Pure and Applied Mathematics Quarterly
Volume 2, Number 2
(*Special Issue: In honor of
John H. Coates, Part 2 of 2*)
519—538, 2006

Iwasawa Theory and Modular Forms

R. Sujatha

Long ago a capital stood here
And its road leads back into the past
The flowers are in bloom
And who would think that springtime
Should pass as in a dream?

Dedicated to John Coates for his sixtieth birthday

The Iwasawa theory of elliptic curves without complex multiplication has been studied extensively in recent years ([2], [4], [17], [30], [22], [7]) culminating in the formulation of a Main Conjecture due to Coates, et al [3]. The main theme of this paper is to study the GL_2 Iwasawa theory of another important class of p-adic Galois representations, namely those arising from modular forms. We shall content ourselves with studying the algebraic questions that occur in this context and obtain results parallel to those proved for the Galois representations arising from elliptic curves.

More precisely, we study the Selmer groups (see §2) associated to the Galois representations coming from modular forms which are not CM (see §1). We shall thus be interested mainly in the case when the image G of the Galois representation is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$, and hence non-abelian. The Selmer group is then a finitely generated discrete (left) module over the non-commutative Iwasawa algebra $\Lambda(G)$ of G (see §2 for details). We remark that the Selmer group that we consider is actually the strict Selmer group in Greenberg's terminology [9] but all our main results (Theorem 2.8 and Theorem 4.1) also hold for the Selmer group as defined in [9] as the two Selmer groups differ by a cofinitely generated $\mathbb{Z}_p$-module. We prove (Theorem 2.8) that the dual Selmer group tensored with $\mathbb{Q}_p$ is

Received October 5, 2005.

infinite dimensional over $\mathbb{Q}_p$. Let L be a finite extension of $\mathbb{Q}$ such that $\mathrm{Gal}(K_\infty/L)$ is pro-p, where K_∞ denotes the trivializing extension of the representation associated to the modular form. We also show that the dual Selmer group over L^{cyc} is infinite for the primitive modular forms of level 1 and even weight and that it even has positive λ-invariant under additional hypotheses (see Theorem 4.1), which is conjectured to hold in general. The corresponding results for the representations coming from elliptic curves can be found in [17], [4], [22] and our methods are similar.

The paper consists of four sections. Section 1 is preliminary in nature where we gather various notation and definitions. In §2, we define the Selmer group which is the main object of study and prove that its dual tensored with $\mathbb{Q}_p$ is infinite dimensional as a $\mathbb{Q}_p$-vector space. In §3, we show that the dual Selmer group has no non-zero pseudo-null submodules and use these results in §4 to get information on the dual Selmer group over cyclotomic extensions.

Acknowledgements: It is a great pleasure to thank John Coates for the numerous mathematical discussions over the years on Iwasawa theory which were immensely insightful and beneficial. We gratefully acknowledge the hospitality of the Morningside Centre and thank the organisers of the conference held in Beijing in honour of J. Coates. We would also like to thank L. Clozel, E. Ghate, D. Prasad and R. Greenberg for useful discussions and the referee for his detailed comments.

1. Preliminaries

Let $f \in S_k(N)$ be a primitive cuspidal modular form of positive weight $k \geq 2$, level N and trivial character for the group $\Gamma_0(N)$. For simplicity, we assume that the Fourier coefficients of f lie in the field $\mathbb{Q}$ of rational numbers. Thus the Fourier expansion of f is of the form

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \quad q = e^{2\pi i z}, \ a_n \in \mathbb{Q}.$$

Let $\overline{\mathbb{Q}}$ (resp. $\overline{\mathbb{Q}}_p$) denote a fixed algebraic closure of $\mathbb{Q}$ (resp. $\mathbb{Q}_p$). We fix an embedding i_p of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_p$ and i_∞ of $\overline{\mathbb{Q}}$ into the field $\mathbb{C}$ of complex numbers. By the results of Eichler, Shimura and Deligne, there is an associated Galois representation, which we denote by

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_p) \tag{1}$$

having the property that at all primes $l \nmid Np$, the representation ρ_f is unramified and

$$\mathrm{tr}(\rho_f(\mathrm{Frob}_l)) = a_l,\ \det(\rho_f(\mathrm{Frob}_l)) = l^{k-1},$$

where a_l is the l^{th} Fourier coefficient of f and Frob_l denotes the Frobenius element at l.

Let V be the two dimensional $\mathbb{Q}_p$-vector space associated to ρ_f. We choose a lattice T left invariant by the Galois action. Then the image of ρ_f may be assumed to be a compact p-adic Lie subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$. After conjugation, one may therefore assume that ρ_f takes values in $\mathrm{GL}_2(\mathbb{Z}_p)$. Let

$$\rho_{f,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/p^n) \tag{2}$$

be the reduction of ρ_f mod p^n. Note that the lattice T is not unique and therefore the representation $\rho_{f,n}$ depends on the choice of the lattice T.

We denote by K_∞ the trivializing extension for the representation ρ_f so that the Galois group $G := \mathrm{Gal}(K_\infty/\mathbb{Q})$ is isomorphic to the image of ρ_f. For $n \geq 1$, we define the field K_n as the finite extension of $\mathbb{Q}$ in K_∞ corresponding to the extension trivializing the representation $\rho_{f,n}$ which implies that $\mathrm{Gal}(K_n/\mathbb{Q})$ is isomorphic to the image of $\rho_{f,n}$. The Galois group $\mathrm{Gal}(K_\infty/K_1)$ is a pro-p group, being contained in the kernel of the reduction map from $\mathrm{GL}_2(\mathbb{Z}_p)$ to $\mathrm{GL}_2(\mathbb{Z}/p)$. Let

$$\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_p^\times \tag{3}$$

be the cyclotomic character giving the action of the Galois group of $\mathbb{Q}$ on all p-power roots of unity. As $\det(\rho_f) = \chi^{k-1}$ and the fixed field of the kernel of χ^{k-1} clearly contains the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}^{\mathrm{cyc}}$ of $\mathbb{Q}$, we see that $\mathbb{Q}^{\mathrm{cyc}} \subseteq K_\infty$. Note also that if the reduced representation $\rho_{f,1}$ is reducible and contains μ_p as a sub-representation, then the field $\mathbb{Q}(\mu_p)$ is contained in K_1 and in this case the Galois group $G(K_\infty/\mathbb{Q}(\mu_p))$ is also pro-p.

Hypothesis: We shall assume throughout the paper that f is *ordinary* at p.

Recall that this means that a_p is a p-adic unit. Let $\mathfrak{p}$ be the prime of $\overline{\mathbb{Q}}$ induced by the embedding i_p. We shall again denote by $\mathfrak{p}$ the restriction of $\mathfrak{p}$ to any subfield of $\overline{\mathbb{Q}}$. Let $\mathcal{D}_p$ denote the decomposition group at p determined by the embedding i_p. Recall [9] that the representation V is *ordinary at p* if it has a one dimensional $\mathbb{Q}_p$-subspace $F^+(V)$ which is left invariant under the action of $\mathcal{D}_p$ with the property that the inertial subgroup I_p acts via a power of the cyclotomic character on $F^+(V)$ and trivially on the one dimensional quotient. The work of Mazur-Wiles [21] shows that if f is ordinary at p, then the associated representation is ordinary at p and that the image of the decomposition group under ρ_f is upper triangular. Let $F/\mathbb{Q}$ be any finite extension of $\mathbb{Q}$, and for each place w of F lying above p, fix a place $\overline{w}$ of $\overline{\mathbb{Q}}$ lying above w and let $\mathcal{D}_w$ denote the decomposition group for $\overline{w}$. It is easily seen that a Galois conjugate of F^+V then provides a one dimensional subspace $F_w^+(V) \subset V$ with the property that the inertia subgroup acts by a power of the cyclotomic character on this subspace and trivially on the one dimensional quotient.

We shall need the following results on CM and non-CM modular forms (cf. [25]). If f is a CM modular form, then the Lie algebra of the image of ρ_f is abelian over $\mathbb{Q}_p$ of dimension 2 while for non-CM modular forms, the Lie algebra of the image of ρ_f is the Lie algebra of $\mathrm{GL}_2(\mathbb{Q}_p)$ and consists of all 2×2 matrices over $\mathbb{Q}_p$. Suppose in addition that the modular form f is ordinary at p. Then the image under ρ_f of a decomposition group at p, as mentioned above, is upper triangular. More precisely, there is a basis of V in which the restriction $\rho_f \mid \mathcal{D}_p$ consists of matrices of the form

$$\begin{pmatrix} \delta & u \\ 0 & \epsilon \end{pmatrix}$$

where $\delta,\ \epsilon : \mathcal{D}_p \to \mathbb{Q}_p^\times$ are characters with ϵ unramified and $u : \mathcal{D}_p \to \mathbb{Q}_p^\times$ is a continuous function. The representation $\rho_f \mid \mathcal{D}_p$ is said to be *split at p* if $V = V_1 \oplus V_2$ where each V_i is a line, stable under $\mathcal{D}_p$. It is conjectured that $\rho_f \mid \mathcal{D}_p$ is split if and only if f is a CM modular form. It is known that if f is a CM modular form, then $\rho_f \mid \mathcal{D}_p$ is split and there are partial results providing strong evidence for the converse (see [14]).

From now on, we fix a lattice T which is stable under the Galois action and consider the discrete module $A := V/T$, so that $A \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^2$. Let C_p be the discrete submodule of A which is the image of $F^+(V)$ in A and put W_p for the discrete quotient A/C_p.

For a finite extension F of $\mathbb{Q}$, let $S(F)$ denote the finite set of primes in F consisting of those that lie above the primes that divide pN. We shall often omit the reference to the field F and use just S to lighten notation. As is usual, we denote by F_S the maximal extension of F unramified outside of S and the archimedean primes. Note that the field $\mathbb{Q}_S$ contains the extension K_∞ and the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}^{\mathrm{cyc}}$ of $\mathbb{Q}$.

2. Selmer groups

Let p be an odd prime. For any profinite group G, we shall define the Iwasawa algebra of G by $\Lambda(G)$. Recall that this is defined as the inverse limit

$$\varprojlim \mathbb{Z}_p[G/H]$$

where H varies over the open normal subgroups of G and the inverse limit is taken with respect to the natural maps.

We consider a modular form f as in §1, its associated representation ρ_f and denote the image of ρ_f by G. Let S denote the set of primes of $\mathbb{Q}$ containing the primes dividing Np defined above. The main object of study will be a *Selmer group* which is a (left) module over the Iwasawa algebra $\Lambda(G)$ as explained below. Let $F/\mathbb{Q}$ be any finite extension of $\mathbb{Q}$, and for each place w of F, fix a place $\overline{w}$ of $\overline{\mathbb{Q}}$ lying above w and let $\mathcal{D}_w$ denote the decomposition group for $\overline{w}$. As f is an ordinary modular form, the representation is ordinary at p. Further, as mentioned before, it follows from the results of Mazur-Wiles that for each place w of F lying above p, there exists a 1-dimensional subspace $F_w^+V \subset V$ such that
(i) $F_w^+(V)$ is stable under the action of the decomposition group $\mathcal{D}_w$ at w,
(ii) The inertia subgroup of $\mathcal{D}_w$ acts on F_w^+V via a power of the cyclotomic character,
(iii) The quotient V/F_w^+V is unramified.

Let C_w denote the image of F_w^+V in V/T and put W_w for the quotient A/C_w. For each place v of $S = S(F)$ and a finite extension L of F, define

$$J_v(L) = \begin{cases} \underset{w|v}{\oplus} H^1(\mathcal{D}_w, A) & \text{if } v \neq p \\ \underset{w|v}{\oplus} H^1(\mathcal{D}_w, W_w) & \text{if } v = p. \end{cases}$$

For an infinite extension $\mathcal{L}$ of $\mathbb{Q}$ contained in $\mathbb{Q}_S$, we set

$$J_v(\mathcal{L}) = \varinjlim J_v(L)$$

where L varies over finite extensions of F in $\mathcal{L}$ and the direct limit is taken with respect to the restriction maps. Following Greenberg [9], we define the *Strict Selmer group* $S_A(\mathcal{L})$ for any extension $\mathcal{L}$ of $\mathbb{Q}$ in K_∞ by

$$(4) \qquad S_A(\mathcal{L}) = \text{Ker } (\lambda(\mathcal{L}) : \ H^1(\mathbb{Q}_S/\mathcal{L}, A) \rightarrow \underset{v \in S}{\oplus} J_v(\mathcal{L})),$$

where $\lambda(\mathcal{L})$ is the natural map induced by restriction.

The definition does in fact depend on the choice of the lattice. However the conclusions of the theorems in this section and the subsequent ones are valid for *any* lattice T of V and in that sense, our main results are independent of the chosen lattice. In Greenberg's terminology [9], the *Selmer group*, which we denote here by $S'_A(L)$, is defined by replacing the decomposition groups in the definition of $J_v(\mathcal{L})$ by the corresponding inertial subgroups. With these definitions, the strict Selmer group is clearly contained in the Selmer group. These Selmer groups are discrete (left) modules over

$\Lambda(G)$ and we shall consider their compact duals. Let $X_A(K_\infty)$ (respectively $X'_A(K_\infty)$) be the Pontryagin dual of $S_A(K_\infty)$ (resp. of $S'_A(K_\infty)$). Our main result in this section is that $X_A(K_\infty) \otimes \mathbb{Q}_p$ is infinite dimensional as a $\mathbb{Q}_p$-vector space. By the above remark, this will also imply the infinite dimensionality of the Selmer group as defined by Greenberg. *We shall therefore consider only the Strict Selmer group and by abuse of terminology refer to it as the Selmer group.* It can be checked that the Strict Selmer group and the Selmer group differ in general by a cofinitely generated $\mathbb{Z}_p$-module. We also remark that in the special case of the representations associated to elliptic curves over number fields, the definition of the Selmer group given here differs slightly from the usual definition. However, we shall mainly be working with Selmer groups over deeply ramified extensions, and over these infinite extensions the two groups coincide.

As it is important to work with pro-p groups, we shall most often put $K_1 = K$ and consider the Selmer group and its dual as modules over the Iwasawa algebra $\Lambda(G_K)$, where G_K is the pro-p group $G_K = \mathrm{Gal}(K_\infty/K)$ (cf. §1). It is then an easy consequence of Nakayama's lemma (cf. [2]) that $X_A(K_\infty)$ is finitely generated as a $\Lambda(G_K)$-module. We want to show that $X_A(K_\infty) \otimes \mathbb{Q}_p$ is finite dimensional as a $\mathbb{Q}_p$-vector space. The corresponding result for the case of the ordinary p-adic representation coming from elliptic curves without complex multiplication is in [4]. The proof there follows ideas outlined by Greenberg and our proof is somewhat similar.

We have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & S_A(K_\infty)^{G_n} \arrow[r] & H^1(\mathbb{Q}_S/K_\infty, A)^{G_n} \arrow[r] & \bigoplus_{v \in S_n} J_v(K_\infty)^{G_n} \\
0 \arrow[r] & S_A(K_n) \arrow[r] \arrow[u, "f_n"] & H^1(\mathbb{Q}_S/K_n, A) \arrow[r] \arrow[u, "g_n"] & \bigoplus_{v \in S_n} J_v(K_n) \arrow[u, "h_n"]
\end{tikzcd} \tag{5}$$

where $G_n := \mathrm{Gal}(K_\infty/K_n)$, $S_n := S(K_n)$ and $h_n = \underset{v \in S_n}{\oplus} h_{n,v}$ is the sum of the local restriction maps.

Lemma 2.1. *The kernel and cokernel of g_n are finite.*

Proof. This can be proved using Lie algebra techniques as in [28]. As the Lie algebra of G_n is either abelian of dimension 2 over $\mathbb{Q}_p$ or equal to the Lie algebra of $\mathrm{GL}_2(\mathbb{Q}_p)$ depending on whether f is CM or non-CM, the proof is particularly simple and we refer the reader to [6, Appendix] for the main ideas. □

Let K_n^{cyc} denote the cyclotomic $\mathbb{Z}_p$-extension of K_n where the fields K_n are as in §1 and denote by H_n the Galois group $\mathrm{Gal}(K_\infty/K_n^{\mathrm{cyc}})$ for $n \geq 1$. We consider the Selmer groups $S_A(K_n^{\mathrm{cyc}})$ in the diagram below:

$$\begin{tikzcd}
0 \arrow[r] & S_A(K_\infty)^{H_n} \arrow[r] & H^1(\mathbb{Q}_S/K_\infty, A)^{H_n} \arrow[r] & \bigoplus_{v\in S_n} J_v(K_\infty)^{H_n} \\
0 \arrow[r] & S_A(K_n^{\mathrm{cyc}}) \arrow[r] \arrow[u, "\alpha_n"] & H^1(\mathbb{Q}_S/K_n^{\mathrm{cyc}}, A) \arrow[r, "\lambda(K_n^{\mathrm{cyc}})"] \arrow[u, "\beta_n"] & \bigoplus_{v\in S_n} J_v(K_n^{\mathrm{cyc}}). \arrow[u, "\gamma_n"]
\end{tikzcd} \tag{6}$$

Here the vertical maps are the natural restriction maps and $\gamma_n = \oplus\gamma_{n,v}$ as v runs over all the primes of $S_n := S(K_n)$. Recall that there are only a finite number of primes in K_n^{cyc} lying over any finite prime of K_n.

Lemma 2.2. *The kernel and cokernel of β_n are finite.*

Proof. We have Ker $\beta_n = H^1(H_n, A)$ and Coker $\beta_n \subseteq H^2(H_n, A)$. One sees that the cohomology groups $H^1(H_n, A)$ and $H^2(H_n, A)$ are finite by an argument entirely analogous to that in [5]. The key observation needed is that $A^{H_n} = A(K_n^{\mathrm{cyc}})$ is finite. As the Lie algebra of H_n is either one dimensional or equal to the Lie algebra of SL_2 (depending on whether f is CM or non-CM), the above finiteness statements follow easily from the vanishing of $H^0(\mathfrak{h}, V)$ where $\mathfrak{h}$ is the Lie algebra of H_n. Note that the Lie algebras of H_n coincide for all n as H_{n+1} is an open subgroup of H_n. If f is a CM modular form, then $\mathfrak{h}$ is abelian of dimension 1 and consists of diagonal matrices of trace zero. If f is a non-CM modular form then $\mathfrak{h}$ has dimension 3 and consists of all 2×2 matrices of trace zero. In both these cases, it is then easily verified that $H^0(\mathfrak{h}, V)$ is zero. This in turn implies the vanishing of $H^i(\mathfrak{h}, V)$ for $i = 1,\ 2$ as in [5] and the lemma follows. □

Lemma 2.3. *Let Γ_n denote the Galois group* $\mathrm{Gal}(K_n^{\mathrm{cyc}}/K_n)$*. If $S_A(K_n^{\mathrm{cyc}})$ is co-torsion as a $\Lambda(\Gamma_n)$-module, then the homomorphism $\lambda(K_n^{\mathrm{cyc}})$ in* (6) *is surjective.*

Proof. This is certainly well-known and classical for the case of Galois representations coming from elliptic curves, see [16, Proposition 2.3] for a proof. Similar arguments with the Poitou-Tate sequence show that the proof carries over in this general case as well. □

Given a prime l of $\mathbb{Q}$ in S, let w denote a prime of K_∞ above l, where by a prime of K_∞, we mean a compatible sequence of primes at each finite extension of K_n in K_∞. Let $\mathcal{G}_{n,w} \subseteq G_n$ and $\mathcal{H}_{n,w} \subset H_n$ denote the intersection respectively of G_n and H_n with the corresponding decomposition groups of w over l. Recall that there are only finitely many primes in K_n^{cyc} lying above any prime of S.

Lemma 2.4. *For a prime v of $S(K_n)$, let $h_{n,v}$ (respectively $\gamma_{n,v}$) denote the corresponding local component of the local restriction map h_n (resp. γ_n). Then*

$$\operatorname{Ker}(h_{n,v}) = \begin{cases} H^1(\mathcal{G}_{n,w}, A) & \text{if } v \nmid p, \\ H^1(\mathcal{G}_{n,w}, A/C_w) & \text{if } v \mid p \end{cases} \tag{7}$$

$$\operatorname{Ker}(\gamma_{n,v}) = \begin{cases} \bigoplus\limits_{v'} H^1(\mathcal{H}_{n,w}, A) & \text{if } v \nmid p, \\ \bigoplus\limits_{v'} H^1(\mathcal{H}_{n,w}, A/C_w) & \text{if } v \mid p, \end{cases} \tag{8}$$

where in (8), *the sum varies over the finite set of primes v' of K_n^{cyc} which lie above v, and w denotes some fixed prime of K_∞ lying above v'.*

Proof. We indicate the proof for (7), the other case being entirely parallel. Given $v \in S(K_n)$, we first note that by Shapiro's lemma, we have

$$(J_v(K_\infty))^{G_n} \simeq \begin{cases} H^0(\mathcal{G}_{n,w}, H^1(K_{\infty,w}, A)) \text{ if } v \nmid p \\ H^0(\mathcal{G}_{n,w}, H^1(K_{\infty,w}, A/C_w) \text{ if } v \mid p \end{cases}$$

where $K_{\infty,w}$ denotes the completion of K_∞ at any prime w of K_∞ lying above v. Therefore

$$\operatorname{Ker}(h_{n,v}) = \operatorname{Ker}(H^1(K_{n,v}, B) \to H^1(K_{\infty,w}, B)^{\mathcal{G}_{n,w}})$$

where $B = A$ or A/C_w according as $v \nmid p$ or $v \mid p$. By the usual inflation-restriction sequence, we see that (7) holds. □

Lemma 2.5. *Let l be any prime, distinct from p, which divides N.*
(i) If $l^2 \nmid N$, and $v \mid l$ in $S(K_n)$, then for $n >> 0$, the group $\operatorname{Ker}(\gamma_{n,v})$ *has $\mathbb{Z}_p$-corank at least 1.*
(ii) If $l^2 \mid N$, then $\operatorname{Ker}(\gamma_{n,v})$ *is trivial for a prime $v \mid l$ in $S(K_n)$ for $n >> 0$, provided the image of the inertial subgroup at v is finite, and* $\operatorname{Ker}(\gamma_{n,v})$ *is infinite otherwise.*

Proof. (*i*) Let w be a prime of $\overline{\mathbb{Q}}$ lying above $v \mid l$. Our hypotheses that the prime $l^2 \nmid N$ and $l \neq p$ ensures that the image $\mathcal{G}_w$ of the decomposition group at w under ρ_f is of dimension 2. This follows on using the results of Carayol ([1], cf. [29, §3]). Indeed, in this case, the corresponding inertial subgroup $\mathcal{I}_w$ of $\mathcal{G}_w$ is one dimensional and hence not finite. By the classical local monodromy theorem of Grothendieck (cf. [13]), as $l \neq p$, the representation ρ_f when restricted to an open subgroup of the inertia subgroup at w has image consisting of matrices which are unipotent. Let $\mathcal{H}_{n,w} = H_n \cap \mathcal{G}_w$. As the trace of the elements in the Lie algebra of $\mathcal{H}_{n,w}$ is zero, we see that the Lie algebra of the image of the inertial subgroup is contained in the image of the Lie algebra of $\mathcal{H}_{n,w}$. But $\mathcal{H}_{n,w}$ is a closed subgroup of $\mathcal{G}_w$ of dimension at most one less than the dimension of $\mathcal{G}_w$. In fact, it is true that in this case the dimension of $\mathcal{H}_{n,w}$ is one (cf. [29, p. 71]). Combining this with the above inclusion, we see that the Lie algebras of $\mathcal{H}_{n,w}$ and $\mathcal{I}_w$ coincide and is in fact nilpotent. Let $\mathfrak{n}$ denote this Lie algebra. By Engel's theorem, we therefore have $H^0(\mathfrak{n}, V)$ has dimension at least 1. This translates to the result that $H^0(\mathcal{H}_{n,w}, V)$ has dimension at least 1 for $n >> 0$ (we simply take n large enough to include the finite extension L of $\mathbb{Q}_l$ such that the image of the inertial subgroup of L is unipotent). We thus get a corresponding divisible subgroup B of A isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ on which $\mathcal{H}_{n,w}$ acts trivially. Hence

$$\mathrm{Ker}(\gamma_{n,v}) = H^1(\mathcal{H}_{n,w}, A) \supset H^1(\mathcal{H}_{n,w}, B) = \mathrm{Hom}(\mathcal{H}_{n,w}, \mathbb{Q}_p/\mathbb{Z}_p).$$

This latter group is easily seen to be infinite with $\mathbb{Z}_p$-corank at least 1.

(ii) If $l^2 \mid N$, then the representation ρ_f restricted to the decomposition group has dimension at most 2. Indeed, if the image of the inertial subgroup is finite, then $\mathcal{G}_{n,w}$ is isomorphic to $\mathbb{Z}_p$ and is topologically generated by the Frobenius for n sufficiently large. In this case, the subgroup $\mathcal{H}_{n,w}$ is trivial for $n >> 0$ and the same is true for $\mathrm{Ker}(\gamma_{n,v})$. If the image of the inertial subgroup is infinite, then the arguments as in (i) apply and the lemma follows. □

Remark 2.6. Consider a prime w of $\overline{\mathbb{Q}}$ lying over a prime $q \in S \setminus \{p\}$, and its restriction to K_∞. It is clear from the above proof (see also [29, §3]) that the image $\mathcal{G}_w$ of the decomposition group $\mathcal{D}_w$ at w is a p-adic Lie group of dimension at most 2 if f is non-CM and of dimension 1 if f is CM. Therefore its dimension is strictly less than the dimension of G. Hence the corresponding number of primes of K_n lying above q is unbounded as $n \to \infty$ in these cases. If w lies over p and f is not CM, then the decomposition group $\mathcal{D}_w$ is of dimension at most three and hence the number of primes of K_n lying above q is again infinite. We shall use this later in the proof of the main theorem of this section.

Proposition 2.7. *Assume that the modular form f is non-CM. Then the group* $\mathrm{Ker}(h_n)$ *contains* $(\mathbb{Z}/p^{k_n})^{t_n}$ *where* $k_n \geq 1$ *and both* $k_n,\ t_n \to \infty$ *as* $n \to \infty$.

Proof. As we have assumed the modular form f to be ordinary, the representation is ordinary at p. As remarked earlier, for any prime w lying above p in the finite extensions K_n of $\mathbb{Q}$, there is then a submodule C_w of A isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ which is invariant under the action of the decomposition group $\mathcal{D}_w$ and such that on the quotient $W_w = A/C_w$ the action of $\mathcal{D}_w$ is unramified. Consider a prime $v \mid p$ in $S(K_n)$. By Lemma 2.4, we have $\mathrm{Ker}(h_{n,v}) = H^1(\mathcal{G}_{n,w}, W_w)$ where $\mathcal{G}_{n,w} \subseteq G_n$ is the image of the decomposition group at a prime w of K_∞ lying over v. Let $\mathcal{I}_{n,w} \subset \mathcal{G}_{n,w}$ denote the image under ρ_f of the corresponding inertial subgroup. The subgroup $\mathcal{I}_{n,w}$ is of codimension 1 in $\mathcal{G}_{n,w}$ (cf. [29, §3.2]). As f is not CM, the group $\mathcal{G}_{n,w}$ consists of upper triangular matrices and hence has dimension at most

3 while $\mathcal{I}_{n,w}$ has dimension at most 2 and acts trivially on W_w. By the Hochschild-Serre spectral sequence, we have a surjection

$$H^1(\mathcal{G}_{n,w}, W_w) \twoheadrightarrow H^0(\Gamma_{n,w}, H^1(\mathcal{I}_{n,w}, W_w)) \tag{9}$$

where $\Gamma_{n,w} = \mathcal{G}_{n,w}/\mathcal{I}_{n,w}$ is isomorphic to $\mathbb{Z}_p$ generated by the appropriate Frobenius element. We now use the fact that $\mathcal{I}_{n,w}$ acts trivially on W_w and hence

$$H^1(\mathcal{I}_{n,w}, W_w) = \mathrm{Hom}(\mathcal{I}_{n,w}/[\mathcal{I}_{n,w}, \mathcal{I}_{n,w}], W_w). \tag{10}$$

On the other hand, by the above remarks on the inertial subgroups (cf. [29, Theorem 4], one sees easily that $\mathcal{I}_{n,w}/[\mathcal{I}_{n,w}, \mathcal{I}_{n,w}]$ is abelian of dimension 1 for $n >> 0$. Hence the group in (10) is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p(\epsilon)$ as a $\Gamma_{n,w}$-module for some character $\epsilon : \Gamma_{n,w} \to \mathbb{Z}_p^*$. If the action is trivial, then $\mathrm{Ker}(h_{n,v})$ is clearly infinite. If on the other hand ϵ is non-trivial, then the group (10) is finite of order p^{k_n} say, with $k_n \neq 0$. In fact, in this case it is easily seen that

$$p^{k_n} = H_0(\Gamma_{n,w}, \mathbb{Z}_p(\epsilon)) = \chi(\Gamma_{n,w}, \mathbb{Z}_p(\epsilon)), \tag{11}$$

where for a compact module M over Γ isomorphic to $\mathbb{Z}_p$,

$$\chi(G, M) = \#\, H_0(G, M)/\#\, H_1(G, M)$$

is the Euler characteristic which is defined when the homology groups are finite.

For $m \geq 0$, the index $[\Gamma_{n,w} : \Gamma_{n+m,w}] = p^m$ and as $\chi(\Gamma_{n+m,w}, M) = p^m \chi(\Gamma_{n,w}, M)$, we see that

$$p^{k_{n+m}} = p^m \cdot p^{k_n}, \tag{12}$$

and therefore

$$H^1(\mathcal{G}_{n,w}, W_w) \supseteq (\mathbb{Z}/p^{k_n}\mathbb{Z}) \tag{13}$$

with $k_n \geq 1$ and $k_n \to \infty$ as $n \to \infty$. Clearly

$$\mathrm{Ker}(h_n) \supseteq \underset{w|p}{\oplus} H^1(\mathcal{G}_{n,w}, W_w) \tag{14}$$

where the sum is taken over all the primes w in K_n dividing p. The proposition now follows from (13), (14) and Remark 2.6. □

We can now prove

Theorem 2.8. *Let f be primitive cuspidal modular form of positive weight $k \geq 2$, level N and ordinary at p. Assume further that f is not CM. With notation as before, the group $X_A(K_\infty) \otimes \mathbb{Q}_p$ is infinite dimensional over $\mathbb{Q}_p$.*

Proof. To prove that $X_A(K_\infty) \otimes \mathbb{Q}_p$ is infinite dimensional over $\mathbb{Q}_p$, as in [4], we first consider the restriction map

$$\alpha_n : S_A(K_n^{\mathrm{cyc}}) \to S_A(K_\infty)^{H_n}. \tag{15}$$

By Lemma 2.2, it has finite kernel. Let $\Gamma_n = \mathrm{Gal}(K_n^{\mathrm{cyc}}/K_n)$. If $X_A(K_n^{\mathrm{cyc}})$ is not $\Lambda(\Gamma_n)$-torsion, then $X_A(K_\infty)$ is obviously infinite dimensional. We therefore assume that $X_A(K_n^{\mathrm{cyc}})$ is $\Lambda(\Gamma_n)$-torsion for all $n = 1,\ 2, \cdots$. By Lemma 2.3, this implies that the map $\lambda(K_n^{\mathrm{cyc}})$ in the bottom row of (6) is surjective. The infinite dimensionality will then follow if we show that the $\mathbb{Z}_p$-corank of $\mathrm{Coker}(\alpha_n)$ is unbounded as $n \to \infty$. By the snake lemma applied to (6), this is equivalent to showing that

$$\mathbb{Z}_p - \text{corank of } (\text{Ker } \ \gamma_n) \text{ is unbounded as } n \to \infty \tag{16}$$

where γ_n is the map as in (6).

If the set $S(K_n)$ contains primes dividing N with the property that the image of the corresponding inertia groups under ρ_f is infinite, then the theorem is true. Indeed, observing that the number of primes in K_n dividing such primes of S tends to infinity as $n \to \infty$, we see that (16) is true by Lemma 2.5 and Remark 2.6. We therefore assume that $S(K_n)$ contains only primes dividing p and analyse the diagram (5). We consider the restriction map

$$f_n : S_A(K_n) \to S_A(K_\infty)^{G_n}.$$

Then the same argument as in [4, Lemma A.2] shows that

$$\mathrm{Ker}(g_n) \simeq (\mathbb{Z}/p^n)^6, \ \text{ for } n \geq 1. \tag{17}$$

Consider the homomorphism

$$\lambda(K_n) : H^1(\mathbb{Q}_S/K_n, A) \to \underset{v \in S}{\oplus} J_v(A)$$

whose kernel is $S_A(K_n)$. Using the Poitou-Tate sequence, the arguments in [4, p. 231-232] along with Proposition 2.7 apply in this situation to show that

$$(\mathbb{Z}/p^{k_n})^{t_n} \hookrightarrow \mathrm{Ker}(h_n) \cap \mathrm{Im}(\lambda(K_n))$$

and both $t_n,\ k_n \to \infty$ as $n \to \infty$. Combining this with (17), the snake lemma applied to (5) proves that

$$(\mathbb{Z}/p^{k_n'})^{t_n'} \hookrightarrow \mathrm{Coker}(f_n). \tag{18}$$

Thus $S_A(K_\infty)^{G_n}$ maps onto $\mathrm{Coker}(f_n)$ which contains a subgroup $(\mathbb{Z}/p^{k_n'})^{t_n'}$ with the property that both $k_n',\ t_n' \to \infty$ as $n \to \infty$. As the p-primary torsion in $S_A(K_\infty)$ is of finite exponent, one concludes as in [4, Appendix]. □

3. Non-existence of pseudo-null submodules

Recall that $G = \mathrm{Gal}(K_\infty/\mathbb{Q})$ and let $\Lambda(G)$ be the corresponding Iwasawa algebra. We consider $X_A(K_\infty)$ as a compact finitely generated $\Lambda(G)$-module. The aim of this section is to prove that $X_A(K_\infty)$ has no non-trivial pseudo-null $\Lambda(G)$-submodules. Recall ([30], [7]) that a finitely generated left module M over a noetherian Auslander regular ring R is said to be *pseudo-null* if the group $E^i(M) := \mathrm{Ext}^i_R(M, R) = 0$ for $i = 0,\ 1$. We follow the arguments of Ochi-Venjakob in [22] where they consider the case of p-adic representations coming from abelian varieties. The one point that we want to stress here is that for the case of representations coming from non-CM ordinary modular forms, it is still a conjecture (albeit with considerable evidence, cf. [14]) that the local decomposition group $\mathcal{G}_p$ has dimension at least 3, which is part of the hypotheses of [22, Theorem 5.2]. However, an extension of their methods allows us to prove the result in general for non-CM modular forms.

For any extension L of $\mathbb{Q}$ in K_∞, let $\lambda(L)$ denote the map

$$\lambda(L) : H^1(\mathbb{Q}_S/L, A) \to \underset{v\in S(L)}{\oplus} J_v(L). \tag{19}$$

We assume that the map $\lambda(K_\infty)$ is surjective. By standard arguments (see [2, Theorem 4.5] for the case of elliptic curves), this is equivalent to the module $X_A(K_\infty)$ being $\Lambda(G)$-torsion. Let $\mathcal{X}_S = \mathcal{X}_S(A/K_\infty)$ denote the compact Pontryagin dual of $H^1(\mathbb{Q}_S/K_\infty, A)$, considered as a $\Lambda(G)$-module. We note also that the Galois group $H^2(\mathbb{Q}_S/K_\infty, A)$ is trivial (cf. [2, §2.5]). Using this along with the Fox-Lyndon resolution technique (see [20], [22, §4.1]), one sees that $\mathcal{X}_S(A/K_\infty)$ is contained in a $\Lambda(G)$-module Y which has projective dimension at most 1 and hence has no non-trivial pseudo-null $\Lambda(G)$-submodule (cf. [22, Theorem 4.6]).

Theorem 3.1. *Let $X_A(K_\infty)$ be the dual of the Selmer group where $A = V/T$ is the divisible module attached to the representation ρ_f for a non-CM ordinary cuspidal primitive modular form f of weight ≥ 2 and level N which is square free. Assume that $X_A(K_\infty)$ is a torsion $\Lambda(G)$-module. Then $X_A(K_\infty)$ has no non-trivial pseudo-null submodule.*

Proof. As mentioned above, the result follows from [22, Theorem 5.2] when the local image $\mathcal{G}_p$ has dimension at least 3, noting that our hypothesis ensures that for $l \in S \setminus \{p\}$, the image $\mathcal{G}_l$ has dimension 2 (see the proof of Lemma 2.5). We assume therefore that $\mathcal{G}_p$ has dimension 2. Now $\mathcal{G}_p$ consists of upper triangular matrices, and as the representation is assumed to be ordinary, the Frobenius acts non-trivially on the unramified quotient W_p. In particular, this implies that the local image $\mathcal{G}_p$ is necessarily split.

For a prime $l \in S$, we have the compact $\Lambda(\mathcal{G}_l)$-modules

$$\mathcal{X}_l := \begin{cases} H^1(\mathbb{Q}_{p,\infty}, W_p)^\vee \text{ } if \ l = p \\ H^1(\mathbb{Q}_{l,\infty}, A)^\vee \text{ } if \ l \in S \setminus p \end{cases}$$

where, as before, W_p denotes the quotient A/C_p and for a discrete $\Lambda(G)$-module M, $M^\vee$ denotes the Pontryagin dual. As in [22, §5], let U denote the $\Lambda(G)$-module

$$U = \mathrm{Ind}_{\mathcal{G}_p}^{G} \ \mathcal{X}_p \oplus \underset{l \in S \setminus p}{\oplus} \mathrm{Ind}_{\mathcal{G}_l}^{G} \mathcal{X}_l.$$

By our assumption that $\mathcal{G}_p$ has dimension 2 and the remarks above on $\mathcal{G}_p$, it follows from [20, 5.2 (c)] that

$$\mathcal{X}_p \oplus \Lambda(\mathcal{G}_p) \tilde{=} Y_p \tag{20}$$

where Y_p is the module defined by the exact sequence

$$0 \to \mathcal{X}_p \to Y_p \to I_p \to 0$$

and $I_p = \mathrm{Ker}(\Lambda(\mathcal{G}_p) \to \mathbb{Z}_p)$ (cf. [20, §4]) is the kernel under the augmentation map. Recall further that there is a $\Lambda(G)$-module Y [22, §4], and a similar exact sequence

$$0 \to \mathcal{X}_S \to Y \to I \to 0 \tag{21}$$

where $I = \mathrm{Ker}(\Lambda(\mathcal{G}) \to \mathbb{Z}_p)$ is the augmentation kernel. The $\Lambda(\mathcal{G}_p)$-module Y_p has projective dimension at most 1 [20], [22, §4], and Y has projective dimension at most 1 as a $\Lambda(G)$-module. By (20), it is clear that the projective dimension of $\mathcal{X}_p$ is also at most 1. As in [22, Proposition 2.4 and §5], the proof of the theorem will be complete if we can show that $E^iE^i(X_A(K_\infty)) = 0$ for all $i \geq 2$ where $E^i(M) := \mathrm{Ext}^i_{\Lambda(G)}(M, \Lambda(G))$. Since we have assumed that $X_A(K_\infty)$ is $\Lambda(G)$-torsion, which is equivalent to the map $\lambda(K_\infty)$ being surjective (cf. [2]), we have the following exact sequence of $\Lambda(G)$-modules:

$$0 \to U \to \mathcal{X}_S \to X_A(K_\infty) \to 0.$$

As the dimension of $\mathcal{G}_l$ is 2 for $l \in S \setminus p$ (see the proof of Lemma 2.5), the proof of [22, Lemma 5.4 (ii)] applied to this case shows that $\mathcal{X}_l$ is zero. The same arguments as in [22, Lemma 5.6] imply that the projective dimensions of $\mathcal{X}_S$ and $X_A(K_\infty)$ over $\Lambda(G)$ are at most 2 and hence $E^iE^i(X_A(K_\infty)) = 0$ for $i \geq 3$. We therefore need only to prove that $E^2E^2(X_A(K_\infty)) = 0$. The above exact sequence gives an exact sequence

$$E^1(X_A(K_\infty)) \to E^1(\mathcal{X}_S) \to E^1(U) \xrightarrow{s} E^2(X_A(K_\infty)) \to E^2(\mathcal{X}_S) \to E^2(U). \tag{22}$$

Let B denote the image of s in the above sequence. Then, as in the proof of [22, Theorem 5.2], it suffices to prove that $E^2(B) = 0$ as this will imply that $E^2E^2(X_A(K_\infty)) = 0$.

Claim $E^2(B) = 0$.

To prove the claim, we first note that as the dimension of G is 4 and $E^i(\mathbb{Z}_p) = 0$ for all $i \neq 4$ [20, Corollary 2.6], it follows from (21) that

$$E^1(\mathcal{X}_S) = E^1(Y). \tag{23}$$

Further by (20), we have

$$E^1_{\mathcal{G}_p}(\mathcal{X}_p) = E^1_{\mathcal{G}_p}(Y_p) \tag{24}$$

where $E^i_{\mathcal{G}_p}(M) = \mathrm{Ext}^i_{\Lambda(\mathcal{G}_p)}(M, \Lambda(\mathcal{G}_p))$. Let Z_A and $Z_p(W_p)$ respectively denote the global and local dualising modules of A over $\Lambda(G)$ and W_p over $\Lambda(\mathcal{G}_p)$, as in [22, Lemma 4.9(i), Proposition 4.10(i)]. As Y and Y_p have projective dimensions 1 respectively over the Iwasawa algebras $\Lambda(G)$ and $\Lambda(\mathcal{G}_p)$, we have

$$E^1(Y) = Z_A, \ E^1_{\mathcal{G}_p}(Y_p) = Z_p(W_p). \tag{25}$$

Here we have used the fact that Z_A is torsion as a $\Lambda(G)$-module (cf. [22, Proposition 4.10]). Further by [22, Lemma 4.9(i)], it follows that $Z_p(W_p)$ is a free $\mathbb{Z}_p$-module of rank 1. By [22, Lemma 5.4(iii)], we have $\mathcal{X}_l = 0$. We therefore have

$$E^1(U) = \mathrm{Ind}^G_{\mathcal{G}_p} \ E^1_{\mathcal{G}_p}(\mathcal{X}_p)$$

We drop the subscript and superscript in the induced module henceforth to lighten notation. By (24) and (25), we see that

$$E^1(U) = \mathrm{Ind} \ Z_p(W_p). \tag{26}$$

Combining this with (23) we get a commutative diagram

$$\begin{tikzcd}
Z_A \arrow[r, "u"] \arrow[d] & \mathrm{Ind} \ Z_p(W_p) \arrow[d] \\
E^1(Y) = E^1(\mathcal{X}_S) \arrow[r] \arrow[d] & E^1(U) \arrow[d] \\
0 & 0
\end{tikzcd}$$

where the vertical arrows are isomorphisms by (25). Consequently, by (22), the module B is isomorphic to the cokernel of the natural map $Z_A \to \mathrm{Ind} \ Z_p(W_p)$. On the other hand, it is clear that the group $\mathrm{Coker}(u)$ is a quotient of $\mathrm{Coker}(u')$, where u' is the natural map $u' : Z_A \to \mathrm{Ind} \ Z_p(A)$. Here $Z_p(A)$ is the dualising module of A over $\Lambda(\mathcal{G}_p)$ and there is clearly a natural surjective map $f : Z_p(A) \twoheadrightarrow Z_p(W_p)$. On applying projective limits to the classical Poitou-Tate sequence (see [23, 1.3.1]), one sees that the cokernel of u' is a free $\mathbb{Z}_p$-module of finite rank. In particular, the module

B is a finitely generated $\mathbb{Z}_p$-module. As the dimension of G is 4, we have $E^2(B) = 0$ which proves the claim.

We now use this in the exact sequence (22). As $\mathcal{X}_p$ has projective dimension atmost 1 over $\Lambda(\mathcal{G}_p)$, we see that $E^2(U) = \text{Ind } E^2(\mathcal{X}_p) = 0$. Therefore (22) gives an exact sequence

$$0 \to B \to E^2(X_A(K_\infty)) \to E^2(\mathcal{X}_S) \to 0.$$

As $\mathcal{X}_S$ is contained in Y which has projective dimension at most 1, we know that $\mathcal{X}_S$ has no non-trivial pseudo-null $\Lambda(G)$-submodule [22, Corollary 4.7 and Proposition 2.4]. Hence $E^iE^i(\mathcal{X}_S) = 0$ for $i \geq 2$. Combining this with the vanishing of $E^2(B)$, it follows that $E^2E^2(X_A(K_\infty)) = 0$ and the theorem is proved. □

Remark 3.2. (i) When f is a CM modular form, it is unclear whether the above methods apply as in this case both G and $\mathcal{G}_p$ have dimension 2. However, the technique used by Perrin-Riou in [24] should imply a similar result.

4. Selmer groups over the cyclotomic extension

In this section, we apply the results of the previous sections to study the Selmer group $X_A(L^{\text{cyc}})$ over L^{cyc} where L is a finite extension of $\mathbb{Q}$ contained in K_∞ such that $\text{Gal}(K_\infty/L)$ is pro-p and L^{cyc} denotes the cyclotomic $\mathbb{Z}_p$-extension of L. Let G_L denote the image of $\text{Gal}(K_\infty/L)$ under ρ_f. The main reason for working over such ground fields L is that the Iwasawa algebra $\Lambda(G_L)$ is then a local noetherian ring and we can apply Nakayama's lemma. Recall that $K = K_1 \subset K_\infty$ is the trivializing extension for the representation $\rho_{f,1}$ and that $\text{Gal}(K_\infty/K)$ is pro-p. We shall further make the hypothesis that $p \geq 5$ so that the Iwasawa algebras have no zero divisors. If the representation $\rho_{f,1}$ is reducible and contains μ_p as a subrepresentation, then the image of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p))$ under ρ_f is also pro-p. We may then take the field L to be $F := \mathbb{Q}(\mu_p)$ which is an abelian extension of $\mathbb{Q}$, instead of K. The advantage in working with F is that one can apply the deep result of Kato [19] proving that the Selmer group $X_A(F^{\text{cyc}})$ is torsion as a $\Lambda(\Gamma_F)$-module where $\Gamma_F = \text{Gal}(F^{\text{cyc}}/F)$, which in turn implies that the homomorphism $\lambda(F^{\text{cyc}})$ in (19) is surjective. For any field L as above, let $G_L := \text{Gal}(K_\infty/L)$ and $H_L := \text{Gal}(K_\infty/L^{\text{cyc}})$, and let G and H respectively denote the Galois groups $G_{\mathbb{Q}}$ and $H_{\mathbb{Q}}$. For any $\Lambda(G)$-module M, let $M(p)$ denote the submodule consisting of all p-power torsion elements. We shall denote by $\mathfrak{M}_H(G)$ the abelian category of finitely generated $\Lambda(G)$-modules M such that $M/M(p)$ is finitely generated when considered as a $\Lambda(H)$-module by restricting scalars. It seems reasonable to conjecture (see [3]) that the Selmer groups $X_A(K_\infty)$ are always in $\mathfrak{M}_H(G)$. With notation as before, our main result is the following:

Theorem 4.1. *Let ρ_f be the representation associated to an ordinary non-CM modular form f and let L be a finite extension of $\mathbb{Q}$ contained in K_∞ such that the Galois group $G := \mathrm{Gal}(K_\infty/L)$ is pro-p. Assume that $p \geq 5$ and that f has level 1. Then $X_A(L^{\mathrm{cyc}})$ is infinite. Moreover, if $X_A(K_\infty)$ is in $\mathfrak{M}_H(G)$, then $X_A(L^{\mathrm{cyc}}) \otimes \mathbb{Q}_p$ has positive dimension over $\mathbb{Q}_p$.*

Proof. We first assume that $X_A(K_\infty)$ is in $\mathfrak{M}_H(G)$ and prove the final assertion of Theorem 4.1. From the hypotheses on f, we see that the set $S := S(L)$ consists precisely of the primes that lie above p. We may clearly assume that $X_A(L^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion and hence that the map $\lambda(L^{\mathrm{cyc}})$ is surjective. We thus have the following commutative diagram:

(27)
$$\begin{tikzcd}
0 \arrow[r] & S_A(K_\infty)^{H_L} \arrow[r] & H^1(\mathbb{Q}_S/K_\infty, A)^{H_L} \arrow[r] & \bigoplus_{v\in S} J_v(K_\infty)^{H_L} & \\
0 \arrow[r] & S_A(L^{\mathrm{cyc}}) \arrow[r] \arrow[u, "\alpha"] & H^1(\mathbb{Q}_S/L^{\mathrm{cyc}}, A) \arrow[r, "\lambda(L^{\mathrm{cyc}})"] \arrow[u, "\beta"] & \bigoplus_{v\in S} J_v(L^{\mathrm{cyc}}) \arrow[r] \arrow[u, "\gamma"] & 0.
\end{tikzcd}$$

We analyse the kernel of $\gamma = \underset{v\in S}{\oplus} \gamma_v$. As in Lemma 2.4,we have $\mathrm{Ker}(\gamma_v) = \underset{v'}{\oplus} H^1(\mathcal{H}_w, W_w)$ where $\mathcal{H}_w = H_L \cap \mathcal{G}_w$, and the sum varies over the finite set of primes v' of L^{cyc} lying above v and w denotes a fixed prime of K_∞ lying above v'. As $p \nmid N$, the Galois representation is (potentially) crystalline and hence the group $H^1(\mathcal{H}_w, W_w)$ is finite by [8, Theorem 1.5]. Further, the group $\mathrm{Ker}(\beta)$ is also finite by Lemma 2.2. Applying the snake lemma, we therefore see that $\mathrm{Ker}(\alpha)$ and $\mathrm{Coker}(\alpha)$ are finite. Let $Y_A(K_\infty)$ denote the quotient module $X_A(K_\infty)/X_A(K_\infty)(p)$. Similarly, let $Y_A(L^{\mathrm{cyc}})$ denote the quotient module $X_A(L^{\mathrm{cyc}})/X_A(L^{\mathrm{cyc}})(p)$, which is a free $\mathbb{Z}_p$-module, thanks to our assumption that $X_A(L^{\mathrm{cyc}})$ is $\Lambda(\Gamma_L)$-torsion. As we have assumed that $X_A(K_\infty) \in \mathfrak{M}_H(G)$, it is clear that by restricting scalars, we also have $X_A(K_\infty) \in \mathfrak{M}_{H_L}(G_L)$. Arguing as in [3, Lemma 5.3], one sees that there is an equality of μ-invariants, namely $\mu_{G_L}(X_A(K_\infty)) = \mu_{\Gamma_L}(X_A(L^{\mathrm{cyc}}))$. On dualising the map α, the above considerations show that

$$\mathrm{rank}_{\mathbb{Z}_p}\, Y_A(L^{\mathrm{cyc}}) = \mathrm{rank}_{\mathbb{Z}_p}\, (Y_A(K_\infty))_{H_L} \tag{28}$$

where, as usual for a $\Lambda(H_L)$-module M, M_{H_L} denotes the coinvariants. Further, we also have (*loc.cit.*) $H_i(H_L, Y_A(K_\infty))$ is finite for all $i \geq 1$. In particular, as H_L is pro-p and $\Lambda(H_L)$ is local, we get (see [18])

(29)
$$r := \mathrm{rank}_{\Lambda(H_L)}\, Y_A(K_\infty) = \sum_{i=0}^{3}(-1)^i \mathrm{rank}_{\mathbb{Z}_p}\, H_i(H_L, Y_A(K_\infty)) = \mathrm{rank}_{\mathbb{Z}_p}\, (Y_A(K_\infty))_{H_L}$$

which by (28) and the finiteness of the higher homology groups, is the same as $\operatorname{rank}_{\mathbb{Z}_p} Y_A(L^{\mathrm{cyc}})$. We claim that this latter rank cannot be zero. Indeed, if it were zero, then $Y_A(K_\infty)$ would be $\Lambda(H_L)$-torsion and therefore pseudo-null by a result of Venjakob [31]. We need the following general lemma, whose simple proof below was pointed out to us by the referee:

Lemma 4.2. *Let G be a pro-p compact p-adic Lie group with no element of order p and having a closed normal subgroup H such that G/H is isomorphic to $\mathbb{Z}_p$. Let M be any module in $\mathfrak{M}_H(G)$ such that M has no non-zero pseudo-null $\Lambda(G)$-submodule. Then $N := M/M(p)$ has no non-zero $\Lambda(G)$-pseudo-null submodule.*

Proof. As M is noetherian, there is an integer k such that p^k annihilates $M(p)$. Let $\kappa : M \to M$ be the map given by multiplication by p^k, so that $\operatorname{Ker}(\kappa) = M(p)$. Clearly the image of κ is isomorphic to $N = M/M(p)$. As N is isomorphic to a $\Lambda(G)$-submodule of M, it plainly has no non-zero pseudo-null submodules. □

The above lemma therefore implies that the rank r in (29) is not zero unless $Y_A(K_\infty) = 0$. But if the latter were true, then $X_A(K_\infty)$ would be p-primary torsion, thereby contradicting Theorem 2.8. Thus we see that $Y_A(K_\infty)$ has positive $\Lambda(H_L)$-rank which by (28) is equal to the λ-invariant of $X_A(L^{\mathrm{cyc}})$ and the final assertion of the theorem is proved.

To prove the first assertion of the theorem, suppose the contrary and assume that $X_A(L^{\mathrm{cyc}})$ is finite. Then by Nakayama's lemma and (27), we see that $X_A(K_\infty)$ is finitely generated over $\Lambda(H_L)$. By [31] and Theorem 3.1, we clearly have $X_A(K_\infty)(p) = 0$ and hence $X_A(K_\infty)$ is in $\mathfrak{M}_H(G)$ and the above results apply, showing that $X_A(L^{\mathrm{cyc}})$ has positive λ-invariant. This is a contradition and therefore $X_A(L^{\mathrm{cyc}})$ is always infinite. The proof of the theorem is now complete.

□

Remark 4.3. (i) We remark that if the level N is equal to p^r with $r > 1$, then $a_p = 0$ and the form is not ordinary. If $N = p$, then ρ_f is ordinary precisely when the weight $k = 2$ (see [9, p. 4]). In this case, it is a classical result that the λ-invariant is positive when the corresponding elliptic curve has split multiplicative reduction at p, thanks to the existence of trivial zeros of p-adic L-functions [11].

We now consider some numerical examples.

Examples 4.4. Take $f = \Sigma_n \tau(n)q^n$ to be the unique normalized cusp form of weight 12 and level 1, which has been studied by Ramanujan and many others. Take $p = 691$, which is an ordinary prime for this form. It is well-known (see [27,

§5] , [15]) that the form f is not of CM type. Ramanujan's congruence

$$\tau(l) \equiv \ 1 + l^{11} \bmod 691$$

implies easily that K_∞ must be a pro-691 extension of the field $K = \mathbb{Q}(\mu_{691})$. As remarked by Greenberg [9], it can be shown that, up to homothety, there are just two $G_{\mathbb{Q}}$-invariant lattices in V, and hence two choices for A. What we now explain holds for both choices of lattices. Let us consider $X_A(K^{\text{cyc}})$, as defined in this paper (note that our normalizations are not the same as that used by Greenberg in [9], [10], and, for simplicity, we do not not spell out in detail here the precise relationship between Greenberg's Selmer groups, which involve the Tate twists of A, and ours). Since the Galois group of $K^{\text{cyc}}/\mathbb{Q}$ is the direct product of a cyclic group Δ of order 690 and a group isomorphic to $\mathbb{Z}_{691}$, we can decompose

$$X_A(K^{\text{cyc}}) = \bigoplus_{i=0}^{689} X_A(K^{\text{cyc}})^{(i)},$$

where $X_A(K^{\text{cyc}})^{(i)}$ denotes the eigenspace in which the group Δ acts via the i-th power of the character giving its action on μ_{691}. Now Theorem 4.1 shows that if $X_A(K_\infty)$ belongs to the category $\mathfrak{M}_H(G)$, then at least one of the $X_A(K^{\text{cyc}})^{(i)} \otimes \mathbb{Q}_p$ must have positive $\mathbb{Q}_p$-dimension for some $i = 0, \cdots, 689$. On the other hand, after taking account of Greenberg's different normalization, one can easily deduce from Greenberg's arguments along with the calculations of Manin and the work of Kato [19] on the Main Conjecture, that

$$X_A(K^{\text{cyc}})^{(i)} \otimes \mathbb{Q}_p = 0 \text{ for } i = 0, 689, 688, \cdots, 680 \mod 690.$$

I am very grateful to Ralph Greenberg for pointing out to me that the methods of his paper with Vatsal [12], for the prime 691, enable one to prove that $X_A(K^{\text{cyc}})(i) \otimes \mathbb{Q}_p$ has positive dimension precisely for odd integers $i = 1, 189, 491, 679$ modulo 690, and in each case the λ-invariant is 1. It does not seem at all easy to prove this more precise result by our methods. Of course, there could also conceivably be even integers i such that $X_A(K^{\text{cyc}})(i) \otimes \mathbb{Q}_p$ has positive λ-invariant. Finally, we remark that similar phenomena occur for other modular forms of level 1 and higher weight and primes p (see ([10, p. 230]) for which there are suitable Ramanujan style congruences.

References

[1] H. Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. ENS **19** (1986), 409–468.

[2] J. Coates, *Fragments of the* GL_2 *Iwasawa theory of elliptic curves without complex multiplication*,Arithmetic theory of elliptic curves (Cetraro, 1997), SLN 1716, Springer, (1999), 1–50.

[3] J. Coates, T. Fukaya, K. Kato, R. Sujatha. O. Venjakob, *The* GL_2*-Main Conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES **101** (2005), 163–208.

[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 Sér. I Math. **329** no. 4, (1999), 309–313.

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

[7] J. Coates, R. Sujatha, P. Schneider, *Links between cyclotomic and* GL_2 *Iwasawa theory*, Documenta Math. Extra Volume in honour of K. Kato, (2003), 187–215.

[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, *Iwasawa theory of p-adic representations*, Adv. Stud. in Pure Math. **17** (1989), 97–137.

[10] R. Greenberg, *Iwasawa theory for motives*, L-functions and Arithmetic ed. J. Coates and M. Taylor, LMS Lecture Notes Series **153** (1991), 211–233.

[11] R. Greenberg, *Trivial zeros of p-adic L-functions*, p-adic monodromy and the Birch and Swinnerton-Dyer conjecture, Amer. Math. Soc., Providence, RI, Contemp. Math. **165** (1994), 149–174.

[12] R. Greenberg, V. Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), 17–63.

[13] A. Grothendieck, Letters of 24/9/64 p.183 and 3-5/10/64 p.204 in Correspondance Grothendieck-Serre, Documents Mathématiques, vol. 2, Soc. Math. France, (2001).

[14] E. Ghate, V. Vatsal, *On the local behaviour of ordinary Λ-adic representations*, Ann. Inst. Fourier, Grenoble **54** (2004), 2143-2162.

[15] E. Ghate, *On the behaviour of ordinary modular Galois representations*, Modular curves and abelian varieties, Progress in Mathematics **224** Birkhauser-Verlag (2004), 105-124.

[16] Y. Hachimori, K. Matsuno, *An analogue of Kida's formula for the Selmer group of elliptic curves*, J. Alg. Geom **8** (1999), 581–601.

[17] S. Howson, *Iwasawa Theory of Elliptic Curves for p-adic Lie Extensions*, Cambridge PhD thesis, (1998).

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

[19] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et applications arithmétique, III,Astérisque **295** (2004) 1117–290.

[20] U. Jannsen, *Iwasawa modules up to isomorphism*, Adv. Stud. in Pure Math. **17** (1989), 171–207.

[21] B. Mazur, A. Wiles, *On p-adic analytic families of Galois representations*, Comp. Math. **59** (1986), 231–264.

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

[23] B. Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques* Astérisque **229** (1995).

[24] B. Perrin-Riou, *Groupe de Selmer d'une courbe elliptique à multiplication complexe*, Compositio Math. **43** (1981), 387–417.

[25] K. Ribet, *Galois representations attached to eigenforms with Nebentypus*, Modular functions of one variable V, LNM 601 (1977), 17–52.

[26] A. Scholl, *Motives for modular forms*, Invent. Math. **100** (1990), 419–430.

[27] J.-P. Serre, Une interprétation des congruences relative à la fonction τ de Ramanujan, Sém. Delange-Pisot Exp. **14** (1967/68).

[28] J.-P. Serre, *Sur les groupes de congruence des variétés abeliénnes. II.* Izv. Akad. Nauk SSSR Ser. Mat. **35** (1971), 731–737.

[29] J. Tilouine, *Modular forms and Galois representations*, Bull. Greek Math. Soc. **46** (2002), 63–78.

[30] O. Venjakob, *On the Iwasawa theory of p-adic Lie extensions*, Comp. Math. **138** (2003), 1–54.

[31] O. Venjakob, *A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory*, Crelle J. **(2003)**, 153–191.

R. Sujatha
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai 400 005, India
E-mail: sujatha@math.tifr.res.in