STRUCTURE OF FINE SELMER GROUPS IN p-ADIC LIE EXTENSIONS

DEBANJANA KUNDU AND SUJATHA RAMDORAI

Abstract. In this paper, the goal is to prove results for fine Selmer groups in different p-adic Lie extensions. A class of examples are provided of elliptic curves where both the Selmer group and the fine Selmer group are trivial in the cyclotomic $\mathbb{Z}_p$-extension of a given number field. The relationship between Conjecture B for CM elliptic curves and the Generalized Greenberg's Conjecture is clarified. Evidence for Conjecture B in previously unknown cases is provided. In particular, for a CM elliptic curve, Conjecture B holds when at the cyclotomic level the fine Selmer group is finite. Furthermore, it is shown that for all elliptic curves over $\mathbb{Q}$, Conjecture B holds at regular primes. This is then extended to a large class of totally imaginary fields.

1. Introduction

The fine Selmer group of elliptic curves is a module over Iwasawa algebras that is of interest in the arithmetic of elliptic curves. It plays an important role in the formulation of the main conjecture in Iwasawa theory. Coates and the second author proposed some conjectures on the structure of the fine Selmer groups, viz. Conjecture A and Conjecture B in [CS05]. Conjecture A is viewed as a generalization of the classical Iwasawa $\mu = 0$ conjecture to the context of the motive associated to an elliptic curve; whereas Conjecture B is in the spirit of generalising Greenberg's pseudonullity conjecture to elliptic curves [Gre01b]. Recently, there has been a renewed interest in studying pseudonull modules over Iwasawa algebras [BCG$^+$15]. It is thus natural to investigate Conjecture B, and this article makes progress in that direction. These conjectures have been generalised to fine Selmer groups of ordinary Galois representations associated to modular forms [JS11]. This article restricts attention to the fine Selmer groups of elliptic curves, often with good reduction at a prime p, over p-adic Lie extensions of the base field. However, the methods easily generalise to the case of ordinary Galois representations and the details are being worked out.

Let E be an elliptic curve over a number field, F. While Conjecture A asserts that its dual fine Selmer group over the cyclotomic $\mathbb{Z}_p$-extension F_{cyc}, is finitely generated as a $\mathbb{Z}_p$-module, Conjecture B is an assertion on the structure of the dual fine Selmer group over special p-adic Lie extensions that contain the cyclotomic $\mathbb{Z}_p$-extension. It is conjectured that the dual fine Selmer group of E over an admissible p-adic Lie extension is pseudonull as a module over the associated Iwasawa algebra. Here, both conjectures are established for a large class of elliptic curves.

Date: October 21, 2019.

2010 *Mathematics Subject Classification.* Primary 11R23.

Key words and phrases. Iwasawa Theory, Fine Selmer groups, Pseudo-Null, Conjecture A, Conjecture B, Generalized Greenberg's Conjecture.

Here is an outline of the paper. Using a result of Greenberg, we prove a general theorem that gives sufficient conditions for the dual fine Selmer group of E over the cyclotomic $\mathbb{Z}_p$-extension to be finite. It is shown that these conditions are satisfied for a large class of elliptic curves. For CM elliptic curves over an imaginary quadratic field K, the Generalized Greenberg's Conjecture (GGC) is shown to be equivalent to Conjecture B for certain pro-p p-adic Lie extensions. Furthermore, Conjecture B over a trivializing extension of K implies GGC for K. This recovers a known result of McCallum [McC01]. Finally, we prove that Conjecture B holds for special classes of admissible p-adic Lie extensions whenever the dual fine Selmer group over the cyclotomic extension is finite for a CM elliptic curve. For all elliptic curves over $\mathbb{Q}$ and p a regular prime, it is possible to show that Conjecture B holds for elliptic curves in the trivializing extension $\mathbb{Q}(E_{p^\infty})$. The same is shown to be true for a large class of imaginary Galois extensions.

Concrete examples for the validity of Conjecture B have been rather sparse. Our result settles the case of some numerical examples that were considered in [CS05, Examples 4.7 and 4.8] but were not fully settled there. Example 4.8 was shown to satisfy Conjecture B provided the elliptic curve had a point of infinite order over the trivialising extension associated to the corresponding Galois representation. This latter condition could not be verified despite advances in computational methods.

The paper consists of six sections. Section 2 is preliminary in nature; the main objects of study are introduced along with the precise assertions of Conjecture A, Conjecture B, and GGC. In Section 3, finiteness of the cyclotomic dual fine Selmer group is proven. The hypotheses are verified in a large class of examples. In Section 4, the relation between Conjecture B for CM elliptic curves and GGC is clarified. In Section 5, evidence for Conjecture B is provided in a large number of cases. Our methods are illustrated with concrete numerical examples. In Section 6, we provide implications of Conjecture B to the fundamental short exact sequence studied in proving the Iwasawa Main Conjecture.

2. Preliminaries

Throughout this article, p will denote an odd prime number, unless mentioned otherwise. F will denote an algebraic number field.

For a p-adic analytic, torsion-free, pro-p group, G, the Iwasawa algebra over $\mathbb{Z}_p$ is denoted by $\Lambda(G)$ [NSW08, Chapter V]. It is a left and right Noetherian ring without zero-divisors. It is also an Auslander regular ring [Ven02]. All modules over the Iwasawa algebra will be considered as left modules. The property of being Auslander regular, in particular, affords an associated dimension theory for finitely generated modules over $\Lambda(G)$. If d is the dimension of G considered as a p-adic analytic manifold, the dimension of $\Lambda(G)$ is $d+1$ [Ven02]. Given a finitely generated $\Lambda(G)$-module, M, its dimension is denoted $\dim(M)$.

Definition. *Let M be a finitely generated $\Lambda(G)$-module. Then M is* ***torsion*** *if* $\dim(M) \leqslant \dim(\Lambda(G)) - 1$. *The module M is* ***pseudo-null*** *if it is of codimension at least 2, or equivalently* $\dim(M) \leqslant \dim(\Lambda(G)) - 2$.

A finitely generated torsion $\Lambda(G)$-module M is a pseudonull $\Lambda(G)$-module if

$$E^i := \operatorname{Ext}^i_{\Lambda(G)}(M, \Lambda(G)) = 0 \qquad i = 0,\ 1. \tag{1}$$

If the module is torsion then $E^0(M) = 0$.

Let E be an elliptic curve defined over F. Consider the Galois modules

$$E_{p^\infty} := \bigcup_{n \geqslant 1} E_{p^n}, \quad T_p(E) := \varprojlim E/p^n E.$$

The notation for the Tate module $T_p(E)$ will often be abbreviated to T if the elliptic curve and the prime is fixed. Set

$$F_\infty = \bigcup_{n \geqslant 1} F(E_{p^n}). \tag{2}$$

Let F_{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F and S be a finite set of primes of F containing the primes above p, the primes of bad reduction of E, and the Archimedean primes. In short, we write $S \supseteq S_p \cup S_{bad} \cup S_\infty$. Let F_S denote the maximal extension of F unramified outside S and set $G_S(F) = \mathrm{Gal}(F_S/F)$. $F_S(p)$ will denote its maximal pro-p quotient. For any extension $\mathcal{L}/F$ contained in F_S, the corresponding Galois group $\mathrm{Gal}(F_S/\mathcal{L})$ is denoted by $G_S(\mathcal{L})$.

Throughout the paper, the focus is on admissible p-adic Lie extensions $\mathcal{L}$, defined in [CS05, Section 1]. It follows from the Weil pairing that F_∞ contains F_{cyc} and is contained in F_S. The Galois group $G_{F_\infty} = \mathrm{Gal}(F_\infty/F)$, has no p-torsion if $p \geqslant 5$ and contains an open, normal, pro-p subgroup. In fact, the extension $F_\infty/F(E_p)$ is always pro-p and hence an admissible extension. Recall, if E has no complex multiplication, then $\mathrm{Gal}(F_\infty/F)$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$; whereas in the CM case, G_{F_∞} contains an open subgroup which is Abelian and isomorphic to $\mathbb{Z}_p^2$.

Consider the compact pro-p p-adic Lie group $G_{\mathcal{L}} = \mathrm{Gal}(\mathcal{L}/F)$, with associated Iwasawa algebra $\Lambda(G_{\mathcal{L}})$. Our main interest will be the modules over $\Lambda(G_{\mathcal{L}})$ that arise in Iwasawa theory, such as the Selmer group and the fine Selmer group. The reader is referred to [CS00, Chapter 2] and [CS05, Section 3] for precise definitions.

For a discrete p-primary (resp. compact pro-p) Abelian group M, its Pontryagin dual defined as

$$M^\vee = \mathrm{Hom}_{\mathrm{cont}}(M, \mathbb{Q}_p/\mathbb{Z}_p),$$

is a compact (resp. discrete) module over the Iwasawa algebra. Let G be a profinite group and M be a G-module. M^G is the subgroup of elements fixed by G and M_G is the largest quotient of M on which G acts trivially. For any p-adic Lie extension $\mathcal{L}$, the dual Selmer group (resp. fine Selmer group) is written as $\mathfrak{X}(E/\mathcal{L})$ (resp. $\mathfrak{Y}(E/\mathcal{L})$). They are both $\Lambda(G_{\mathcal{L}})$-modules. Define the compact $G_{\mathcal{L}}$-modules

$$\mathcal{Z}^i(E/\mathcal{L}) = \mathcal{Z}^i(T_p(E)/\mathcal{L}) := \varprojlim H^i(G_S(L), T_p(E)) \quad \text{for } i = 0,\ 1,\ 2. \tag{3}$$

Here L runs over all finite extensions of F contained in $\mathcal{L}$ and the projective limit is taken with respect to the corestriction maps. These are the i-th Iwasawa cohomology modules. By [CS05, Lemma 2.1], $\mathcal{Z}^0(E/\mathcal{L}) = 0$. It is known $\mathcal{Z}^2(E/\mathcal{L})$ is $\Lambda(G_{\mathcal{L}})$-torsion if and only if $H^2(G_S(\mathcal{L}), E_{p^\infty}) = 0$ [CS05, Lemma 3.1].

For $\mathcal{L} = F_{\mathrm{cyc}}$, consider the dual fine Selmer group $\mathfrak{Y}(E/F_{\mathrm{cyc}})$. Conjecture A is the following assertion.

Conjecture. *[CS05, Conjecture A] Let E be an elliptic curve defined over a number field F and p be an odd prime. $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module.*

The dimension theory for modules over Auslander regular rings provides another equivalent definition for certain kinds of pseudonull modules as described below.

Let $\mathcal{L}/F$ be an admissible p-adic Lie extension. Set $G_{\mathcal{L}} = \mathrm{Gal}(\mathcal{L}/F)$ and $H_{\mathcal{L}} = \mathrm{Gal}(\mathcal{L}/F_{\mathrm{cyc}})$. A finitely generated $\Lambda(G_{\mathcal{L}})$-module which is also finitely generated as a $\Lambda(H_{\mathcal{L}})$-module, is in fact a torsion $\Lambda(G_{\mathcal{L}})$-module. A $\Lambda(G_{\mathcal{L}})$-module is pseudonull if and only if it is $\Lambda(H_{\mathcal{L}})$-torsion [VV03].

Conjecture B is inspired by the following conjecture of Greenberg. This is often referred to as the Generalized Greenberg's Conjecture.

Conjecture. *[Gre01b, Conjecture 3.5] Let F be any number field and p be any prime. Let $\widetilde{F}$ denote the compositum of all $\mathbb{Z}_p$-extensions of F and $\widetilde{L}$ denote the pro-p Hilbert class field of $\widetilde{F}$. Set $\widetilde{X} = \mathrm{Gal}(\widetilde{L}/\widetilde{F})$. It is a pseudonull module over the ring $\widetilde{\Lambda} = \mathbb{Z}_p[[\mathrm{Gal}(\widetilde{F}/F)]]$.*

Conjecture B concerns the phenomenon of certain arithmetic Iwasawa modules for p-adic Lie extensions of dimension strictly greater than 1 being much smaller than intuitively expected.

Conjecture. *[CS05, Conjecture B] Let E be an elliptic curve defined over a number field F, such that $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module. Let $\mathcal{L}/F$ be an admissible p-adic Lie extension and $G_{\mathcal{L}}$ be a pro-p p-adic Lie group of dimension strictly greater than 1. Then $\mathfrak{Y}(E/\mathcal{L})$ is a pseudonull $\Lambda(G_{\mathcal{L}})$-module.*

2.1. **Powerful Diagram.** The Powerful Diagram is a generalization of the work of Jannsen. It is a useful tool in the study of arithmetic modules arising in Iwasawa theory. It combines ideas from arithmetic, profinite groups and uses the Fox-Lyndon resolution. For the sake of completeness we review the relevant results. The reader is referred to [OV02, Section 4] for details.

Let $\mathcal{G}$ be a finitely generated pro-p group of p-cohomological dimension $\leqslant 2$, with d generators. Then $\mathcal{G}$ has a **free presentation**,

$$0 \to \mathcal{N} \to \mathcal{F}(d) \to \mathcal{G} \to 0.$$

Thus, $\mathcal{G}$ is a quotient of a free pro-p group $\mathcal{F}(d)$ of rank d and $\mathcal{N}$ is the kernel. To this presentation one can associate the Fox-Lyndon resolution,

$$0 \to \mathcal{N}^{ab}(p) \to \Lambda(\mathcal{G})^d \to \Lambda(\mathcal{G}) \to \mathbb{Z}_p \to 0.$$

The projective $\Lambda(\mathcal{G})$-module $\mathcal{N}^{ab}(p)$ is called the p-**relation module of** $\mathcal{G}$.

Let A be a fixed p-divisible p-primary Abelian group of finite $\mathbb{Z}_p$-co rank r with a continuous $\mathcal{G}$-action. For a finitely generated $\Lambda(\mathcal{G})$-module M define the **twist**,

$$M^{\#} := M \otimes_{\mathbb{Z}_p} A^{\vee}.$$

We restrict ourselves to the following specific case. Let p be a fixed odd prime, E be an elliptic curve defined over F such that F_{∞}/F is a pro-p group, and $S \supseteq S_p \cup S_{bad} \cup S_{\infty}$. In our case $A = E_{p^\infty}$, hence $r = 2$. Fix the following Galois groups.

$$\mathcal{G} = \text{maximal pro} - p \text{ part of } \mathrm{Gal}(F_S/F)$$
$$\mathcal{H} = \text{maximal pro} - p \text{ part of } \mathrm{Gal}(F_S/F_{\infty})$$
$$G = \mathrm{Gal}(F_{\infty}/F) \quad \text{(this is a pro} - p \text{ group by assumption)}$$

Consider the composition of the maps $\mathcal{F}(d) \to \mathcal{G} \to G$ and denote its kernel by $\mathcal{R}$. Set the notation

$$Y_{\infty} = Y_{A,F_{\infty}} = (I(\mathcal{G})^{\#})_{\mathcal{H}} \text{ where } I(\mathcal{G}) \text{ is the augmentation ideal}$$
$$J_{\infty} = J_{A,F_{\infty}} = \ker\left((\Lambda(\mathcal{G})^{\#}))_{\mathcal{H}} \to (A^{\vee})_{\mathcal{H}}\right)$$
$$d = \dim_{\mathbb{F}_p} H^1(\mathcal{G}, \mathbb{F}_p)$$

$$
\begin{tikzcd}
 & & & 0 & 0 & \\
 & & & J_{A,F_\infty} \arrow[u] \arrow[r, equal] & J_{A,F_\infty} \arrow[u] & \\
0 \arrow[r] & H^2(G_S(F_\infty), A)^\vee \arrow[r] & (\mathcal{N}^{ab}(p)^\#)_{\mathcal{H}} \arrow[r] & \Lambda(G)^{dr} \arrow[u] \arrow[r] & Y_{A,F_\infty} \arrow[u] \arrow[r] & 0 \\
0 \arrow[r] & H^2(G_S(F_\infty), A)^\vee \arrow[u, equal] \arrow[r] & (H^1(\mathcal{N}^{ab}(p), A)^{\mathcal{H}})^\vee \arrow[u, "\simeq"] \arrow[r] & H^1(\mathcal{R}, A) \arrow[u] \arrow[r] & H^1(G_S(F_\infty), A)^\vee \arrow[u] \arrow[r] & 0 \\
 & & & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd}
$$

FIGURE 1. Powerful Diagram

The above commutative diagram is referred to as the *Powerful Diagram.*

As a consequence $(\mathcal{N}^{ab}(p)^\#)_{\mathcal{H}}$ is a projective module [OV02, Lemma 4.5]. If A is a trivial $\mathcal{H}$-module, then

$$(\mathcal{N}^{ab}(p)^\#)_{\mathcal{H}} \simeq (\mathcal{N}^{ab}(p)_{\mathcal{H}})^\#.$$

Note that if $H^2(G_S(F_\infty), A) = 0$, then Y_{A,F_∞} has projective dimension $\leqslant 1$. Further, it is known J_∞ has no non-zero torsion submodules [OV03, Page 27].

3. Fine Selmer Groups in the Cyclotomic Extension

The goal of this section is to prove that for density one ordinary primes, (fine) Selmer group is trivial in the cyclotomic $\mathbb{Z}_p$-extension for rank 0 elliptic curves with good ordinary reduction at primes above p.

3.1. **Trivial Fine Selmer Groups in the Cyclotomic Tower.**
Throughout this section the following hypothesis holds.

Hypothesis. *The Shafarevich-Tate group of an elliptic curve is finite.*

Fix a number field F and an odd prime p. Let E be an elliptic curve over F with good ordinary reduction at all primes above p. Set $\Gamma = \mathrm{Gal}(F_{\mathrm{cyc}}/F)$. If $\mathrm{Sel}(E/F)_p$ is finite, by Mazur's Control Theorem, $\mathrm{Sel}(E/F_{\mathrm{cyc}})_p$ is $\Lambda(\Gamma)$-cotorsion [Gre01a, Corollary 4.9]. This happens for example, if E/F is a rank 0 elliptic curve.

Let $f_E(T)$ be the characteristic polynomial generating the characteristic ideal of $\mathfrak{X}(E/F_{\mathrm{cyc}})$. If $\mathrm{Sel}(E/F)_p$ is finite, then $f_E(0) \neq 0$ [Gre99].

Denote by $\widetilde{E}_v$, the reduction of E modulo v over the residue field, κ_v. Recall v is called an *anomalous prime* if p divides $\left|\widetilde{E}_v(f_v)\right|$ [Maz72, Section 1(b)]. Let c_v be the Tamagawa number and denote by $c_v^{(p)}$ the highest power of p dividing it.

The main theorem of this section is stated below. It strengthens a result of Greenberg, who proved the result for $F = \mathbb{Q}$ [Gre99, Proposition 5.1]. In particular, our theorem provides evidence for Conjecture A for a large class of elliptic curves over a general number field.

Theorem 3.1. *Let F be a number field and E be an elliptic curve of rank 0 over F. Assume that the Shafarevich-Tate group of E/F is finite. Varying over primes of good ordinary reduction,* $\mathrm{Sel}(E/F_{\mathrm{cyc}})_p$ *is trivial for all primes outside a set of density 0. In particular, Conjecture A holds for* $\mathfrak{Y}(E/F_{\mathrm{cyc}})$.

Proof. With the setting as in the theorem, it is known [Gre99, Section 4]

$$f_E(0) \sim \left(\prod_{v\ bad} c_v^{(p)}\right)\left(\prod_{v|p} \left|\widetilde{E}_v(f_v)_p\right|^2\right)\left|\operatorname{Sel}(E/F)_p\right| \Big/ \left|E(F)_p\right|^2 \tag{4}$$

where $a \sim b$ for $a,\ b \in \mathbb{Q}_p^\times$ means that a, b have the same p-adic valuation. Consider an elliptic curve E with the following four properties:

(i) E is a rank 0 elliptic curve defined over F, with $E(F)_p = 0$
(ii) E has good ordinary non-anomalous reduction at primes above p
(iii) $\text{Ш}(E/F)_p$ is trivial
(iv) p does not divide the Tamagawa number c_v, where v is a bad prime.

It follows from (4) that for such an elliptic curve, $f_E(0)$ is a unit.

If E is a rank 0 elliptic curve with $E(F)_p = 0$, then $\operatorname{Sel}(E/F)_p = \text{Ш}(E/F)_p$. When $f_E(0)$ is a unit, we know $\mathfrak{X}(E/F_{\text{cyc}})$ (and hence $\mathfrak{Y}(E/F_{\text{cyc}})$) is finite. Equivalently, both $\operatorname{Sel}(E/F_{\text{cyc}})_p$ and $R(E/F_{\text{cyc}})_p$ are finite. When $E(F)_p = 0$, it is further known that $\mathfrak{X}(E/F_{\text{cyc}})$ has no non-trivial finite Λ-submodules [HM00]. Thus, $\mathfrak{X}(E/F_{\text{cyc}})$ must be trivial, if it is finite. Since $\mathfrak{Y}(E/F_{\text{cyc}})$ must also be trivial, Conjecture A holds for $\mathfrak{Y}(E/F_{\text{cyc}})$ when E/F is an elliptic curve satisfying (i)-(iv).

In [MR10], the authors show that given F, there exist 'many' rank 0 elliptic curves over F. It remains to check that given such a rank 0 elliptic curve, $f_E(0)$ is a unit for density 1 primes. This follows from the following observations:

(a) given an elliptic curve E over a number field F, by a result of Merel it is known that for all but finitely many primes $E(F)_p = 0$.
(b) given an elliptic curve E/F, it has good reduction at primes above p for all but finitely many p. Using a Chebotarev density argument, for density 1 ordinary primes, it is known E has non-anomalous reduction at p [Mur97].
(c) by hypothesis, given E, condition (iii) holds away from a finite set of primes.
(d) at bad places, the Tamagawa number is finite and bounded. Given an elliptic curve, condition (iv) holds away from a finite set of primes.

The proof is now complete. □

Remark 3.2. It is important to emphasize that for a fixed elliptic curve over F, it is possible that $f_E(0)$ is a unit when $E(F)_p$ is non-trivial; for example if there is anomalous reduction at the prime p. It is also possible that such elliptic curves have $\operatorname{Sel}(E/F_{\text{cyc}})_p = 0$ [CS00, Theorem 3.11 and Remark 3.12(v)]. Elliptic curves with these properties exist [CS00, Chapter 5] and are considered later in the paper. Therefore, there are some elliptic curves that are excluded by our theorem. This raises the following natural question.

Question. Let E be a rank 0 elliptic curve defined over F. Is $\mathfrak{Y}(E/F_{\text{cyc}})$ trivial for all but finitely many primes?

4. Relating Conjecture B to the Generalized Greenberg's Conjecture (GGC)

In this section, the goal is to clarify the relationship between GGC and Conjecture B for CM elliptic curves. Both these conjectures pertain to the pseudonullity of certain Iwasawa modules. Even though Conjecture B was proposed as a generalization of GGC, the precise formulation of this relationship is rather intricate. This connection is made explicit using the Powerful Diagram (see Figure 1).

Let K be an imaginary quadratic field and $\mathcal{O}_K$ be its ring of integers. Let E/K be an elliptic curve with CM by $\mathcal{O}_K$. Set

$$F = K(E_p), \quad F_\infty = K(E_{p^\infty}), \quad G = G_{F_\infty} = \mathrm{Gal}(F_\infty/F), \quad \mathcal{G}_\infty = \mathrm{Gal}(F_\infty/K).$$

Note that G is a pro-p group with $G \simeq \mathbb{Z}_p^2$. Set $\widetilde{K}$ (resp. $\widetilde{F}$) to be the compositum of all $\mathbb{Z}_p$-extensions of K (resp. F). Since the Leopoldt conjecture is known for (imaginary) quadratic fields, $\widetilde{K}$ is the unique $\mathbb{Z}_p^2$ Galois extension of K. Throughout this section, we make the following assumption.

Hypothesis. *$p \neq 2, 3$ is a prime. p is unramified in K.*

By the theory of CM, $\mathcal{G}_\infty = G \times \Delta$ where $\Delta \simeq \mathrm{Gal}(F/K)$ is a finite Abelian group. Since p does not ramify in K, we know $p \nmid |\Delta|$.

By the Weil pairing, $K(E_p) \supset K(\mu_p)$. If $E(K)[p] \neq 0$, then the degree of the extension $K(E_p)/K(\mu_p)$ is either trivial or equal to p. Since $p \nmid |\Delta|$, it forces

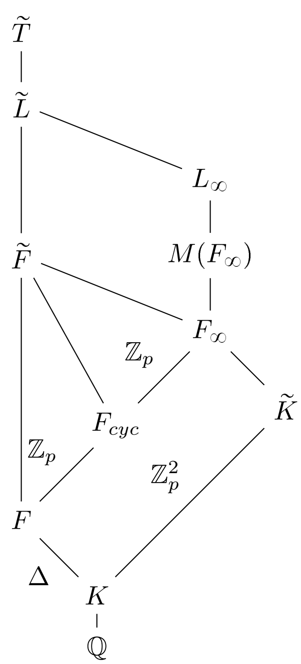
$$F = K(E_p) = K(\mu_p).$$

Further, from the theory of CM we obtain $F_\infty = F\widetilde{K}$. Thus, the trivializing extension F_∞ contains F_{cyc} and is an admissible p-adic Lie extension. Note $F_\infty \subseteq \widetilde{F}$.

Denote by $\widetilde{L}$ (resp. L_∞) the pro-p Hilbert class field tower of $\widetilde{F}$ (resp. F_∞). This is the maximal Abelian unramified pro-p-extension of $\widetilde{F}$ (resp. F_∞). Denote by $\widetilde{T}$ the maximal Abelian extension of $\widetilde{F}$ unramified outside S. Set the notation

$$\widetilde{X} = X_{nr}^{\widetilde{F}} = \mathrm{Gal}(\widetilde{L}/\widetilde{F}), \quad X_{nr}^{F_\infty} = \mathrm{Gal}(L_\infty/F_\infty), \quad X_S^{\widetilde{F}} = \mathrm{Gal}(\widetilde{T}/\widetilde{F}). \tag{5}$$

For convenience, the field diagram of the set up is drawn below.



For any p-adic Lie extension $\mathcal{L}/F$, the Galois group $\mathrm{Gal}(\mathcal{L}/F)$ is denoted by $G_{\mathcal{L}}$. In this section, for most parts $\mathcal{L} = F_\infty$ or $\widetilde{F}$. Let $M(\mathcal{L})$ be the maximal unramified

Abelian p-extension of $\mathcal{L}$ such that every prime of $\mathcal{L}$ above p splits completely. Recall

Conjecture (Generalized Greenberg's Conjecture for $\widetilde{F}/F$)**.** *With notation as above, $X_{nr}^{\tilde{F}}$ is a pseudonull $\Lambda(G_{\widetilde{F}})$-module.*

Let E be an elliptic curve over F and $\mathcal{L}/F$ be as above. When $G_S(\mathcal{L})$ acts trivially on E_{p^∞}, Conjecture B for $\mathfrak{Y}(E/\mathcal{L})$ has an equivalent formulation in terms of pseudonullity of a Galois extension of $\mathcal{L}$ (see [CS05, Page 827]).

Conjecture (Conjecture B for $\mathcal{L}/F$)**.** *Let E be an elliptic curve defined over F. Let $\mathcal{L}/F$ be a pro-p, p-adic Lie extension such that $G_S(\mathcal{L})$ acts trivially on E_{p^∞}. Set $\mathfrak{Y}(\mathcal{L}) = \mathrm{Gal}\,(M(\mathcal{L})/\mathcal{L})$. Then $\mathfrak{Y}(\mathcal{L})$ is a pseudonull $\Lambda(G_{\mathcal{L}})$-module.*

In the first main theorem of this section, we prove that the for an S-admissible p-adic Lie extension $\mathcal{L}/F$ that contains the trivializing extension F_∞, pseudonullity of the Iwasawa module $X_{nr}^{\mathcal{L}}$ is equivalent to the pseudonullity of a quotient module.

Theorem 4.1. *Let $\mathcal{L} = F_\infty$ or $\widetilde{F}$. Then $X_{nr}^{\mathcal{L}}$ is pseudonull if and only if Conjecture B holds for $\mathfrak{Y}(E/\mathcal{L})$. Equivalently, $X_{nr}^{\mathcal{L}}$ is pseudonull if and only if $\mathfrak{Y}(\mathcal{L})$ is pseudonull.*

We begin by stating a result from [Ven03]. See also [Ven03, Page 32].

Lemma 4.2. *[Ven03, Theorem 4.9] Assume that $\mu_p \subset F$ and let $\mathcal{L} = F_\infty$ or $\widetilde{F}$. $X_{nr}^{\mathcal{L}}$ is pseudo-null if and only if $X_S^{\mathcal{L}}$ is torsion-free.*

Proof of Theorem 4.1. By Lemma 4.2, to prove the theorem it is enough to prove

$$X_S^{\mathcal{L}} \text{ is torsion-free} \;\Leftrightarrow\; \text{Conjecture B holds for } \mathfrak{Y}(E/\mathcal{L}). \tag{6}$$

Simplifying the LHS of (6)*:* In the classical setting [Ven03, Section 4.1.1],

$$X_S^{\mathcal{L}} = H^1(G_S(\mathcal{L}), \mathbb{Q}_p/\mathbb{Z}_p)^\vee \simeq \mathrm{Gal}(F_S/\mathcal{L})^{ab}(p).$$

In this setting, the rightmost column of the Powerful Diagram becomes (cf Figure 1)

$$0 \to X_S^{\mathcal{L}} \to Y_S^{\mathcal{L}} \to J^{\mathcal{L}} \to 0.$$

Since it is well-known that $J_{\mathcal{L}}$ has no non-zero torsion submodules, it follows

$$X_S^{\mathcal{L}} \text{ is torsion-free} \;\Leftrightarrow\; Y_S^{\mathcal{L}} \text{ is torsion-free}. \tag{7}$$

Simplifying the RHS of (6)*:* From the standard Poitou-Tate sequence (see [CS05, Equation 45]) it follows that Conjecture B for $\mathfrak{Y}(E/\mathcal{L})$ is equivalent to the pseudonullity of the Iwasawa cohomology module $\mathcal{Z}^2(E/\mathcal{L})$ (cf (3)). It is known [Ven03, Propostion 2.12]

$$\mathcal{Z}^2(E/\mathcal{L}) = \mathcal{Z}^2(\mathbb{Z}_p(1)) \otimes T_p(E/\mathcal{L}). \tag{8}$$

This gives

$$\begin{aligned} \text{Conjecture B holds for } \mathfrak{Y}(E/\mathcal{L}) \Leftrightarrow\;& \mathcal{Z}^2(E/\mathcal{L}) \text{ is pseudo-null} \\ \Leftrightarrow\;& \mathcal{Z}^2(\mathbb{Z}_p(1)) \text{ is pseudonull.} \end{aligned}$$

To prove the theorem it suffices to show $Y_S^{\mathcal{L}}$ is torsion-free if and only if $\mathcal{Z}^2(\mathbb{Z}_p(1))$ is pseudonull. This is precisely [Ven03, Proposition 2.16]. □

The second result we prove shows that Conjecture B is indeed a generalization of GGC. We keep the notation introduced at the beginning of this section.

Theorem 4.3. *If there exists one CM elliptic curve E/K, such that $\mathfrak{Y}(E/K(E_{p^\infty}))$ is pseudonull, then GGC holds for K, $K(\mu_p)$, and $K(E_p)$.*

The following lemma assures pseudo-nullity over a larger tower, once it holds for a non-trivial quotient.

Lemma 4.4 (Pseudonullity Lifting Lemma)**.** *Let $\mathcal{F}/\mathbb{Q}$ be a finite Galois extension that contains μ_p. As before, let $\widetilde{\mathcal{F}}$ be the compositum of all $\mathbb{Z}_p$-extensions of $\mathcal{F}$. Let $\mathrm{Gal}(\widetilde{\mathcal{F}}/\mathcal{F}) \simeq \mathbb{Z}_p^n$ and $\mathcal{F}' \subset \widetilde{\mathcal{F}}$ be such that $\mathrm{Gal}(\mathcal{F}'/\mathcal{F}) \simeq \mathbb{Z}_p^d$ for some $2 \leqslant d < n$. If $X_{nr}^{\mathcal{F}'}$ is pseudonull then GGC holds for $\widetilde{\mathcal{F}}/\mathcal{F}$.*

Proof. This lemma is a special case of [Ban07, Theorem 12]. Since $\mathcal{F}$ contains μ_p, the technical conditions in the mentioned theorem are satisfied by [LNQD00, Theorem 3.2] or [Ban07, Remark 15]. □

The next lemma studies pseudonullity of Galois modules under base change.

Lemma 4.5 (Pseudonullity Shifting Lemma)**.** *Let $\mathcal{F}$ be a number field and $\mathcal{F}'/\mathcal{F}$ be a $\mathbb{Z}_p^d$-extension. Suppose $\mathcal{F}_1/\mathcal{F}$ is a finite extension such that $\mathbb{F} = \mathcal{F}' \cdot \mathcal{F}_1$. If $X_{nr}^{\mathbb{F}}$ is a pseudonull module, then $X_{nr}^{\mathcal{F}'}$ is a pseudonull module.*

Proof. For a proof, see [Kle16, Theorem 3.1(1)]. □

We can now provide a proof of the theorem.

Proof of Theorem 4.3. Let E/K be a CM elliptic curve such that Conjecture B holds for $\mathfrak{Y}(E/K(E_{p^\infty}))$. By [Rub89, Lemma 2], it is guaranteed that E has good reduction everywhere over $F = K(E_p)$. We choose the set S to be precisely the set of Archimedean primes and primes above p.

We had set the notation $F_\infty = K(E_{p^\infty})$. Conjecture B holds for $\mathfrak{Y}(F_\infty)$ by assumption. By Theorem 4.1, $\mathfrak{Y}(F_\infty)$ is pseudonull if and only if $X_{nr}^{F_\infty}$ is pseudonull. Using Lemma 4.4 with $\mathcal{F} = F = K(E_p)$ and $\mathcal{F}' = F_\infty$, pseudonullity of $X_{nr}^{F_\infty}$ can be lifted; thus GGC holds for $\widetilde{F}/F$.

By the theory of CM, $F_\infty = F\widetilde{K}$. Here $\widetilde{K}$ is the compositum of all $\mathbb{Z}_p$-extensions of K. Since K is an (imaginary) quadratic extension, $\mathrm{Gal}(\widetilde{K}/K) \simeq \mathbb{Z}_p^2$ and $\widetilde{K}$ is the unique $\mathbb{Z}_p^2$ extension of K. Suppose Conjecture B holds for $\mathfrak{Y}(F_\infty)$. Applying Lemma 4.5 with $\mathbb{F} = F_\infty = F\widetilde{K}$, pseudonullity of $X_{nr}^{F_\infty}$ can be "shift down" to pseudonullity of $X_{nr}^{\widetilde{K}}$. This is precisely GGC for the imaginary quadratic field K.

Now, $K(\mu_p) \subseteq K(E_p)$. So, there is a $\mathbb{Z}_p^2$- extension of $K(\mu_p)$, say K'_∞, such that

$$K'_\infty = K(\mu_p)\widetilde{K}; \quad F_\infty = FK'_\infty.$$

Applying Lemma 4.5 with $\mathbb{F} = F_\infty = FK'_\infty$, pseudonullity of $X_{nr}^{F_\infty}$ can be "shift down" to the pseudonullity of $X_{nr}^{K'_\infty}$. Again by Lemma 4.4, pseudonullity can be "lifted"; thus GGC holds for $K(\mu_p)$. □

Remark 4.6. It is possible to imitate the proof of Theorem 4.3 to show that if there exists one CM elliptic curve $E/\mathbb{Q}$ such that Conjecture B holds for $\mathfrak{Y}(E/\mathbb{Q}(E_{p^\infty}))$, then GGC holds for $\mathbb{Q}(\mu_p)$. This recovers a result of McCallum [McC01].

5. Pseudonullity Conjecture for Elliptic Curves

As remarked in Section 1, evidence for Conjecture B is very sparse. In [CS05], the authors considered two possible examples of elliptic curves for which Conjecture B would hold, which were however conditional. In Example 4.8 (loc. cit.) this was contingent on the existence of a point of infinite order over the trivializing extension. It is worth mentioning that computational methods could not resolve this question in the last two decades. The main thrust of this section is to remove the conditionality in the concrete examples considered in [CS05] and provide evidence for Conjecture B (see Theorem 5.4).

5.1. **Finite Fine Selmer Group at the Cyclotomic Level.** In this section, we study Conjecture B for CM elliptic curves.

Let E be a CM elliptic curve defined over a number field F and p be an odd prime of good ordinary reduction. In this case, $\mathrm{Gal}(F_\infty/F)$ contains an open subgroup which is Abelian and isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. Assume $G = \mathrm{Gal}(F_\infty/F)$ is pro-p, and set $H = \mathrm{Gal}(F_\infty/F_{\mathrm{cyc}})$.

For any p-adic Lie group $\mathcal{G}$, let $\Lambda(\mathcal{G})$ be its associated Iwasawa algebra and I be the augmentation ideal of $\Lambda(\mathcal{G})$. For a finitely generated $\Lambda(\mathcal{G})$-module M, the co-invariance $M_{\mathcal{G}} := H_0(\mathcal{G}, M) = M/IM$ is a finitely generated $\mathbb{Z}_p$-module.

Lemma 5.1. *With the setting as above, the following natural map is a pseudo-isomorphism, i.e. it has a finite kernel and cokernel,*

$$\mathfrak{Y}(E/F_\infty)_H \to \mathfrak{Y}(E/F_{\mathrm{cyc}}).$$

Proof. Consider the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R(E/F_{\mathrm{cyc}})_p & \longrightarrow & \mathrm{Sel}(E/F_{\mathrm{cyc}})_p & \longrightarrow & C(F_{\mathrm{cyc}})_p & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\
0 & \longrightarrow & R(E/F_\infty)_p^H & \longrightarrow & \mathrm{Sel}(E/F_\infty)_p^H & \longrightarrow & C(F_\infty)_p^H & &
\end{array}$$

β is an isomorphism [PR81, Lemma 1.1(i) and Lemma 1.3]. Therefore $\ker(\beta)$ and $\mathrm{coker}(\beta)$ are trivial; hence $\ker(\alpha) = 0$. We know $\ker(\gamma) = \bigoplus_{v|p} H^1(H_v, E(F_{\infty,v})[p^\infty])$ is finite [CSW01]. Therefore, by the snake lemma, $\mathrm{coker}(\alpha)$ must be finite. $\square$

Since E is an elliptic curve with CM, both G and H are Abelian. In particular, $\Lambda(H) \simeq \mathbb{Z}_p[[T]]$.

Lemma 5.2. *Let M be a finitely generated $\Lambda(H)$-module. If M_H is a finite module, then M is a pseudonull $\Lambda(G)$-module.*

Proof. If M_H is finite, the higher homology groups, $H_i(H, M)$ are trivial for all $i > 0$ [Ser12, Chapter IV, Appendix II]. Since $\Lambda(H)$ is a regular local ring, the rank of a module is equal to its homological rank (see [How02]). Therefore, $\Lambda(H)$-rank of M is 0 and M is $\Lambda(H)$-torsion. The lemma follows from the equivalent definition of pseudonullity [VV03] (see Section 2). $\square$

The main theorem of this section is stated below.

Theorem 5.3. *With the set up as above, if $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ is finite, $\mathfrak{Y}(E/F_\infty)$ is a pseudonull $\Lambda(G)$-module.*

Proof. By Lemma 5.1, it follows that if $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ is a finite module, then $\mathfrak{Y}(E/F_\infty)_H$ is finite. The theorem follows from Lemma 5.2. $\square$

5.2. **Conjecture B for Regular Primes.** Let p be an odd prime. Consider an elliptic curve E defined over F, such that $F \supset \mu_p$ and p does not divide the class number of F. We prove that Conjecture B holds for the trivializing extension $F(E_{p^\infty})$.

Theorem 5.4. *Consider a Galois extension $F/\mathbb{Q}$ containing μ_p where $p \nmid |\mathrm{Cl}(F)|$ and p is totally ramified in F. Suppose F_∞/F is a pro-p extension. For E an elliptic curve defined over F, $\mathfrak{Y}(E/F_\infty)$ is a pseudonull module.*

Proof. By the definition of pseudonullity, it is enough to prove

$$E^i(\mathfrak{Y}(E/F_\infty)) = 0 \quad \text{for } i = 0, 1. \tag{9}$$

By Poitou-Tate duality [CS05, Equation 43],

$$\mathfrak{Y}(E/F_\infty) \hookrightarrow \mathcal{Z}^2(E/F_\infty).$$

Therefore $\mathfrak{Y}(E/F_\infty)$ is a pseudonull $\Lambda(G)$-module if $\mathcal{Z}^2(E/F_\infty)$ is pseudonull, i.e.

$$E^i(\mathcal{Z}^2(E/F_\infty)) = 0 \quad \text{for } i = 0, 1.$$

Since F_∞ is the trivializing extension, we know $H^2(G_S(F_\infty), E_{p^\infty}) = 0$ and $\mathcal{Z}^2(E/F_\infty)$ is a torsion $\Lambda(G)$-module [CS05, Lemma 2.4]. Thus, $E^0(\mathcal{Z}^2(E/F_\infty)) = 0$. It is left to show that $E^1(\mathcal{Z}^2(E/F_\infty)) = 0$ which is the content of the following proposition. □

Proposition 5.5. *With the setting as in the statement of Theorem 5.4,*

$$E^1(\mathcal{Z}^2(E/F_\infty)) = 0.$$

Proof. Recall [OV03, Proposition 3.5]. Suppose all terms have standard meaning,

$$E^1(\mathcal{Z}^2(E/F_\infty)) \simeq H^1(G_S(F_\infty), E_{p^\infty})^\vee_{tors}. \tag{10}$$

To prove the proposition it is enough to show $H^1(G_S(F_\infty), E_{p^\infty})^\vee_{tors} = 0$. This is done by a thorough analysis of the Powerful Diagram (cf Figure 1). For this proof we retain the notation introduced in Section 2.1.

The rightmost column of the Powerful Diagram is the short exact sequence

$$0 \to H^1(G_S(F_\infty), E_{p^\infty})^\vee \to Y_\infty \to J_\infty \to 0. \tag{11}$$

Since J_∞ has no non-trivial torsion submodules [OV03, Page 27], the proposition follows if Y_∞ has no Λ-torsion. Since F_∞ is the trivializing extension, the top row of the Powerful Diagram is the following short exact sequence,

$$0 \to \left(\mathcal{N}^{ab}(p) \otimes_{\mathbb{Z}_p} E^\vee_{p^\infty}\right)_{\mathcal{H}} \to \Lambda(G)^{2d} \to Y_\infty \to 0 \tag{12}$$

where $d := \dim_{\mathbb{F}_p} H^1(\mathcal{G}, \mathbb{F}_p)$. We now analyse the first term of the exact sequence. It is known [OV03, Proof of Theorem 3.2]

$$\left(\mathcal{N}^{ab}(p) \otimes_{\mathbb{Z}_p} E^\vee_{p^\infty}\right)_{\mathcal{H}} = \Lambda(G)^{2s}$$

where $s = d - r_2 - 1$ when $p \neq 2$. Therefore (12) becomes

$$0 \to \Lambda(G)^{2s} \to \Lambda(G)^{2d} \to Y_\infty \to 0. \tag{13}$$

By [NSW08, Lemma 10.7.3] we know

$$d = 1 + \sum_{\mathfrak{p} \in S} \delta_{\mathfrak{p}} - \delta + \dim_{\mathbb{F}_p}(\mathrm{Cl}_S(F)/p). \tag{14}$$

where $\delta_{\mathfrak{p}}$ (resp. δ) is 1 if $\mu_p \subseteq F_{\mathfrak{p}}$ (resp. $\mu_p \subseteq F$) and 0 otherwise. By hypothesis, F contains μ_p, so $\delta = 1$. Also by hypothesis, $p \nmid |\mathrm{Cl}(F)|$. Since the class group of a number field is always finite and the S-class group is a subgroup of the class group, it follows that $\dim_{\mathbb{F}_p}(\mathrm{Cl}_S(F)/p) = 0$. Choose $S = S_p \cup S_{bad} \cup S_\infty$. Since p ramifies totally in F, $|S_p| = 1$. Further, since F is a totally imaginary field, $|S_\infty| = r_2$. Thus,

$$\begin{aligned} |S| &= |S_p| + |S_\infty| + |S_{bad}| \\ &= 1 + r_2 + |S_{bad}| \end{aligned}$$

Under our hypothesis, the contribution of $\delta_{\mathfrak{q}} = 0$ for $\mathfrak{q} \in S \backslash S_p$. Therefore from (14)

$$\begin{aligned} d &= r_2 + 1. \\ \Rightarrow s &= d - r_2 - 1 = 0. \end{aligned}$$

Since $s = 0$, from (13) it follows $Y_\infty \simeq \Lambda(G)^{2d}$ and hence it is torsion free. This finishes the proof. $\square$

5.3. **Numerical Examples for Conjecture B.** Recall p is called *regular* if it does not divide the class number of $\mathbb{Q}(\mu_p)$. The special case of Theorem 5.4, recorded below fully settles numerical examples considered in [CS05].

Theorem 5.6. *Let E be an elliptic curve defined over $\mathbb{Q}$. Set $F = \mathbb{Q}(\mu_p)$ such that p is a regular prime. Then Conjecture B is true for $\mathfrak{Y}(E/\mathbb{Q}(E_{p^\infty}))$.*

Example 5.7. [CS05, Example 4.7] Consider the following elliptic curve $E/\mathbb{Q}$,

$$E : y^2 + xy = x^3 - x - 1.$$

This is a non-CM elliptic curve of conductor 294. Take $p = 7$. Here, $F_\infty = \mathbb{Q}(E_{7^\infty})$ is a pro-7 extension of $F = \mathbb{Q}(\mu_7)$. E has good ordinary reduction at the unique prime above 7, split multiplicative reduction at the primes above 2, and the unique prime above 3. The conditions of Theorem 5.6 are satisfied, so Conjecture B holds.

Example 5.8. [CS05, Example 4.8] Consider the elliptic curve $E/\mathbb{Q}$ defined by

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

This is an elliptic curve of conductor 150 without CM. With $p = 5$, $F_\infty = \mathbb{Q}(E_{5^\infty})$ is a pro-5 extension of $F = \mathbb{Q}(\mu_5)$. It was shown in [CS05] that either Conjecture B holds or there is no point of infinite order over F_∞. The latter possibility was not ruled out in the intervening years, despite advances in computational methods. Our theorem settles this example theoretically as the hypotheses are satisfied.

Example 5.9. [CS00, Chapter 5] Consider the elliptic curve $E/\mathbb{Q}$ defined by

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

This is an elliptic curve of conductor 11 without CM. When $F = \mathbb{Q}(\mu_5)$ and $p = 5$, it is proven in [CS00, Theorem 5.4] that $\mathrm{Sel}(E/F_{\mathrm{cyc}})_p = 0$. Theorem 5.6 shows that Conjecture B holds for $\mathfrak{Y}(E/F_\infty)$ where $F_\infty = \mathbb{Q}(E_{5^\infty})$.

We give one final example from the CM case to illustrate our theorem.

Example 5.10. Consider the elliptic curve $E/\mathbb{Q}$ defined by

$$E : y^2 + y = x^3 + 156.$$

This is an elliptic curve of conductor 256 with CM by $\mathbb{Q}(\sqrt{-3})$. When $F = \mathbb{Q}(\mu_3)$ and $p = 3$, it is known (see [LMF13, Elliptic Curve 225.d2]) that $E(\mathbb{Q})_{tors} = \mathbb{Z}/3\mathbb{Z}$. Set $F_\infty = \mathbb{Q}(E_{3^\infty})$. It follows from the Weil pairing that F_∞/F is a pro-3 extension.

Theorem 5.6 shows that Conjecture B holds for $\mathfrak{Y}(E/F_\infty)$. As noted in Remark 4.6, we recover that GGC holds for $\mathbb{Q}(\mu_3)$.

6. Applications

In this section, we study the implications of Conjecture B to the four term exact sequence studied in proving the Main Conjecture.

6.1. **The (Cyclotomic) Main Conjecture.** For simplicity, assume the base field is $\mathbb{Q}$. The cyclotomic Main Conjecture for the p-primary Selmer group $\mathrm{Sel}_p(E/\mathbb{Q}_{\mathrm{cyc}})$ is the following statement.

Conjecture. *Let E be an elliptic curve defined over $\mathbb{Q}$ with good ordinary or multiplicative reduction at p. The Pontryagin dual $\mathfrak{X}(E/\mathbb{Q}_{\mathrm{cyc}})$ of the Selmer group is a torsion $\Lambda(\Gamma)$-module. Furthermore, its characteristic ideal is generated by a p-adic L-function $\mathcal{L}(E/\mathbb{Q}_{\mathrm{cyc}})$ in $\Lambda(\Gamma)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$. If $E[p]$ is an irreducible* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-representation, then $\mathcal{L}(E/\mathbb{Q}_{\mathrm{cyc}})$ is in $\Lambda(\Gamma)$.*

As a consequence of global duality, we have the following short exact sequence of torsion $\Lambda(\Gamma)$-modules

$$0 \to \frac{\mathcal{Z}^1(E/\mathbb{Q}_{\mathrm{cyc}})}{\langle Z\rangle} \to \frac{\mathcal{Z}^1_p(E/\mathbb{Q}_{\mathrm{cyc},p})}{\langle Z_p\rangle} \to \mathfrak{X}(E/\mathbb{Q}_{\mathrm{cyc}}) \to \mathfrak{Y}(E/\mathbb{Q}_{\mathrm{cyc}}) \to 0. \tag{15}$$

Here, $\mathcal{Z}^1(E/\mathbb{Q}_{\mathrm{cyc}})$ is the compact Iwasawa cohomology group as defined in (3) and $\mathcal{Z}^1_p(E/\mathbb{Q}_{\mathrm{cyc},p})$ is the the local Iwasawa cohomology group which is defined analogously. Here, Z is the Euler system constructed by Kato which is a free $\Lambda(\Gamma)$-module inside $\mathcal{Z}^1(E/\mathbb{Q}_{\mathrm{cyc}})$ and $\langle Z\rangle$ is the submodule generated by the Euler system. Under the natural functorial map, the image of $\langle Z\rangle$ generates a submodule of the local Iwasawa cohomolgy group, denoted by $\langle Z_p\rangle$.

The Coleman isomorphism interpolates the (dual) Bloch-Kato exponential maps. This isomorphism, yields the following identification

$$\mathrm{Col}\colon \mathcal{Z}^1_p(E/\mathbb{Q}_{\mathrm{cyc},p}) \simeq \Lambda(\Gamma).$$

It was further shown by Kato that the image $\mathrm{Col}(Z_p)$ is precisely the p-adic L-function that appears in the statement of the Main Conjecture.

The philosophy in proving the Main Conjecture is to show that the first and the last term of the short exact sequence 15 have the same characteristic power series. Since the characteristic power series is multiplicative in exact sequences, this forces the second and the third term to have the same characteristic power series which is precisely the statement of the Main Conjecture.

In a large number of examples considered in the earlier sections, $\mathfrak{X}(E/\mathbb{Q}_{\mathrm{cyc}})$ was trivial. This yields the isomorphism

$$\frac{\mathcal{Z}^1(E/\mathbb{Q}_{\mathrm{cyc}})}{\langle Z\rangle} \simeq \frac{\mathcal{Z}^1_p(E/\mathbb{Q}_{\mathrm{cyc},p})}{\langle Z_p\rangle}.$$

If the Main Conjecture holds, the triviality of the dual fine Selmer group implies that the first term is pseudo-null (equivalently finite in a $\mathbb{Z}_p$-extension). But we know that the second term of 15 is of projective dimension 1, so it has no non-zero finite submodules. Thus, the first term must must be trivial. This shows that if the dual Selmer group is trivial over the cyclotomic extension, all terms in the exact sequence 15 are trivial. In particular, the Euler system generates $\mathcal{Z}^1(E/\mathbb{Q}_{\mathrm{cyc}})$.

More generally, consider a p-adic Lie extension $\mathcal{L}/\mathbb{Q}$ of dimension at least 2. We obtain a short exact sequence similar to 15

$$0 \to \frac{\mathcal{Z}^1(E/\mathcal{L})}{\langle Z\rangle} \to \frac{\mathcal{Z}^1_p(E/\mathcal{L}_p)}{\langle Z_p\rangle} \to \mathfrak{X}(E/\mathcal{L}) \to \mathfrak{Y}(E/\mathcal{L}) \to 0, \tag{16}$$

where $\mathcal{L}_p$ is the localization of $\mathcal{L}$ at p and the other terms are defined as before. It is important to note that in this full generality, existence of the Euler system $\langle Z\rangle$ is still conjectural. However, they have been constructed in some special cases and the validity of the Main Conjecture has been verified, see [Rub91], [PR04], [SU14].

Let $E/\mathbb{Q}$ be an elliptic curve. If the Main Conjecture is valid over $\mathbb{Q}(E_{p^\infty})$ and Conjecture B holds for $\mathfrak{Y}(E/\mathbb{Q}(E_{p^\infty}))$, then by the same argument as before we have that $\frac{\mathcal{Z}^1(E/\mathbb{Q}(E_{p^\infty}))}{\langle Z\rangle}$ must be pseudo-null and therefore trivial.

6.2. **Tamagawa Number Conjecture.** The next application relates to isogeny invariance and the Tamagawa Number conjecture (TNC), as considered by Bloch and Kato in [BK07] (see also [Kin01] and [Bar02]). The context and setting is as in [BK07, §7]; one considers the motive associated to an elliptic curve with complex multiplication. Thus $E/\mathbb{Q}$ is an elliptic curve with CM by the ring of integers in an imaginary quadratic field. Note $\mathcal{Z}^i(E/\mathbb{Q}) = H^i(G_S(\mathbb{Q}), T_pE(1))$.

For the Galois extension $\mathcal{L}/\mathbb{Q}$ with Galois group G, let φ be the natural map

$$\varphi : \left(\mathcal{Z}^1(T_p(E)(1)/\mathcal{L})\right)_G \to H^1(G_S(\mathbb{Q}), T_p(E)(1)).$$

This map is an inclusion. When the Euler system exists, let $\mathfrak{z}$ denote its image under this map.

The extensions $\mathcal{L}$ that will be considered is either the cyclotomic extension $\mathbb{Q}_{\mathrm{cyc}}$ or the trivialising extension $\mathbb{Q}(E_{p^\infty})$ with Galois group G which is pro-p.

The essence of the TNC is the assertion that $\mathcal{Z}^i(E/\mathbb{Q})$ is finite and

$$\#\left(\frac{\mathcal{Z}^1(T_p(E)(1)/\mathcal{L})}{\mathfrak{z}}\right) = \#\left(\mathcal{Z}^2(T_p(E)(1)/\mathcal{L})\right). \tag{17}$$

Viewed through the lens of Iwasawa theory, this translates to the assertion that the Euler characteristics of the first and last terms in the exact sequence (16), when defined, are finite and equal.

It is shown in [BK07, Proposition 5.14] that the TNC is invariant under isogeny. Given two isogenous elliptic curves E and E' over $\mathbb{Q}$, the validity of TNC for one implies the same for the other. Recall that over the trivialising extension $\mathbb{Q}(E_{p^\infty})$, Conjecture B implies that $\mathcal{Z}^2(T_p(E)(1)/\mathbb{Q}(E_{p^\infty}))$ is pseudonull; hence its Euler characteristic, whenever defined, is trivial. The same is true for the Euler characteristic of $\mathcal{Z}^2(T_p(E')(1)/\mathbb{Q}(E_{p^\infty}))$.

Consider the Euler system element $Z_{\infty,E}$ (resp. $Z'_{\infty,E'}$) of E (resp. E') in $\mathcal{Z}^1(T_p(E)(1)/\mathbb{Q}(E_{p^\infty})$ (resp. $\mathcal{Z}^1(T_p(E')(1)/\mathbb{Q}(E_{p^\infty}))$. Denote the corresponding $\Lambda(\Gamma)$-submodules they generate by $\langle Z\rangle$ (resp. $\langle Z'\rangle$). Let the image of the Euler system in $H^1(\mathbb{Q}_S/\mathbb{Q}, T_p(E)(1))$ (resp. in $H^1(\mathbb{Q}_S/\mathbb{Q}, T_p(E')(1))$) be $\overline{\mathfrak{z}}$ (resp. $\overline{\mathfrak{z}'}$). For a compact $\Lambda(G)$-module M, let $\chi_G(M)$ denote the G-Euler characteristic of M, when it is defined. Recall that Conjecture B is isogeny invariant, so when the Conjecture holds for E (and hence also for E') over $\mathbb{Q}(E_{p^\infty})$, we have

$$\chi_G\left(\mathcal{Z}^2(T_p(E)(1)/\mathbb{Q}(E_{p^\infty}))\right) = \chi_G\left(\mathcal{Z}^2\left(T_p(E')(1)/\mathbb{Q}(E_{p^\infty})\right)\right) = 1.$$

Further, we also obtain

$$\chi_G\left(\frac{\mathcal{Z}^1\left(T_p(E)(1)/\mathbb{Q}(E_{p^\infty})\right)}{\langle Z\rangle}\right) = \chi_G\left(\frac{\mathcal{Z}^1\left(T_p(E')(1)/\mathbb{Q}(E_{p^\infty})\right)}{\langle Z'\rangle}\right) = 1.$$

If $\theta : E \to E'$ is the isogeny map, let θ_* be the induced functorial map, then

$$\theta_* : \mathcal{Z}^1\left(T_p(E)(1)/\mathbb{Q}(E_{p^\infty})\right) \to \mathcal{Z}^1\left(T_p(E')(1)/\mathbb{Q}(E_{p^\infty})\right).$$

As explained in Section 6.1, we have the following equalities of $\Lambda(G)$-modules

$$\langle Z_{\infty,E}\rangle = \mathcal{Z}^1\left(T_p(E)/\mathbb{Q}(E_{p^\infty})\right),$$
$$\langle \theta_*\left(Z_{\infty,E}\right)\rangle = \langle Z'_{\infty,E'}\rangle = \mathcal{Z}^1\left(T_p(E')/\mathbb{Q}(E_{p^\infty})\right),$$

It would be interesting to explicitly understand the precise relationship between the elements $\theta_*\left(Z_{\infty,E}\right)$ and $Z'_{\infty,E'}$, given that they generate the same $\Lambda(G)$-module.

The final application that we record is the observation that examples where the fine Selmer groups vanish also provide evidence for a conjecture of Jannsen (see [Jan89, Conjecture 1]).

Acknowledgements

The first author thanks University of British Columbia for its hospitality. The second author is supported by the NSERC Discovery Grant 2019-03987. We thank Kumar Murty, Meng Fai Lim, Kestutis Česnavičius, Sören Kleine, Andrea Bandini, and Ralph Greenberg for many helpful discussions.

References

[Ban07] Andrea Bandini. Greenberg's conjecture and capitulation in $\mathbb{Z}_p^d$-extensions. *Journal of Number Theory*, 122(1):121–134, 2007.

[Bar02] Francesc Bars. On the Tamagawa number conjecture for CM elliptic curves defined over $\mathbb{Q}$. *Journal of Number Theory*, 95(2):190–208, 2002.

[BCG+15] FM Bleher, T Chinburg, R Greenberg, M Kakde, G Pappas, R Sharifi, and MJ Taylor. Higher Chern classes in Iwasawa theory. *arXiv preprint arXiv:1512.00273*, 2015.

[BK07] Spencer Bloch and Kazuya Kato. l-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift*, pages 333–400. Springer, 2007.

[CS00] John Coates and Ramdorai Sujatha. *Galois cohomology of elliptic curves.* Narosa, 2000.

[CS05] John Coates and Ramdorai Sujatha. Fine Selmer groups of elliptic curves over p-adic Lie extensions. *Mathematische Annalen*, 331(4):809–839, 2005.

[CSW01] John Coates, Ramdorai Sujatha, and Jean-Pierre Wintenberger. On the Euler-Poincaré characteristics of finite dimensional p-adic Galois representations. *Publications mathematiques de l'IHES*, 93:107–143, 2001.

[Gre99] R Greenberg. Iwasawa theory for elliptic curves. Arithmetic theory of elliptic curves (Cetraro, 1997), 51–144. *Lecture Notes in Math*, 1716, 1999.

[Gre01a] Ralph Greenberg. Introduction to Iwasawa theory for elliptic curves. *Arithmetic algebraic geometry*, 9:407–464, 2001.

[Gre01b] Ralph Greenberg. Iwasawa theory—past and present. *Adv. Studies in Pure Math*, 30:335–385, 2001.

[HM00] Yoshitaka Hachimori and Kazuo Matsuno. On finite Λ-submodules of Selmer groups of elliptic curves. *Proceedings of the American Mathematical Society*, pages 2539–2541, 2000.

[How02] Susan Howson. Euler characteristics as invariants of Iwasawa modules. *Proceedings of the London Mathematical Society*, 85(3):634–658, 2002.

[Jan89] Uwe Jannsen. On the ℓ-adic cohomology of varieties over number fields and its galois cohomology. In *Galois Groups over mathbbQ*, pages 315–360. Springer, 1989.

[JS11] Somnath Jha and R Sujatha. On the Hida deformations of fine Selmer groups. *Journal of Algebra*, 338(1):180–196, 2011.

[Kin01] Guido Kings. The Tamagawa number conjecture for CM elliptic curves. *Invent. math.*, 143(3):571–627, 2001.

[Kle16] Sören Kleine. Relative extensions of number fields and Greenberg's generalised conjecture. *Acta Arithmetica*, 174:367–392, 2016.

[LMF13] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2013. [Online; accessed 29 September 2019].

[LNQD00] Arthur Lannuzel and Thong Nguyen Quan Do. Greenberg conjectures and pro-p-free extensions of a number field. *Manuscripta Mathematica*, 102(2):187–209, 2000.

[Maz72] Barry Mazur. Rational points of Abelian varieties with values in towers of number fields. *Inventiones mathematicae*, 18(3-4):183–266, 1972.

[McC01] William G McCallum. Greenberg's conjecture and units in multiple p-extensions. *American Journal of Mathematics*, 123(5):909–930, 2001.

[MR10] Barry Mazur and Karl Rubin. Ranks of twists of elliptic curves and Hilbert's tenth problem. *Inventiones mathematicae*, 181(3):541–575, 2010.

[Mur97] V Kumar Murty. Modular forms and the Chebotarev density theorem II. *London Mathematical Society Lecture Note Series*, pages 287–308, 1997.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. Cohomology of number fields, 2008.

[OV02] Yoshihiro Ochi and Otmar Venjakob. On the structure of Selmer groups over p-adic Lie extensions. *Journal of Algebraic Geometry*, 11(3):547–580, 2002.

[OV03] Yoshihiro Ochi and Otmar Venjakob. On the ranks of Iwasawa modules over p-adic Lie extensions. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 135, pages 25–43. Cambridge University Press, 2003.

[PR81] Bernadette Perrin-Riou. Groupe de Selmer d'une courbe elliptique à multiplication complexe. *Compositio Mathematica*, 43(3):387–417, 1981.

[PR04] Robert Pollack and Karl Rubin. The main conjecture for CM elliptic curves at supersingular primes. *Annals of mathematics*, pages 447–464, 2004.

[Rub89] Karl Rubin. Tate–Shafarevich groups of elliptic curves with complex multiplication. In *Algebraic Number Theory—in honor of K. Iwasawa*, pages 409–419. Mathematical Society of Japan, 1989.

[Rub91] Karl Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Inventiones mathematicae*, 103(1):25–68, 1991.

[Ser12] Jean-Pierre Serre. *Local algebra.* Springer Science & Business Media, 2012.

[SU14] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL_2. *Inventiones mathematicae*, 195(1):1–277, 2014.

[Ven02] Otmar Venjakob. On the structure theory of the Iwasawa algebra of a p-adic lie group. *Journal of the European Mathematical Society*, 4(3):271–311, 2002.

[Ven03] Otmar Venjakob. On the Iwasawa theory of p-adic Lie extensions. *Compositio Mathematica*, 138(1):1–54, 2003.

[VV03] Otmar Venjakob and Denis Vogel. A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory. *Journal fur die Reine und Angewandte Mathematik*, pages 153–192, 2003.

Department of Mathematics, University of Toronto, Bahen Centre, 40 St. George St., Room 6290, Toronto, Ontario, Canada, M5S 2E4

Email address: dkundu@math.utoronto.ca

Mathematics Department, 1984, Mathematics Road, University of British Columbia, Vancouver, Canada, V6T1Z2

Email address: sujatha@math.ubc.ca