ELLIPTIC CURVES AND IWASAWA'S $\mu = 0$ CONJECTURE

R. SUJATHA

To Parimala on the occasion of her sixtieth birthday

1. Introduction

A fundamental problem in algebraic number theory concerns the study of the absolute Galois group of the field $\mathbb{Q}$ of rational numbers. Class field theory partially resolves this problem by explicitly describing the Galois groups of the maximal abelian extension of any number field. The study of various representations of the absolute Galois group of $\mathbb{Q}$ that occur naturally in arithmetic geometry affords another approach in attacking this problem. In this note, we shall outline yet another path, which has its origins in Iwasawa theory and describes the Galois groups of certain infinite extensions of p-adic Lie extensions of a number field. This article is largely expository in nature, with the exception of the last part of section 4, where we give a different proof of Theorem 4.5 that fits with the approach in this paper (see [17, Lemma 1] for a simpler proof). Here is how the paper is organised. We start with a brief discussion of Iwasawa's celebrated $\mu = 0$ conjecture, and show how it may also be viewed as a conjecture for the trivial Tate motive. Thereafter, we explain how Iwasawa's $\mu = 0$ conjecture proves the freeness of certain pro-p Galois groups of infinite p-adic Lie extensions of $\mathbb{Q}$. We then proceed to describe the analogue of this conjecture for the motive of an elliptic curve, whose formulation was carried out in a joint work with J. Coates a few years ago ('Conjecture A' in [2]). Finally, we discuss some recent results that prove Conjecture A in special cases.

Throughout, p will denote an odd prime and $\mathbb{Z}_p$ (respectively $\mathbb{Q}_p$), will denote the ring of p-adic integers (resp. the field of p-adic numbers). Given any number field F, we shall denote by F^{cyc} the cyclotomic $\mathbb{Z}_p$-extension of F. Recall that an extension $\mathcal{L}$ of F is said to be a p-adic Lie extension if the Galois group $\mathrm{Gal}(\mathcal{L}/\mathbb{Q})$ is a p-adic Lie group [12]. The cyclotomic extension F^{cyc} is a basic example of a p-adic Lie extension of F, and has been studied extensively for over a century, culminating in Iwasawa's seminal works [8], [9]. For any finite set S of primes in a number field F, F_S denotes the maximal extension of F unramified outside S. We shall always assume that S contains the set S_p of primes in F that lie above p, and the archimedean primes. Given a field L, the p-cohomological dimension of the field will be denoted by $\mathrm{cd}_p(L)$. If G is a profinite group, the Iwasawa algebra of G is denoted by $\Lambda(G)$, and we recall that it is defined as

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

where U runs over all open normal subgroups of G, with the inverse limit being taken with respect to the natural surjections. For any number field F, we shall denote the Galois group $\mathrm{Gal}(F^{\mathrm{cyc}}/F)$ of the cyclotomic extension by Γ. Given a discrete module M over the Iwasawa algebra $\Lambda(G)$, we denote its compact Pontryagin dual by $M^\vee$. For any module M over the Iwasawa algebra $\Lambda(G)$, $M(p)$ denotes the p-primary torsion submodule of M.

It is a pleasure to acknowledge the hospitality provided by Postech University, Pohang, Korea, while this work was under preparation. We would also like to warmly thank YoungJu Choie for making the visit memorable, and John Coates for helpful discussions and comments on this article.

2. Iwasawa's $\mu = 0$ conjecture

In this section, we describe the celebrated $\mu = 0$ conjecture of Iwasawa. To do this, we first recall the structure theorem for finitely generated modules over the Iwasawa algebra $\Lambda(G)$, where G is any group isomorphic to $\mathbb{Z}_p$. In this case, there is an isomorphism of the Iwasawa algebra $\Lambda(G)$ with the power series ring $\mathbb{Z}_p[[T]]$ in one variable, with the property that, if γ is a fixed topological generator of G, the isomorphism maps the element $\gamma - 1$ to T. If M and N are finitely generated $\Lambda(G)$-modules, then M and N are said to be *pseudo − isomorphic* if there is a $\Lambda(G)$-homomorphism $f : M \to N$ with finite kernel and cokernel. The following structure theorem was proved by Iwasawa and independently by Serre (cf. [1, Chap. VII, §4]):-

Theorem 2.1. *Let M be a finitely generated module over $\Lambda(G)$. Then there is a pseudo-isomorphism*

$$f \,:\, M \to \Lambda(G)^r \bigoplus \left(\overset{k}{\underset{i=1}{\oplus}} \Lambda(G)/\mathfrak{p}_i^{n_i} \right),$$

where the $\mathfrak{p}_i$'s are prime ideals of height one. Further, the set of prime ideals $\{\mathfrak{p}_i\}$ and the set of integers $\{n_i\}$ are unique upto a bijection of the indexing set.

The integer r is called the rank of M. The importance of this theorem lies in the fact that it enables us to define two key invariants for finitely generated torsion $\Lambda(G)$-modules. Let M be a finitely generated torsion $\Lambda(G)$-module so that it has rank zero. Write $\mathfrak{p}_{i_j}$, $(1 \le j \le k)$, for the set of prime ideals occurring in the structure theorem such that $\mathfrak{p}_{i_j} = p$. Then the μ-invariant of M is defined as

$$\mu(M) = \sum_j n_{i_j},$$

and the λ-invariant of M is defined as

$$\lambda(M) = \ \mathbb{Z}_p\text{−rank of } M/M(p),$$

where $M(p)$ denotes the p-primary torsion submodule of M. Note that if $\mu(M) = 0$, then M is a finitely generated $\mathbb{Z}_p$-module. Further, as the height one prime ideals of $\Lambda(G)$ are principal, the *characteristic ideal* of M denoted $\mathrm{ch}_G(M)$, and defined by

$$\mathrm{ch}_G(M) := \prod_{i=1}^{k} \mathfrak{p}_i^{n_i},$$

is a principal ideal. Any generator of $\mathrm{ch}_G(M)$ is called a *characteristic power series* of M, which can be assumed to be a distinguished polynomial in $\mathbb{Z}_p[[T]]$, thanks to Weierstrass' preparation theorem. The degree of the characteristic polynomial of M is clearly the λ-invariant. If M is an arbitrary finitely generated $\Lambda(G)$-module, then we set $\mu(M) := \mu(M_{\mathrm{tors}})$ where M_{tors} is the $\Lambda(G)$-torsion submodule of M.

Let F be a number field and F^{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F, with $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F) \simeq \mathbb{Z}_p$. We denote by F_∞ the maximal abelian, p-extension of F^{cyc} which is unramified everywhere. In other words, F_∞ is the p-Hilbert class field of F^{cyc}. Let X_∞ denote the Galois group $\mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. As X_∞ is abelian, it has a natural structure of a Γ-module. Indeed, given an element γ in Γ and an element x in X_∞, the action is defined by

$$\gamma.x = \tilde{\gamma}x\tilde{\gamma}^{-1},$$

where $\tilde{\gamma}$ is any lift of γ to $\mathrm{Gal}(F_\infty/F)$. It is easily checked that the action is independent of the lift since X_∞ is abelian. Further, it is well-known that any $\mathbb{Z}_p$-module with a continuous Γ-action has a natural structure as a compact $\mathbb{Z}_p[[\Gamma]]$-module and thus X_∞ is a compact module over the Iwasawa algebra. The following theorem is due to Iwasawa [8]:-

Theorem 2.2. *(Iwasawa) X_∞ is a finitely generated torsion $\Lambda(\Gamma)$-module.*

Iwasawa further conjectured that X_∞ is a finitely generated $\mathbb{Z}_p$-module, or equivalently $\mu(X_\infty) = 0$. Ferrero and Washington [4] proved that the conjecture holds when $F/\mathbb{Q}$ is an abelian extension. For $F = \mathbb{Q}$, we have $\mathbb{Q}_\infty = \mathbb{Q}^{\mathrm{cyc}}$, and there is a unique prime of $\mathbb{Q}^{\mathrm{cyc}}$ above p as p is totally ramified in $\mathbb{Q}^{\mathrm{cyc}}$. As the ideal class group of $\mathbb{Q}$ is zero, we thus have that the group $(X_\infty)_\Gamma$ of Γ-coinvariants is trivial, and hence X_∞ is itself zero. Sinnott [16] later gave a different proof of the Ferrero-Washington theorem. It should be noted that Iwasawa gave examples of non-cyclotomic $\mathbb{Z}_p$-extensions of $\mathbb{Q}$ whose p-Hilbert class fields have positive μ-invariant [10].

We shall next consider other infinite extensions of F^{cyc}. Given a finite set S of primes in F that contains S_p and the archimedean primes, we recall that F_S denotes the maximal extension of F that is unramified outside S. As the primes in S_p are the only non-archimedean primes that ramify in F^{cyc}, we have $F_S \supseteq F^{\mathrm{cyc}}$.

Definition 2.3. $F_S(p)$ is defined to be the maximal Galois extension of F in F_S such that the Galois group $\mathrm{Gal}(F_S(p)/F)$ is pro-p.

Note that the profinite degree of $F_S/F_S(p)$ is not necessarily prime to p. Also, $F_S(p) \supseteq F^{\mathrm{cyc}}$ and $F_S(p)$ has no Galois p-extensions of F in F_S, i.e. $H^1(\mathrm{Gal}(F_S/F_S(p), \mathbb{Z}/p) = 0$. For a group H, let H^{ab} denote the abelianisation of H.

Definition 2.4. $F_S(p)^{\mathrm{ab}}$ is the Galois extension of F^{cyc} such that $\mathrm{Gal}(F_S(p)^{\mathrm{ab}}/F^{\mathrm{cyc}}) = (\mathrm{Gal}(F_S(p)/F^{\mathrm{cyc}}))^{\mathrm{ab}}$. We denote this Galois group by X_S.

Again, as X_S is abelian, we see that it has a structure of a $\Lambda(\Gamma)$-module, and the following theorem was proved by Iwasawa [8]:-

Theorem 2.5. *(Iwasawa) X_S is a finitely generated $\Lambda(\Gamma)$-module of rank $r_2(F)$, the number of complex embeddings of F. Further, $\mu(X_S) = \mu(X_\infty)$.*

3. Free pro-p groups and Iwasawa's $\mu = 0$ conjecture

Recall that a free pro-p group $\mathfrak{G}$ over a set T is a pro-p group $\mathfrak{G}$, along with a map $i : T \to \mathfrak{G}$ satisfying the following properties: (i) Every open subgroup of $\mathfrak{G}$ contains all but a finite number of elements of $i(T)$, (ii) If $j : T \to \tilde{\mathfrak{G}}$ is any other map with the property (i) into a pro-p group $\tilde{\mathfrak{G}}$, then there exists a unique homomorphism $f : \mathfrak{G} \to \tilde{\mathfrak{G}}$ such that $j = f \circ i$.

For any group G, let $\mathrm{cd}_p(G)$ denote the p-cohomological dimension of G. Recall that $\mathrm{cd}_p(G) = n$ if the cohomology groups $H^k(G, M)$ are trivial for all $k \geq n+1$, and all p-primary torsion modules M. In particular, if G is a pro-p group, then $\mathrm{cd}_p(G) = n$ if and only if $H^k(G, M) = 0$ for all $k > n$, and M any discrete p-primary torsion G-module. The following theorem (see[15]) characterises free pro-p groups:-

Theorem 3.1. *A pro-p group $\mathfrak{G}$ is free if and only if $\mathrm{cd}_p(\mathfrak{G}) = 1$.*

We return to the our number field F. The *Weak Leopoldt Conjecture* for F^{cyc} is the assertion

$$H^2(\mathrm{Gal}(F_S/F^{\mathrm{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p) = 0. \tag{1}$$

This is equivalent to the assertion that $H_2(\mathrm{Gal}(F_S/F^{\mathrm{cyc}}), \mathbb{Z}_p) = 0$, where H_i denotes group homology. Viewing $\mathbb{Z}_p$ as the trivial Tate motive, the Weak Leopoldt Conjecture is thus a statement on the vanishing of the second cohomology group associated to the Pontryagin dual of the trivial Tate motive. Iwasawa proved that the Weak Leopoldt Conjecture for F^{cyc} holds in general for any number field F. However, the corresponding vanishing remains unknown for other $\mathbb{Z}_p$-extensions of F. With notation as before, we have the following theorem.

Theorem 3.2. *The Galois group $G_{S,p}(F^{\mathrm{cyc}}) := \mathrm{Gal}(F_S(p)/F^{\mathrm{cyc}})$ is a free pro-p group if and only if $\mu(X_S) = 0$, (or equivalently if $\mu(X_\infty) = 0$).*

Proof. By Theorem 2.5, it suffices to consider the $\Lambda(\Gamma)$-module X_S. Consider the long exact Galois cohomology sequence associated to

$$0 \to \mathbb{Z}/p \to \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}_p/\mathbb{Z}_p \to 0.$$

Suppose that $G_{S,p}(F^{\mathrm{cyc}})$ is a free pro-p group. Then by Theorem 3.1, we have $\mathrm{cd}_p(G_{S,p}(F^{\mathrm{cyc}}))$ is one and hence $H^2(G_{S,p}(F^{\mathrm{cyc}}), \mathbb{Z}/p) = 0$. Taking Pontryagin duals of the long exact sequence, along with the vanishing result of the Weak Leopoldt Conjecture (1), we see that

$$p - \text{primary torsion of } (H^1(G_{S,p}(F^{\mathrm{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p))^\vee = 0. \tag{2}$$

But this implies that $G_{S,p}(F^{\mathrm{cyc}})^{\mathrm{ab}}$ has no non-trivial p-torsion, and hence clearly $\mu(X_S) = 0$. For the converse, we need to use one additional fact from Iwasawa theory, namely that the Pontryagin dual $(H^1(G_{S,p}(F^{\mathrm{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p))^\vee$ has no finite non-zero $\Lambda(\Gamma)$-submodule [8].

Suppose now that $\mu(X_S) = 0$. By the structure theorem for finitely generated $\Lambda(\Gamma)$-modules, it follows that the p-torsion of $(H^1(G_{S,p}(F^{\mathrm{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p))^\vee$ is finite, and futher, by the above remark, it is in fact trivial. We therefore have $H^2(G_{S,p}(F^{\mathrm{cyc}}), \mathbb{Z}/p) = 0$. But the cohomological dimension of $G_{S,p}(F^{\mathrm{cyc}})$ is at most 2, as it is a closed subgroup of $\mathrm{Gal}(F_S/F)$ which has cohomological dimension 2 [15]. The conclusion now follows from Theorem 3.1. □

4. An analogue for elliptic curves

The next simplest motive after the trivial Tate motive is the motive associated to an elliptic curve. Guided by the philosophy that results for the Tate motive have elliptic curve analogues, one seeks the corresponding results for elliptic curves of the material in the previous section. Let E be an elliptic curve over the number field F and as before, let p be an odd prime. We take S to be the finite set consisting of primes S_p in F that lie above p, the archimedean primes, and the primes of bad reduction for the elliptic curve. Put $G_F = \mathrm{Gal}(\bar{F}/F)$ for the absolute Galois group of F. Let

$$E_{p^\infty} := \bigcup_{n \geq 0} E_{p^n}$$

where $E_{p^n} := E_{p^n}(\bar{F})$ is the discrete G_F-module of p^n-torsion points on $E(\bar{F})$. The Tate module of E, denoted $T_p(E)$, is defined by

$$T_p(E) = \varprojlim E_{p^n},$$

and $V_p(E) = T_p(E) \otimes \mathbb{Q}_p$, is the corresponding two dimensional $\mathbb{Q}_p$-vector space with a continuous action of G_F. For the purposes of this article, we shall choose to be simple minded and consider the G_F-module $V_p(E)$ as the 'dual of the Tate motive of the elliptic curve E'. We first discuss the analogous $\Lambda(\Gamma)$-modules in this context.

As before, let F_∞ denote the p-Hilbert class field of F^{cyc} and X_∞ the Galois group $\mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. At a first glance, classical Iwasawa theory for elliptic curves suggests that the corresponding $\Lambda(\Gamma)$-module in this context is the Pontryagin dual of the Selmer group over the cyclotomic extension. Recall that for a finite Galois extension L of F, the Selmer group $S(E/L)$ of E over L is a discrete $\mathrm{Gal}(L/F)$-module and is defined as

$$S(E/L) = \mathrm{Ker}\left(H^1(\mathrm{Gal}(F_S/L), E_{p^\infty})) \to \underset{v \in S}{\oplus} J_v(E/L)\right), \tag{3}$$

where

$$J_v(E/L) = \underset{w|v}{\oplus} H^1(\mathrm{Gal}(\bar{L}_w/L_w), E)(p).$$

The Selmer group of E over F^{cyc} is defined as the direct limit of $S(E/L)$ as L varies over finite extensions of F in F^{cyc}. Its Pontryagin dual is denoted by $\mathfrak{X}(E/F^{\mathrm{cyc}})$ and is well-known to be a finitely generated module over $\Lambda(\Gamma)$. It is a deep conjecture due to Mazur that if E has good ordinary reduction at the primes above p, $\mathfrak{X}(E/F^{\mathrm{cyc}})$ is a torsion $\Lambda(\Gamma)$-module and there are plenty of numerical examples known where this conjecture holds. With this knowledge, one is naturally led to wonder if $\mathfrak{X}(E/F^{\text{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module, which would be the analogue of Iwasawa's $\mu = 0$ conjecture. However, Mazur already gave examples where this is not true, and the fact that the μ-invariant of $\mathfrak{X}(E/F^{\text{cyc}})$ is not zero causes endless technical difficulties in Iwasawa theory! An explicit example is the elliptic curve $E/\mathbb{Q}$ of conductor 11, defined by

$$E\,:\,y^2+y=x^3-x^2-10x-20.$$

For the prime $p = 5$, it is known that $\mathfrak{X}(E/\mathbb{Q}^{\text{cyc}})$ is not a finitely generated $\mathbb{Z}_p$-module. One is thus naturally led to speculate on the common ground in this context for the trivial Tate motive and the motive of an elliptic curve.

Definition 4.1. The *fine Selmer group* for E over a finite extension L of F, denoted $R(E/L)$ is defined by

$$R(E/L) = \text{Ker}\left(H^1(\text{Gal}(F_S/L), E_{p^\infty}) \to \underset{v\in S}{\oplus} K_v^1(L)\right),$$

where

$$K_v^1(E/L) = \underset{w|v}{\oplus} H^1(\text{Gal}(\bar{L}_w/L_w, E_{p^\infty}).$$

The fine Selmer group of E over F^{cyc}, denoted $R(E/F^{\text{cyc}})$ is defined to be the direct limit of $R(E/L)$ as L varies over finite extensions of F in F^{cyc}.

The fine Selmer group $R(E/F^{\text{cyc}})$ is a discrete finitely generated module over the Iwasawa algebra $\Lambda(\Gamma)$, and its compact Pontryagin dual is denoted by $\mathfrak{Y}(E/F^{\text{cyc}})$. This latter module is clearly a quotient of $\mathfrak{X}(E/F^{\text{cyc}})$. The Weak Leopoldt Conjecture for elliptic curves in this context is the assertion that

$$H^2(\text{Gal}(F_S/F^{\text{cyc}}), E_{p^\infty}) = 0. \tag{4}$$

This conjecture is still open and is known to be true, for instance, if $F = \mathbb{Q}$ and $E(\mathbb{Q})$ has Mordell-Weil rank at most one. A deep result of Kato [11] proves (4) for all but a finite number of primes p for every elliptic curve E over $\mathbb{Q}$. If (4) holds, then one can show (see [2, Lemma 3.1]) that $\mathfrak{Y}(E/F^{\text{cyc}})$ is a torsion $\Lambda(\Gamma)$-module. In [2], we formulated the following Conjecture jointly with J. Coates.

Conjecture 4.2. *(Coates-Sujatha) $\mathfrak{Y}(E/F^{\text{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module.*

We believe that $\mathfrak{Y}(E/F^{\text{cyc}})$ is the analogue of X_∞ in this context, and that the above conjecture is the right analogue of Iwasawa's $\mu = 0$ conjecture for the motive of an elliptic curve. In fact, the Galois group X_∞ has a natural quotient X'_∞, which is the Galois group of the maximal abelian p-extension of F^{cyc} that is unramified everywhere, and in which all primes above p split completely. Note that all other primes which do not lie above p automatically split in any unramified p-extension. Iwasawa showed that $\mu(X_\infty) = \mu(X'_\infty)$. Let $F(E_{p^\infty})$ denote the Galois extension of F obtained by attaching to F the coordinates of all p-primary torsion points of $E(\bar{F})$. The following result is proved in [2, Theorem 3.4].

Theorem 4.3. *Let p be an odd prime number such that the extension $F(E_{p^\infty})/F$ is pro-p. Then Conjecture 4.2 holds for E over F^{cyc} if and only if the Iwasawa $\mu = 0$ conjecture holds for F^{cyc}.*

Thus, if Iwasawa's $\mu = 0$ conjecture were known to be true for all number fields, then Conjecture 4.2 would follow. In general however, Conjecture 4.2 turns out to be rather delicate to prove. This is to be expected, given its close relationship to Iwasawa's $\mu = 0$ conjecture. Analogous to the case of the Tate motive, one can establish the following result, which was independently noticed by Greenberg [7].

Proposition 4.4. *Assume* (4) *holds. Then Conjecture 4.2 is equivalent to the assertion that* $H^2(\mathrm{Gal}(F_S/F^{\mathrm{cyc}}, E_p) = 0$.

Proof. We only give a sketch of the proof. Consider the $\Lambda(\Gamma)$-modules

$$\mathcal{Z}^2(T_p(E)/F^{\mathrm{cyc}}) := \varprojlim_{F'} H^2(\mathrm{Gal}(F_S/F', T_p(E)), \ \mathcal{Z}^2(E_p/F^{\mathrm{cyc}}) := \varprojlim_{F'} H^2(\mathrm{Gal}(F_S/F', E_p),$$

where the inverse limit is taken with respect to the natural corestriction maps over all finite extensions F' of F contained in F^{cyc}. It can be shown (see [2]) that the modules $\mathcal{Z}^2(E_p/F^{\mathrm{cyc}})$ and $(H^2(\mathrm{Gal}(F_S/F^{\mathrm{cyc}}, E_p))^\vee$ have the same μ-invariant. Hence the vanishing of $H^2(\mathrm{Gal}(F_S/F^{\mathrm{cyc}}), E_p)$ is equivalent to the assertion that $\mathcal{Z}^2(E_p/F^{\mathrm{cyc}})$ is finite. On the other hand, if (4) holds, then it can be shown [2] that $\mathcal{Z}^2(T_pE/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. Combining this with the fact that

$$\mathcal{Z}^2(T_pE/F^{\mathrm{cyc}})/p \simeq \mathcal{Z}^2(E_p/F^{\mathrm{cyc}}),$$

and that the latter has μ-invariant zero if it is finite, it is easily seen that the finiteness of $\mathcal{Z}^2(E_p/F^{\mathrm{cyc}})$ is equivalent to the assertion that $\mathcal{Z}^2(T_pE/F^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module. To complete the proof, we only need to remark that $\mathcal{Z}^2(T_pE/F^{\mathrm{cyc}})$ and $\mathcal{Y}(E/F^{\mathrm{cyc}})$ differ by finitely generated $\mathbb{Z}_p$-modules, a fact that can be deduced from the Poitou-Tate exact sequence. □

A natural question that arises is whether Conjecture 4.2 is isogeny invaraint. Though we have been unable to establish this in full generality, we shall prove the following theorem.

Theorem 4.5. *Let $E/\mathbb{Q}$ be an elliptic curve with a rational p-isogeny over $\mathbb{Q}$. The Conjecture 4.2 holds for E/F^{cyc}.*

Proof. Let W denote the kernel of the isogeny. Put $F = \mathbb{Q}(\mu_p, W)$ for the abelian extension of $\mathbb{Q}$ defined as the composite of $\mathbb{Q}(\mu_p)$ and the trivialising extension of W. Also let $F_1 = \mathbb{Q}(E_p)$. It is easy to check that the hypothesis implies that F_1/F is a Galois p-extension. Further, as $F/\mathbb{Q}$ is abelian, Iwasawa's $\mu = 0$ conjecture holds for the Galois group of $F_\infty/F^{\mathrm{cyc}}$, where F_∞ is the maximal abelian p-extension of F^{cyc} unramified everywhere. Let $F_{S,p}$ denote the maximal pro-p quotient of $\mathbb{Q}_S/F$. By Theorem 3.2, the Galois group $\mathrm{Gal}(F_S(p)/F^{\mathrm{cyc}})$ is free pro-p. Hence the subgroup $\mathrm{Gal}(F_S(p)/F_1^{\mathrm{cyc}})$ is also free pro-p. By Theorem 3.1, we deduce that the cohomology groups $H^2(\mathbb{Q}_S/F_1^{\mathrm{cyc}}, E_p)$ and $H^2(\mathbb{Q}_S/F^{\mathrm{cyc}}, E_p)$ are trivial. Let Δ be the Galois group of $F/\mathbb{Q}$; it can also be identified with the Galois group $F^{\mathrm{cyc}}/\mathbb{Q}^{\mathrm{cyc}}$. Note that Δ has order dividing $(p-1)^2$ and is hence prime to p. From the Hochschild-Serre spectral sequence

$$H^p(\Delta, H^q(\mathrm{Gal}(F_S(p)/F^{\mathrm{cyc}}), E_p)) \Rightarrow H^n(\mathrm{Gal}(\mathbb{Q}_S(p)/\mathbb{Q}^{\mathrm{cyc}}), E_p),$$

it immediately follows that $H^2(\mathrm{Gal}(\mathbb{Q}_S(p)/\mathbb{Q}^{\mathrm{cyc}}), E_p) = 0$. To finish the proof of the theorem, we need to prove that $H^2(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}^{\mathrm{cyc}}), E_p) = 0$, by Proposition 4.4. To this end, consider the Hochschild-Serre spectral sequence

$$H^p(\mathrm{Gal}(F_S(p)/\mathbb{Q}^{\mathrm{cyc}}), H^q(\mathrm{Gal}(\mathbb{Q}_S/F_S(p)), E_p)) \Rightarrow H^n(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}^{\mathrm{cyc}}), E_p).$$

The module E_p is trivialised over $F_S(p)$ as the field F_1 is contained in $F_S(p)$ by our hypothesis. Thus $H^1(\mathrm{Gal}(\mathbb{Q}_S/F_S(p)), E_p) \simeq H^1(\mathrm{Gal}(\mathbb{Q}_S/F_S(p)), \mathbb{Z}/p) = 0$, by the definition of $F_S(p)$. Further, $H^2(\mathrm{Gal}(\mathbb{Q}_S/F_S(p)), E_p) \simeq H^2(\mathrm{Gal}(\mathbb{Q}_S/F_S(p)), \mathbb{Z}/p \oplus \mathbb{Z}/p) = 0$ (see [15]). Finally, since $\mathrm{cd}_p(\mathrm{Gal}(F_S(p)/F^{\mathrm{cyc}}) = 2$, we conclude from the above Hochschild-Serre spectral sequence that $H^2(\mathrm{Gal}\,\mathbb{Q}_S/\mathbb{Q}^{\mathrm{cyc}}, E_p) = 0$ and this completes the proof of the theorem. □

We end this article with a few other observations. It is entirely pertinent to wonder about the analogue of Conjecture A for elliptic curves over a general $\mathbb{Z}_p$-extension. In other words, suppose that E is an elliptic curve over a number field F and that F_∞ is an arbitrary $\mathbb{Z}_p$-extension of F. As before, let S be the finite set of primes containing the primes in F that lie above p, and the primes of bad reduction for E. Let $\mathfrak{Y}(E/F_\infty)$ denote the dual of the fine Selmer group considered as a module over $\Lambda(G)$ where $G = \mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}_p$. Assuming that $\mathfrak{Y}(E/F_\infty)$ is a $\Lambda(G)$-torsion module, when is $\mathfrak{Y}(E/F_\infty)$ a finitely generated $\mathbb{Z}_p$-module?

Let E be an elliptic curve with complex multiplication by an imaginary quadratic field K of class number one. Assume that E is defined over K and that the odd prime p splits into prime $p = \mathfrak{p}\mathfrak{p}^*$ in the ring of integers $\mathcal{O}_K$ of K. Let $K(E_{\mathfrak{p}^n})$ denote the field extension of K obtained by adjoining all the $\mathfrak{p}^n$-division points of E and consider the infinite Galois extension

$$K_\infty := K(E_{\mathfrak{p}^\infty}) = \bigcup_{n\geq 0} K(E^n_{\mathfrak{p}}).$$

Then $K(E_{\mathfrak{p}^\infty})$ is $\mathbb{Z}_p$-extension of $K(E_{\mathfrak{p}})$ and we write $G = \mathrm{Gal}(K(E_{\mathfrak{p}^\infty})/K)$ for the corresponding Galois group and $\Lambda(G)$ for the associated Iwasawa algebra. Let X_∞ be the maximal abelian p-extension of K_∞ that is unramified outside of the set of primes above $\mathfrak{p}$. It is known [13] that X_∞ is a finitely generated torsion $\Lambda(G)$-module. Let $S^{\mathfrak{p}}(E/K_\infty)$ (resp. $R^{\mathfrak{p}}(E/K_\infty)$) denote the $\mathfrak{p}$-Selmer group (resp. $\mathfrak{p}$-fine Selmer group) of E over K_∞. To be precise, these modules are defined by taking $\mathfrak{p}$ instead of p in (3) and Definition 4.1 respectively. Let $\mathfrak{X}^{\mathfrak{p}}(E/K_\infty)$ and $\mathfrak{Y}^{\mathfrak{p}}(E/K_\infty)$ be the respective compact duals of the Selmer group and the fine Selmer group. We then have [13]

$$S^{\mathfrak{p}}(E/K_\infty) = \mathrm{Hom}\,(X_\infty, E^\infty_{\mathfrak{p}}),$$

and hence it follows that $\mathfrak{X}^{\mathfrak{p}}(E/K_\infty)$ and $\mathfrak{Y}^{\mathfrak{p}}(E/K_\infty)$ are both finitely generated $\Lambda(G)$-torsion modules. It was shown by Gillard and Schneps independently ([7], [14]) that X_∞ has μ-invariant zero. We denote by K_S the maximal extension of K that is unramified outside the primes of S. Let $G_{S,p}(K_\infty)$ denote the maximal pro-p quotient of the Galois group $\mathrm{Gal}(K_S/K_\infty)$. By a result of Perrin-Riou [13], it is known that the Weak Leopoldt Conjecture holds for K_∞ and the Galois modules $E_{\mathfrak{p}^\infty}$ and E_{p^∞}; in other words that

$$H^2(\mathrm{Gal}(K_S/K_\infty), E_{\mathfrak{p}^\infty}) = 0,\ H^2(\mathrm{Gal}(K_S/K_\infty), E_{p^\infty}) = 0. \tag{5}$$

Arguing as in §3 (cf. Theorem 3.2), it then follows that $G_{S,p}(K_\infty)$ is free and hence has p-cohomological dimension at most one. Further, using the Hochschild-Serre spectral sequence as in the proof of Theorem 4.5, one then sees that

$$H^2(\mathrm{Gal}(K_S/K_\infty), E_{\mathfrak{p}}) = 0,\ H^2(\mathrm{Gal}(K_S/K_\infty), E_p) = 0.$$

It seems difficult to directly deduce Conjecture A for K^{cyc} or F^{cyc}, where $F = K(E_{\mathfrak{p}})$ by these methods. In [5], the following stronger conjecture was put forth (see also [3]):-

Conjecture 4.6. *Let K be an imaginary quadratic field and let E be an elliptic curve defined over K such that $\mathrm{End}_K(E)\otimes\mathbb{Q}$ is isomorphic to K. Let p be an odd prime which splits in K, and such that E has good reduction at both primes of K above p. Then the dual Selmer group of E over K^{cyc} is a finitely generated $\mathbb{Z}_p$-module. In particular, if E is defined over $\mathbb{Q}$, the dual Selmer group of E over $\mathbb{Q}^{\mathrm{cyc}}$ is a finitely generated $\mathbb{Z}_p$-module.*

In this case, let $F = K(E_p)$ and $F_\infty = K(E_{p^\infty})$, and put $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. All we know at present, is that in this case the dual Selmer group of E over F_∞ is a finitely generated $\Lambda(H)$-module if and only if the dual Selmer group of E over F^{cyc} is a finitely generated $\mathbb{Z}_p$-module.

References

[1] N. Bourbaki, Elements of Mathematics, Commutative Algebra, Chapters 1–7, Springer (1989).

[2] J. Coates, R. Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Annalen **331** (2005), 809–839.

[3] J. Coates, R. Sujatha, *On the $M_H(G)$-comjecture for elliptic curves*, in preparation.

[4] B. Ferrero, L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.

[5] J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. Inst. Hautes tudes Sci. **101** (2005), 163–208.

[6] Gillard, *Transformation de Mellin-Leopoldt des fonctions elliptiques*, J. Number Theory **25** (1987), 379–393.

[7] R. Greenberg, *Iwasawa Theory, Projective Modules, and Modular Representations*, Mem. AMS, To appear.

[8] K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[9] K. Iwasawa, *On the theory of cyclotomic fields, J. Math. Soc. Japan* **20** (1964), 42–82.

[10] K. Iwasawa, *On the -invariants of Z_1-extensions*, Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, Kinokuniya, Tokyo, (1973), 1–11.

[11] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms. Cohomologies p-adiques et applications arithmétiques III*, Astérisque **295** (2004), 117–290.

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

[13] B. Perrin-Riou, *Arithmétique des courbes elliptiques et thorie d'Iwasawa*, Mém. Soc. Math. France (N.S.) **17** (1984).

[14] L. Schneps, *On the -invariant of p-adic L-functions attached to elliptic curves with complex multiplication*, J. Number Theory **25** (1987), 20–33.

[15] J.-P. Serre, Cohomologie Galoisienne, Fifth edition. Lecture Notes in Mathematics, 5. Springer-Verlag, Berlin, (1994).

[16] W. Sinnott, *On the -invariant of the* Γ*-transform of a rational function*, Invent. Math. **75** (1984), 273–282.

[17] C. Wuthrich, *Extending Kato's result to curves with p-isogenies*, Mathematical Research Letters **13** (2006), 713–718.

School of Mathematics Tata Institute of Fundamental Research Homi Bhabha Road Mumbai 400 005, India

E-mail address: sujatha@math.tifr.res.in