\infty})/K), \quad H = G(K(E_{p^\infty})/K(\mu_{p^\infty})).$$

Thus G is a p-adic Lie group of dimension 2, H is a closed normal subgroup of G which is isomorphic to $\mathbb{Z}_p$, and $\Gamma G/H$ is isomorphic to $\mathbb{Z}_p$. If M is a $\mathbb{Z}_p$-module on which G_K-acts, $M(n)$, as usual will denote the n-fold Tate twist of M by $T_p(\mu) = \varprojlim \mu_{p^n}$. We now consider the G-module

$$W = T_p(E).$$

As is shown in [8] (see [8], formula (48)), we then have

$$H_0(H,W) = \mathbb{Z}_p, \quad H_1(H,W) = \mathbb{Z}_p(-1).$$

To compute the corresponding f_W in $Q(\Gamma)$, let $\chi : G_K \to \mathbb{Z}_p^*$ be the cyclotomic character of G_K, i.e. $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for all σ in G_k and all ζ in μ_{p^∞}. Fix a topological generator γ of Γ, and identify $\Lambda(\Gamma)$ with the ring $\mathbb{Z}_p[[T]]$ of formal power series in T with coefficients in $\mathbb{Z}_p$ by mapping γ to $1+T$. Then we see immediately that

$$f_W = \frac{T}{T + 1 - \chi(\gamma)^{-1}}.$$

In particular, f_W does not belong to $\Lambda(\Gamma)$ in this example. We note also that, since G has dimension > 1, W is certainly a pseudo-null $\Lambda(G)$-module because W is a finitely generated $\mathbb{Z}_p$-module (see [24], Prop. 3.6).

EXAMPLE 4. We now assume that $G = C \times H$, and we take a $\Lambda(H)$-module M of the form

$$M = \Lambda(H)/\Lambda(H)g, \tag{51}$$

where g is any non-zero element of $\Lambda(H)$. To make M into a $\Lambda(G)$-module, it suffices to give a continuous action of C on M, which commutes with the H-action. Fix a topological generator c of C. If z is any element of $\Lambda(H)$, we write $z(0)$ for the image of z under the augmentation map in $\mathbb{Z}_p$. We now take units w and u in $\Lambda(H)$ satisfying

$$gw = ug, \quad w(0) \equiv u(0) \equiv 1 \bmod p. \tag{52}$$

We let c act on M by

$$c.(z + \Lambda(H)g) = zw + \Lambda(H)g. \tag{53}$$

This is well-defined by the first condition in (52), and extends to a continuous action of C by the second condition in (52). Conversely, let M be any $\Lambda(G)$-module which is of the form (51) as a $\Lambda(H)$-module with $g \neq 0$. It is then easy to see that the action of c on M is necessarily given by (53), where u and w are units in $\Lambda(H)$ satisfying (52), because $\Lambda(H)$ is a local ring. As discussed before Lemma 4.4, this $\Lambda(G)$-module M is pseudo-null because it is plainly $\Lambda(H)$-torsion. To compute the invariant f_M of M, we consider the exact sequence of $\Lambda(G)$-modules

$$0 \to \Lambda(H) \xrightarrow{\cdot g} \Lambda(H) \to M \to 0, \tag{54}$$

where c acts on the first copy of $\Lambda(H)$ by right multiplication by u, and on the second by right multiplication by w. Taking H-coinvariants of (54), we obtain that $H_i(H, M) = 0$ for $i \geq 1$, and the exact sequence of $\Lambda(C)$-modules

$$0 \to H_1(H, M) \to \mathbb{Z}_p \xrightarrow{\cdot g(0)} \mathbb{Z}_p \to H_0(H, M) \to 0; \tag{55}$$

here c acts on the first copy of $\mathbb{Z}_p$ by multiplication by $u(0)$, and on the second by multiplication by $w(0)$. Thus

$$f_M(T) = (T - w(0) + 1)/(T - u(0) + 1). \tag{56}$$

This is not a unit in $\Lambda(\Gamma)$ provided $w(0) \neq u(0)$.

To obtain concrete examples of such modules M with $w(0) \neq u(0)$, we now assume that H contains a subgroup which is a semi-direct product of the following form. Let H_0 and C_0 be two closed subgroups of H which are isomorphic to $\mathbb{Z}_p$, and which are such that

$$xhx^{-1} = h^{\phi(x)} \quad (x \in C_0,\ h \in H_0),$$

where $\phi : C_0 \hookrightarrow \mathrm{Aut}(H_0) = \mathbb{Z}_p{}^*$ is a continuous injective group homomorphism. We note that this hypothesis is valid for any H which is open in $SL_n(\mathbb{Z}_p)$ ($n \geq 2$), or more generally for any compact H which is open in the group of $\mathbb{Q}_p$-points of a split semi-simple algebraic group over $\mathbb{Q}_p$. Now fix a toplogical generator h_0 of H_0, and any element γ of C_0 with $\gamma \neq 1$. Define

$$g = h_0 - 1,\ w = \gamma + p^r,$$

where r is any integer ≥ 1. We then have

$$gw = ug, \text{ where } u = \gamma \cdot \frac{h_0^{\phi(\gamma)} - 1}{h_0 - 1} + p^r.$$

Hence

$$w(0) = 1 + p^r, \quad u(0) = \phi(\gamma) + p^r,$$

and so $u(0) \neq w(0)$ because ϕ is injective. Moreover, as $w(0)$ and $u(0)$ are not equal to 1, we see that M has finite G-Euler characteristic, which by Lemma 4.2 is given by

$$\chi(G, M) = \ \left| \frac{\phi(\gamma) - 1 + p^r}{p^r} \right|_p .$$

This therefore gives a new class of pseudo-null $\Lambda(G)$-modules, which are not finitely generated over $\mathbb{Z}_p$, and which have a non-trivial G-Euler characteristic.

Finally, we interpret this example as a statement about K-theory classes. Writing $K_0(\mathfrak{M}_H(G))$ for the Grothendieck group of $\mathfrak{M}_H(G)$, it is clear from Lemma 4.1 that the map $M \mapsto f_M$ induces a homomorphism from $K_0(\mathfrak{M}_H(G))$ to $Q(\Gamma)^*/\Lambda(\Gamma)^*$. Now let M be any $\Lambda(G)$-module of the form (51) as a $\Lambda(H)$-module with $g \neq 0$. It follows from the computation of f_M given by (56) that the class of M in $K_0(\mathfrak{M}_H(G))$ is non-zero.

Let $\mathcal{C}^o(G)$ denote the abelian category of finitely generated torsion $\Lambda(G)$-modules which contains $\mathfrak{M}_H(G)$ as a full subcategory. Thus there is a natural map

$$i : K_0(\mathfrak{M}_H(G)) \to K_0(\mathcal{C}^0(G))$$

on the Grothendieck groups. Again, let M be a $\Lambda(G)$-module of the form (51). Writing $[M]$ for the class of M in $K_0(\mathfrak{M}_H(G))$, we have just seen that $[M]$ is not zero provided $w(0) \neq u(0)$. However, we now show that $i[M] = 0$. Let

$Q(G)$ denote the skew-field of fractions of $\Lambda(G)$, and let $\Omega(G)$ be the abelian group defined by

$$\Omega(G) := Q(G)^*/\Lambda(G)^*[Q(G)^*, Q(G)^*], \tag{57}$$

where for any ring A, A^* denotes the multiplicative group of units in A and $[A^*, A^*]$ is the commutator subgroup. It is well-known [1] that the localisation sequence yields an isomorphism

$$\phi : K_0(\mathcal{C}^0(G)) \simeq \Omega(G)$$

which sends the class of any module of the form $(\Lambda(G)/\Lambda(G)z)$, $z \neq 0$ in $\Lambda(G)$, to the class of z in $\Omega(G)$. Hence (54) shows that $\phi(i([M]))$ is the coset of $(c-u)^{-1}(c-w)$. We prove that this coset is trivial in $\Omega(G)$. Indeed, since c is in the centre of G, by (52), we get

$$g(c-w) = (c-u)g. \tag{58}$$

Hence in $\Omega(G)$, we have

$$\begin{aligned} g(c-u)^{-1}(c-w) &= g(c-w)(c-u)^{-1} \\ &= (c-u)g(c-u)^{-1} \quad \text{by (58)} \\ &= (c-u)(c-u)^{-1}g \\ &= g. \end{aligned}$$

Since $\Omega(G)$ is a group, it follows that the class of $(c-u)^{-1}(c-w)$ in $\Omega(G)$ is trivial, as required.

References

[1] H. Bass, Algebraic K-theory, W.A. Benjamin, Inc., (1968).

[2] J. Coates, *Fragments of the GL_2 Iwasawa theory of elliptic curves without complex multiplication*, in Arithmetic Theory of Elliptic curves, ed. C. Viola, Lecture Notes in Math. 1716 (1997), 1–50.

[3] J. Coates, R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. 124 (1996), 124–178.

[4] J. Coates, S. Howson, *Euler characteristics and elliptic curves II*, Journal of Math. Society of Japan, 53 (2001), 175–235.

[5] J. Coates, R. Sujatha, *Euler-Poincaré characteristics of abelian varieties*, C.R. Acad. Sci. Paris, t.329, Série I (1999), 309–313.

[6] J. Coates, R. Sujatha, Galois cohomology of elliptic curves, TIFR Lecture Notes Series, Narosa Publishing house (2000).

[7] J. Coates, P. Schneider, R. Sujatha, *Modules over Iwasawa algebras*, Journal of the Inst. of Math Jussieu, 2 (2003), 73–108.

[8] J. Coates, R. Sujatha, J.-P. Wintenberger, *On the Euler-Poincaré characteristics of finite dimensional p-adic Galois representations*, Publ. Math. IHES, 93 (2001), 107–143.

[9] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math. 47 (1978), 85–99.

[10] R. Greenberg, *Iwasawa theory for Elliptic curves*, in Arithmetic Theory of Elliptic curves, ed. C. Viola, Lecture Notes in Math. 1716 (1997), 1–50.

[11] S. Howson, *Euler characteristics as invariants of Iwasawa modules*, Proc. London Math. Soc. 85 (2002), 634–658.

[12] Y. Hachimori, O. Venjakob, *Completely faithful Selmer groups over Kummer extensions*, this volume.

[13] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, To appear.

[14] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. IHES 26 (1965), 389–603.

[15] B. Mazur, *Rational points of abelian varieties in towers of number fields*, Invent. Math. 18 (1992), 183–266.

[16] B. Mazur, J. Tate, *The p-adic sigma function*, Duke Math. J. 62 (1991), 663-688.

[17] B. Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa, et points de Heegner*; Bull. Soc. Math. France 115 (1987), 399-456.

[18] B. Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adiques*, Invent. Math., 109 (1992), 137–185.

[19] P. Schneider, *p-adic height pairings II*, Invent. Math., 79 (1985), 329–374.

[20] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, Ann. of Math., 88 (1968), 492–517.

[21] B. Totaro, *Euler characteristics for p-adic Lie groups*; Publ. Math. IHES 90 (1999), 169–225.

[22] O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc. 4 (2002), 271–311.

[23] O. Venjakob, *A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory*, Jour. reine und angew. Math. 559 (2003), 153–191.

[24] Y. Ochi, O. Venjakob, *On the structure of Selmer groups over p-adic Lie extensions*; J. Alg. Geom. 11 (2002), 547–576.

John Coates
DPMMS, University of Cambridge
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB, England
j.h.coates@dpmms.cam.ac.uk

Peter Schneider
Mathematisches Institut
Westfälische Wilhelms-Universität
Einsteinstr. 62
D-48149 Münster, Germany
pschnei@math.uni-muenster.de

Ramdorai Sujatha
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai 400 005, India
sujatha@math.tifr.res.in