CONTROL THEOREMS FOR FINE SELMER GROUPS

DEBANJANA KUNDU AND MENG FAI LIM

Abstract. We study the growth of the p-primary fine Selmer group, $R(E/F')$, of an elliptic curve over an intermediate sub-extension F' of a p-adic Lie extension, $\mathcal{L}/F$. We estimate the $\mathbb{Z}_p$-corank of the kernel and cokernel of the restriction map $r_{\mathcal{L}/F'} : R(E/F') \to R(E/\mathcal{L})^{\mathrm{Gal}(\mathcal{L}/F')}$ with F' a finite extension of F contained in $\mathcal{L}$. We also show that the growth of the fine Selmer groups in these intermediate sub-extension is related to the structure of the fine Selmer group over the infinite level. On specializing to classical (possibly non-commutative) p-adic Lie extensions, we prove finiteness of the kernel and cokernel and provide growth estimates on their orders.

1. Introduction

Iwasawa theory began as the study of ideal class groups over infinite towers of number fields [16]. In his fundamental paper [32], Mazur developed an analogous theory to study the growth of Selmer groups of Abelian varieties in $\mathbb{Z}_p$-extensions. He proved what is nowadays called a "control theorem", which we describe briefly here. Let A be an Abelian variety defined over a number field, F, with potential good ordinary reduction at all primes above p, and let $\mathcal{L}$ be a $\mathbb{Z}_p$-extension of F. For every intermediate sub-extension F' of $\mathcal{L}/F$, we have natural maps

$$s_{\mathcal{L}/F'} : \mathrm{Sel}(A/F') \longrightarrow \mathrm{Sel}(A/\mathcal{L})^{\mathrm{Gal}(\mathcal{L}/F')}$$

on the Selmer groups induced by the restriction maps on cohomology. Mazur's Control Theorem asserts that the kernel and cokernel of $s_{\mathcal{L}/F'}$ are finite and bounded independent of F'. The Control Theorem has subsequently been generalized to general p-adic Lie extensions by Greenberg [11]. Such a Control Theorem has great importance in Iwasawa theory. In [32], Mazur conjectured that the Selmer group $\mathrm{Sel}(A/F^{\mathrm{cyc}})$ is cotorsion over $\mathbb{Z}_p[\![\Gamma]\!]$, where $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$ and F^{cyc} is the cyclotomic $\mathbb{Z}_p$-extension of F. The first theoretical evidence towards this conjecture was provided by Mazur himself; using the Control Theorem, he verified the conjecture when $\mathrm{Sel}(A/F)$ is finite. Till date, this conjecture is known only when E is an elliptic curve over $\mathbb{Q}$ and F is an Abelian extension of $\mathbb{Q}$; see [18, 38]. The Selmer group $\mathrm{Sel}(A/F^{\mathrm{cyc}})$ is known to be related to a p-adic L-function via the *main conjecture*. Therefore, Mazur's Control Theorem opens up a channel to extract information on $\mathrm{Sel}(A/F)$ from the said main conjecture which provides an invaluable approach towards the study of the Birch and Swinnerton-Dyer Conjecture (for instance, see [18, 38, 45]). The Control Theorem connects the Selmer groups at the finite layers with the Selmer group over the infinite tower, thereby allowing one to deduce properties of this arithmetic object over the infinite tower from those at the finite layers, and vice versa.

Recently, there has been an interest in the study the *fine Selmer group* (see [6, 17, 23, 25, 27, 30, 36, 49, 51]). This is a subgroup of the classical Selmer group obtained by imposing stronger

Date: October 20, 2021.
2010 *Mathematics Subject Classification.* Primary 11R23.
Key words and phrases. control theorem, fine Selmer groups.

vanishing conditions at primes above p (see §5 for its definition). In [6], Coates and Sujatha initiated a systematic study of the fine Selmer group and postulated conjectures on its structure over a p-adic Lie extension. In this paper, we prove Control Theorems for fine Selmer groups of elliptic curves in general p-adic Lie extensions. This allows us to deduce properties of the fine Selmer group over the infinite tower from those at the finite layers, and vice versa. We remark that the (classical) Control Theorem can be proven only when the Abelian variety has potential good ordinary reduction at primes above p (see [10, p. 51]); however, our results do not require this hypothesis.

First, we establish estimates on the $\mathbb{Z}_p$-coranks of the kernel and cokernel of the restriction maps

$$r_{\mathcal{L}/F'} : R(E/F') \longrightarrow R(E/\mathcal{L})^{\mathrm{Gal}(\mathcal{L}/F')}$$

for a p-adic Lie extension $\mathcal{L}/F$. Using these, we show how the module theoretic structure of $R(E/\mathcal{L})$ determines the growth of $\mathbb{Z}_p$-coranks of $R(E/F')$ in intermediate sub-fields F'. To obtain sharper results, we specialize to three cases of p-adic Lie extensions: $\mathbb{Z}_p^d$-extensions, multi-false-Tate extensions, and the trivializing extension obtained by adjoining to F all the p-power division points of the elliptic curve, E. In each of these cases, we show (under appropriate assumptions) that the kernel and cokernel of the restriction map are finite, and establish growth estimates for their orders.

For a $\mathbb{Z}_p^d$-extension, Control Theorems have been studied in [39, 49, 51, 27], often with additional hypotheses. Our results however, are more general and can provide precise growth estimates for the kernel and cokernel of $r_{\mathcal{L}/F'}$. Further, we prove that if $R(E/F)$ is finite, then $R(E/F_\infty)$ is cotorsion over $\mathbb{Z}_p[\![G]\!]$, where $G = \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p^d$. This provides the impetus to conjecture the following.

Conjecture (Conjecture Y_d)**.** *Let F_∞ be a p-adic extension of F with $G = \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p^d$. Then $R(E/F_\infty)^\vee$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module.*

When $d = 1$, this is conjectured by the second named author in [27]. Currently, we refrain from formulating a more general conjecture, such as over a non-commutative p-adic extension *not* containing the cyclotomic $\mathbb{Z}_p$-extension, as we feel there is insufficient evidence towards the same.

Control Theorems for fine Selmer groups over non-commutative extensions (e.g. (multi) false-Tate extensions and trivializing extensions) have not been recorded in the literature. The key step of controlling the growth of the cokernel requires careful analysis of the local restriction maps at primes above p. We emphasize that the method of proof differs from that of Greenberg in [11], where he developed a Lie algebraic approach to attack this sort of problems. The main reason for requiring a different approach is that we want to estimate the growth of cohomology groups of open subgroups of a p-adic Lie group. However, open subgroups share the same Lie algebra, therefore the cohomology of the Lie algebra cannot distinguish the cohomology groups of the subgroups. Our analysis is therefore significantly different, intricate, and in fact, more effective than the case of the (classical) Selmer group. Our results show that the (conjectured) structure of the fine Selmer group at the infinite level has bearing on the growth of the size of $R(E/F_n)[p^n]$. Finally, we remark that our argument uses an improvement of Tate's Lemma (see Lemma 2.3) which should be interesting in its own right, and should potentially have further applications.

It would seem that some of our results may be extended to fine Selmer groups attached to Abelian varieties, modular forms or even broader classes of Galois representations of interest. Our case of representations arising from elliptic curves can therefore be seen as a first step in this line of study.

We now give an outline of the paper. In §2, 3, we record algebraic facts required throughout this article. In §4, we estimate the growth of cohomology groups of the p-division points of an elliptic curve in a p-adic Lie extension of a local field. In §5, we prove a Control Theorem which studies the growth of the $\mathbb{Z}_p$-coranks of the kernel and cokernel of the restrictions maps in a general

p-adic Lie extension. We also study an analogue where we vary the cyclotomic $\mathbb{Z}_p$-extensions of the intermediate sub-extensions. In §6, we prove more precise versions of the Control Theorem in special cases and establish (with growth estimates) the finiteness of the kernel and cokernel of the restriction map. In §7, we provide numerical examples to illustrate our otherwise abstract results.

2. Some Basic Estimates on Cohomology

In this section, we record estimates on the cohomology groups which are required throughout the article. For an Abelian group, M, let $M[p^j]$ denote the subgroup of M consisting of elements of M annihilated by p^j. Write $M[p^\infty]$ for $\cup_{j\geq 1} M[p^j]$. If M is a discrete p-primary Abelian group or a compact pro-p Abelian group, we define its *Pontryagin dual*, $M^\vee = \mathrm{Hom}_{\mathrm{cont}}(M,\ \mathbb{Q}_p/\mathbb{Z}_p)$. For a profinite group, G, and a G-module, M, let M^G be the subgroup of M consisting of elements fixed by G and M_G be the largest quotient of M on which G acts trivially. If M is a discrete G-module, we write $H^i\left(G,\ M\right)$ for the i-th Galois cohomology group of G with coefficients in M.

Lemma 2.1. *Let G be a pro-p group and M be a discrete G-module which is cofinitely generated over $\mathbb{Z}_p$. If $h_1(G) = \dim_{\mathbb{Z}/p\mathbb{Z}}\left(H^1\left(G,\ \mathbb{Z}/p\mathbb{Z}\right)\right)$ is finite, then*

$$\dim_{\mathbb{Z}/p\mathbb{Z}}\left(H^1\left(G,\ M\right)[p]\right) \leq h_1(G)\left(\mathrm{corank}_{\mathbb{Z}_p}(M) + \mathrm{ord}_p\left|M/M_{\mathrm{div}}\right|\right).$$

If $h_2(G) = \dim_{\mathbb{Z}/p\mathbb{Z}}\left(H^2\left(G,\ \mathbb{Z}/p\mathbb{Z}\right)\right)$ is finite, then

$$\dim_{\mathbb{Z}/p\mathbb{Z}}\left(H^2\left(G,\ M\right)[p]\right) \leq h_2(G)\left(\mathrm{corank}_{\mathbb{Z}_p}(M) + \mathrm{ord}_p\left|M/M_{\mathrm{div}}\right|\right).$$

Proof. The first inequality is proven in [29, Lemma 3.2]. The second inequality is proven similarly. □

When M is a finite G-module, we have the following sharper conclusion.

Lemma 2.2. *Let G be a pro-p group and M be a (finite) discrete G-module which is a finite p-group. If $h_1(G) = \dim_{\mathbb{Z}/p\mathbb{Z}}\left(H^1\left(G,\ \mathbb{Z}/p\mathbb{Z}\right)\right)$ is finite, then $H^1\left(G,\ M\right)$ is finite with*

$$\mathrm{ord}_p\left|H^1\left(G,\ M\right)\right| \leq h_1(G)\,\mathrm{ord}_p|M|\,.$$

If $h_2(G) = \dim_{\mathbb{Z}/p\mathbb{Z}}\left(H^2\left(G,\ \mathbb{Z}/p\mathbb{Z}\right)\right)$ is finite, then $H^2\left(G,\ M\right)$ is finite with

$$\mathrm{ord}_p\left|H^2\left(G,\ M\right)\right| \leq h_2(G)\,\mathrm{ord}_p|M|\,.$$

Proof. This follows from a standard dévissage argument and noting that the only simple discrete G-module is $\mathbb{Z}/p\mathbb{Z}$ with trivial G-action (cf. [34, Corollary 1.6.13]). □

Recall that if F is a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$ which contains a primitive root of unity, and $\Gamma = \mathrm{Gal}(F(\mu_{p^\infty})/F)$, then Tate's Lemma (see [46, p. 526]) asserts that $H^1(\Gamma, \mathbb{Q}_p/\mathbb{Z}_p(i)) = 0$ for $i \neq 0$. Observe that $H^0(\Gamma, \mathbb{Q}_p/\mathbb{Z}_p(i))$ is finite by virtue of $i \neq 0$. Motivated by this observation, we prove the following lemma which can be thought of as a generalization of Tate's Lemma. We note that our argument is different from the classical proof.

Lemma 2.3. *Let $G \cong \mathbb{Z}_p$ and M be a discrete, p-divisible G-module, which is cofinitely generated over $\mathbb{Z}_p$. If M^G is finite, then $H^1(G, M) = 0$.*

Proof. Set $U = M^\vee$. This is a compact $\mathbb{Z}_p[\![G]\!]$-module which is finitely generated over $\mathbb{Z}_p$. Thus, it is torsion over $\mathbb{Z}_p[\![G]\!]$, and

$$0 = \operatorname{rank}_{\mathbb{Z}_p[\![G_n]\!]}(U) = \operatorname{rank}_{\mathbb{Z}_p} U_G - \operatorname{rank}_{\mathbb{Z}_p} U^G.$$

This combined with the hypothesis that $U_G = (M^G)^\vee$ is finite, yields that U^G is finite. Since M is p-divisible, U is $\mathbb{Z}_p$-torsion free. Since U^G is finite, it follows that $U^G = 0$. But,

$$H^1(G,\ M)^\vee \cong (M_G)^\vee \cong U^G = 0,$$

where the first isomorphism follows from [34, Proposition 1.7.7(i)]. □

3. Modules over the Iwasawa Algebra

Throughout, p denotes a fixed prime. We record algebraic facts required throughout the article.

3.1. **Uniform pro-p groups.** In this subsection, we lay out some facts regarding a uniform pro-p group. For further background on these groups, we refer the reader to [8].

For a finitely generated pro-p group, G, we write $G^{p^n} = \langle g^{p^n} \mid g \in G\rangle$, i.e., the group generated by the p^n-th-powers of elements in G. We also write $G^{\{p^n\}} = \{g^{p^n} \mid g \in G\}$, i.e., the set consisting of the p^n-th-powers of elements in G. The pro-p group G is said to be *powerful* if $G/\overline{G^p}$ (resp. $G/\overline{G^4}$) is Abelian for odd p (resp. $p = 2$). Here $\overline{(\cdot)}$ denotes the closure with respect to the topology of the pro-p group. The lower p-series of G is defined by $P_1(G) = G$, and

$$P_{n+1}(G) = \overline{P_n(G)^p[P_n(G), G]},\ \text{for } i \geq 1.$$

By [8, Theorem 3.6], if G is powerful, then $G^{p^n} = G^{\{p^n\}} = P_{n+1}(G)$. Further, the p-power map

$$P_n(G)/P_{n+1}(G) \xrightarrow{\cdot p} P_{n+1}(G)/P_{n+2}(G)$$

is surjective for each $n \geq 1$. If the p-power maps are isomorphisms for all $n \geq 1$, we say G is *uniformly powerful* (abbrv. *uniform*). Then, $[G : P_2(G)] = [P_i(G) : P_{n+1}(G)]$ for every $n \geq 1$. Consequently, $[G : P_{n+1}(G)] = p^{nd}$, where $d = \dim G$ (see [8, Definition 4.1]). A well-known result of Lazard (cf. [8, Corollary 8.34]) asserts that a compact p-adic Lie group always contains an open normal uniform subgroup. Therefore, one can always reduce consideration for a general compact p-adic Lie group to the case of a uniform group, which we will do throughout the paper. In particular, for a uniform group, we have $G^{p^n} = G^{\{p^n\}}$, which will be utilized without further mention.

We record the following lemma which will also be applied frequently without mention.

Lemma 3.1. *Let G be a uniform group and N be a closed normal subgroup of G such that $R := G/N$ is uniform. Then N is also uniform. Furthermore, writing $N_n = N^{p^n}$, $G_n = G^{p^n}$, and $R_n = R^{p^n}$, we have $N_n = G_n \cap N$ and $G_n/N_n \cong R_n$.*

Proof. Using [8, Proposition 4.31], N is a uniform group. Clearly, one has $N_n \subseteq G_n \cap N$. Conversely, let $x \in G_n \cap N$. Then $x = y^{p^n}$ for some $y \in G$; hence the coset yN is a torsion element in $R = G/N$. Since R is assumed to be uniform, it has no p-torsion (cf. [8, Theorem 4.5]); so $yN = N$ or $y \in N$. Hence $x = y^{p^n} \in N_n$. This proves the first equality. The second follows from the observation that

$$G_n/N_n = G_n/(G_n \cap N) \cong G_nN/N = G^{p^n}N/N = (G/N)^{p^n} = R_n.$$

□

3.2. **Torsion modules and pseudo-null modules.** For a compact p-adic Lie group, G, its Iwasawa algebra is the completed group algebra of G over $\mathbb{Z}_p$. It is given by

$$\mathbb{Z}_p[\![G]\!] = \varprojlim_U \mathbb{Z}_p[G/U],$$

where U runs over the open normal subgroups of G and the inverse limit is taken with respect to the canonical projection maps.

When G is pro-p and has no p-torsion, it is well-known that $\mathbb{Z}_p[\![G]\!]$ is an Auslander regular ring (cf. [47, Theorem 3.26]; for the definition of Auslander regular rings, see [47, Definition 3.3]). Furthermore, the ring $\mathbb{Z}_p[\![G]\!]$ has no zero divisors (cf. [35]), and therefore, admits a skew field, $Q(G)$, which is flat over $\mathbb{Z}_p[\![G]\!]$ (see [9, Chapters 6 and 10] or [20, Chapter 4, §9 and §10]). If M is a finitely generated $\mathbb{Z}_p[\![G]\!]$-module, define the $\mathbb{Z}_p[\![G]\!]$-rank of M as

$$\operatorname{rank}_{\mathbb{Z}_p[\![G]\!]} M = \dim_{Q(G)} Q(G) \otimes_{\mathbb{Z}_p[\![G]\!]} M.$$

A $\mathbb{Z}_p[\![G]\!]$-module, M, is *torsion* if $\operatorname{rank}_{\mathbb{Z}_p[\![G]\!]} M = 0$. Equivalently, M is torsion if and only if $\operatorname{Hom}_{\mathbb{Z}_p[\![G]\!]}(M,\ \mathbb{Z}_p[\![G]\!]) = 0$ (cf. [24, Lemma 2.2.1]). A torsion $\mathbb{Z}_p[\![G]\!]$-module, M, is *pseudo-null* if $\operatorname{Ext}^1_{\mathbb{Z}_p[\![G]\!]}(M,\ \mathbb{Z}_p[\![G]\!]) = 0$. Finally, we record a result which will be frequently used in our discussion.

Proposition 3.2 (Harris [13])**.** *Let G be a d-dimensional uniform group. Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module. Then,*

$$\operatorname{rank}_{\mathbb{Z}_p}(M_{G_n}) = \operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M) p^{dn} + O\left(p^{(d-1)n}\right).$$

3.3. **μ_G-invariant.** In this subsection, G will denote a uniform group. Therefore, both $\mathbb{Z}_p[\![G]\!]$ and $\mathbb{F}_p[\![G]\!]$ are Auslander regular rings with no zero divisors. For a finitely generated $\mathbb{Z}_p[\![G]\!]$-module, M, it follows from [15, Proposition 1.11] (or [47, Theorem 3.40]) that there is a $\mathbb{Z}_p[\![G]\!]$-homomorphism

$$\varphi : M[p^\infty] \longrightarrow \bigoplus_{i=1}^{s} \mathbb{Z}_p[\![G]\!]/\pi^{\alpha_i},$$

whose kernel and cokernel are pseudo-null $\mathbb{Z}_p[\![G]\!]$-modules. Furthermore, the integers s and α_i are uniquely determined. We define the *μ_G-invariant*, $\mu_G(M) = \sum_{i=1}^{s} \alpha_i$.

Lemma 3.3. *Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module. Suppose there is a $\mathbb{Z}_p[\![G]\!]$-homomorphism*

$$\varphi : M[p^\infty] \longrightarrow \bigoplus_{i=1}^{s} \mathbb{Z}_p[\![G]\!]/p^{\alpha_i},$$

whose kernel and cokernel are pseudo-null $\mathbb{Z}_p[\![G]\!]$-modules. Then,

$$\mu_G(M/p^n) = n \operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M) + \sum_{i=1}^{s} \min\{n, \alpha_i\} \quad \text{for } n \geq 1.$$

In particular, M is a torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant if and only if $\mu_G(M/p) = 0$.

Proof. The first equality is [24, Lemma 2.4.1]; the equivalence assertion follows immediately. □

Proposition 3.4. *For G a d-dimensional uniform group, and M a finitely generated $\mathbb{F}_p[\![G]\!]$-module,*

$$\operatorname{ord}_p|M_{G_n}| = \mu_G(M) p^{dn} + O\left(p^{(d-1)n}\right).$$

Proof. See [37, Théorème 2.1] or [24, Proposition 2.5.1]. □

4. Local Considerations

We now estimate the growth of the first cohomology group of the p-division points of an elliptic curve in a p-adic Lie extension of a local field. For an extension $\mathcal{L}$ of a local field, and a $\mathrm{Gal}(\overline{\mathcal{L}}/\mathcal{L})$-module, M, we write $H^i(\mathcal{L},\ M)$ for the cohomology group $H^i\left(\mathrm{Gal}(\overline{\mathcal{L}}/\mathcal{L}),\ M\right)$. Throughout, K is a local field and K_∞ is a uniform p- adic Lie extension, i.e., it is a pro-p extension of K with Galois group $G = \mathrm{Gal}\left(K_\infty/K\right)$ which is assumed to be uniform. We write $G_n = G^{p^n}$.

4.1. **Local field over $\mathbb{Q}_\ell$ with $\ell \neq p$.** Let K be a finite extension of $\mathbb{Q}_\ell$, where $\ell \neq p$. By a classical result of Iwasawa (cf. [34, Theorem 7.5.3]), if K_∞/K is a uniform p-adic Lie extension, we know that $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ or $\mathbb{Z}_p \rtimes \mathbb{Z}_p$. Further, Iwasawa's result shows that the $\mathbb{Z}_p \rtimes \mathbb{Z}_p$-extension of K is unique. We now estimate the growth of the first cohomology group in both cases.

Proposition 4.1. *Let E be an elliptic curve defined over K, and K_∞/K be a uniform extension of K. Then, the group $H^1\left(G_n,\ E(K_\infty)[p^\infty]\right)$ is finite for every n. Furthermore, the following assertions are true.*

(*a*) *If* $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, *then* $\left|H^1\left(G_n,\ E(K_\infty)[p^\infty]\right)\right| = O(1)$.

(*b*) *If* $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$, *then* $\dim_{\mathbb{Z}/p\mathbb{Z}}\left(H^1\left(G_n,\ E(K_\infty)[p^\infty]\right)[p]\right) = O(1)$ *and* $\mathrm{ord}_p\left|H^1\left(G_n,\ E(K_\infty)[p^\infty]\right)\right| = O(n)$.

Proof. (*a*) This is proven in [27, Lemma 3.4].

(*b*) The first estimate follows from Lemma 2.1. For the second estimate, note that by Iwasawa's result (cf. [34, Theorem 7.5.3]), K_∞ has no non-trivial p-extension, so $H^1(K_\infty,\ E[p^\infty]) = 0$. By the inflation-restriction sequence, we obtain that

$$H^1\left(G_n,\ E(K_\infty)[p^\infty]\right) \cong H^1(K_n,\ E[p^\infty]).$$

Here K_n refers to the field fixed by G_n. Since $\ell \neq p$, the latter is isomorphic to $H^1(K_n,\ E)[p^\infty]$; this in turn is isomorphic to $\left(E(K_n)[p^\infty]\right)^\vee$ by Tate-duality (cf. [33, Chap. I, Corollary 3.4]). It is now easy to see that this is finite and $\mathrm{ord}_p\left|\left(E(K_n)[p^\infty]\right)^\vee\right| = O(n)$.

□

4.2. **Local field over $\mathbb{Q}_p$.** We now consider the situation when K is a finite extension of $\mathbb{Q}_p$, and E is an elliptic curve defined over K. We begin with the following easy observation.

Proposition 4.2. *Let K_∞ be a uniform p-adic Lie extension extension of K of dimension d. Suppose $E(K_\infty)[p^\infty]$ is finite. Then, the group $H^1(G_n,\ E(K_\infty)[p^\infty])$ is finite and*

$$\mathrm{ord}_p\left|H^1\left(G_n,\ E\left(K_\infty\right)[p^\infty]\right)\right| = O(1).$$

Proof. This follows from Lemma 2.2. □

Proposition 4.3. *Let K_∞ be a $\mathbb{Z}_p^d$-extension of K. Then $H^1\left(G_n,\ E(K_\infty)[p^\infty]\right)$ is finite and*

$$\mathrm{ord}_p\left|H^1\left(G_n,\ E(K_\infty)[p^\infty]\right)\right| = O(n).$$

Proof. Observe that $H^0\left(G_n,\ E\left(K_\infty\right)[p^\infty]\right) = E(K_n)[p^\infty]$ is finite because for any elliptic curve over a local field the torsion subgroup is finite, see [44, Proposition VII.6.3]. The finiteness of $H^1\left(G_n,\ E\left(K_\infty\right)[p^\infty]\right)$ is then now essentially a consequence of this and [42, Chap. IV., Theorem

1]. (One may also consult p. 106 in *op. cit.*, where they obtain a result for $k[G]$, where k is a field. But the same discussion carries over if k is replaced by $\mathbb{Z}_p$.) In view of this finiteness observation, we may apply Lemma 2.1 to conclude that $\dim_{\mathbb{Z}/p\mathbb{Z}} H^1\left(G_n,\ E(K_\infty)[p^\infty]\right)[p]$ is bounded independent of n. On the other hand, by [7, Theorem 2.8] (or [22, Lemma 2.1.1]) there exists a constant c independent of n such that p^{dn+c} annihilates $H^1\left(G_n,\ E(K_\infty)[p^\infty]\right)$. The assertion follows from these observations. □

Remark 4.4. *If* $\mathrm{Gal}(K_\infty/K) = \mathbb{Z}_p$, *we have the following better estimate (see [27, Lemma 3.4])*

$$\mathrm{ord}_p\left|H^1\left(G_n,\ E\left(K_\infty\right)\left[p^\infty\right]\right)\right| = O(1).$$

Let $K_\infty = K\left(\mu_{p^\infty},\ \sqrt[p^\infty]{\alpha_1}, \ldots,\ \sqrt[p^\infty]{\alpha_{d-1}}\right)$, where $\alpha_1, \ldots, \alpha_{d-1} \in K^\times$ whose image in $K^\times/(K^\times)^p$ are linearly independent over $\mathbb{F}_p$. This is a *multi-false-Tate extension of a local field*, K.

Proposition 4.5. *Let* K_∞ *be a multi-false-Tate extension of a local field of dimension* ≥ 2. *Suppose* E *is an elliptic curve defined over* K *with potential good reduction. Then, the group* $H^1\left(G_n,\ E(K_\infty)[p^\infty]\right)$ *is finite with*

$$\mathrm{ord}_p\left|H^1\left(G_n,\ E(K_\infty)[p^\infty]\right)\right| = O(1).$$

Proof. Since E has potential good reduction at K, we see that $E(K_\infty)[p^\infty]$ is finite by a result of Kubo-Taguchi [19, Theorem 1.1]. The claim follows from this observation and Proposition 4.2. □

If E has split multiplicative reduction, then $H^1\left(G_n,\ E(K_\infty)[p^\infty]\right)$ can be infinite. This is a well-known fact. However, for a lack of proper reference, we shall supply an argument here.

Proposition 4.6. *Let* E *be an elliptic curve defined over* K *with split multiplicative reduction. Suppose that* K *contains a primitive* p*-th root of unity. Let* $K_\infty = K\left(\mu_{p^\infty},\ \sqrt[p^\infty]{\alpha}\right)$ *such that* $E[p^\infty]$ *is not realized over* K_∞. *Then the group* $H^1\left(G,\ E[p^\infty]\right)$ *is infinite, where* $G = \mathrm{Gal}(K_\infty/K)$.

Proof. From the theory of Tate curves, we have a short exact sequence

$$0 \longrightarrow \mu_{p^\infty} \longrightarrow E[p^\infty] \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$$

of $\mathrm{Gal}(\overline{K}/K)$-modules. Taking $\mathrm{Gal}(\overline{K}/K_\infty)$-invariance, we obtain the exact sequence,

$$0 \longrightarrow \mu_{p^\infty} \longrightarrow E(K_\infty)[p^\infty] \xrightarrow{f} \mathbb{Q}_p/\mathbb{Z}_p.$$

Since $E[p^\infty]$ is not realized over K_∞, the $\mathbb{Z}_p$-corank of $E(K_\infty)[p^\infty]$ is at most one. The above sequence implies that the image of f, B (say), is finite. Thus, we have a short exact sequence,

$$0 \longrightarrow \mu_{p^\infty} \longrightarrow E(K_\infty)[p^\infty] \xrightarrow{f} B \longrightarrow 0$$

of G-modules. Taking G-cohomology, we obtain the following exact sequence

$$B^G \longrightarrow H^1(G,\ \mu_{p^\infty}) \longrightarrow H^1(G,\ E(K_\infty)[p^\infty]).$$

Since B is finite, the proposition will follow once we show that $H^1(G,\ \mu_{p^\infty})$ is infinite. For this, we appeal to the inflation-restriction sequence; there exists a short exact sequence

$$0 \longrightarrow H^1(\Gamma,\ \mu_{p^\infty}) \longrightarrow H^1(G,\ \mu_{p^\infty}) \longrightarrow H^1(H,\ \mu_{p^\infty})^\Gamma \longrightarrow 0,$$

where $\Gamma = \mathrm{Gal}(K^{\mathrm{cyc}}/K)$. By Kummer theory, $H \cong T_p\mu_{p^\infty}$ as Γ-modules. Thus,

$$H^1(H,\ \mu_{p^\infty})^\Gamma \cong \mathrm{Hom}(T_p\mu_{p^\infty}, \mu_{p^\infty})^\Gamma \cong (\mathbb{Q}_p/\mathbb{Z}_p)^\Gamma = \mathbb{Q}_p/\mathbb{Z}_p,$$

which is an infinite group. We have therefore established the proposition. □

In Proposition 4.8, we will see that one can still say something on the growth of the $\mathbb{Z}_p$-corank. Now consider the case of $K_\infty = K(E[p^\infty])$, i.e., the extension obtained by adjoining all the p-power division points of the elliptic curve, E. Here, we have no assumption on the reduction type of E.

Proposition 4.7. *Let E/K be an elliptic curve such that $K/\mathbb{Q}_p$ is finite, and let $K_\infty = K(E[p^\infty])$. Suppose $G = \mathrm{Gal}(K_\infty/K)$ is uniform. Writing $G_n = G^{p^n}$, the group $H^1\left(G_n,\ E[p^\infty]\right)$ is finite with p-power order $O(n)$.*

Proof. By base changing, we assume that $E[p]$ is rational over K and has semi-stable reduction at K. If E has complex multiplication, then $G \cong \mathbb{Z}_p^2$ and the conclusion follows from Proposition 4.3.

We will now consider the case of elliptic curves without complex multiplication. Suppose that E has split multiplicative reduction. By the theory of Tate curves, there exists $q \in K$ such that $E(\overline{K}) \cong \overline{K}^\times/q^{\mathbb{Z}}$ as $\mathrm{Gal}(\overline{K}/K)$-modules. Since K is assumed to contain $E[p]$, it also contains μ_p. Therefore, $K(\mu_{p^\infty})$ is a $\mathbb{Z}_p$-extension of K. Write $\mathcal{H} = \mathrm{Gal}(K_\infty/K(\mu_{p^\infty}))$ and $\Upsilon = \mathrm{Gal}(K(\mu_{p^\infty})/K)$. The theory of Tate curves tells us that K_∞ is obtained from $K(\mu_{p^\infty})$ by adjoining all the p-power roots of q. Thus, K_∞ is a false-Tate extension of K. Furthermore, there is a short exact sequence

$$0 \longrightarrow \mu_{p^\infty} \longrightarrow E[p^\infty] \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$$

of $\mathrm{Gal}(\overline{K}/K)$-modules. Taking $\mathcal{H}$-cohomology, we obtain the following exact sequence

$$0 \to \mu_{p^\infty} \to H^0(\mathcal{H}, E[p^\infty]) \to \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\delta} H^1(\mathcal{H}, \mu_{p^\infty}) \to H^1(\mathcal{H}, E[p^\infty]) \to H^1(\mathcal{H}, \mathbb{Q}_p/\mathbb{Z}_p) \to 0,$$

where the final zero comes from the fact that $\mathcal{H} \cong \mathbb{Z}_p$ has p-cohomological dimension 1. By Kummer theory, the connecting homomorphism, denoted by δ, is an isomorphism. Thus, we obtain $H^0(\mathcal{H},\ E[p^\infty]) \cong \mu_{p^\infty}$ and $H^1(\mathcal{H},\ E[p^\infty]) \cong H^1(\mathcal{H},\ \mathbb{Q}_p/\mathbb{Z}_p)$. Write $\mathcal{H}_n = \mathcal{H}^{p^n}$ and $\Upsilon_n = \Upsilon^{p^n}$; then a similar argument also yields $H^0(\mathcal{H}_n,\ E[p^\infty]) \cong \mu_{p^\infty}$ and $H^1(\mathcal{H}_n,\ E[p^\infty]) \cong H^1(\mathcal{H}_n,\ \mathbb{Q}_p/\mathbb{Z}_p)$ as Υ_n-modules. By the inflation-restriction sequence, we obtain

$$0 \longrightarrow H^1(\Upsilon_n,\ E[p^\infty]^{\mathcal{H}_n}) \longrightarrow H^1(G_n,\ E[p^\infty]) \longrightarrow H^1(\mathcal{H}_n,\ E[p^\infty])^{\Gamma_n} \longrightarrow 0.$$

Now $H^1(\Upsilon_n,\ E[p^\infty]^{\mathcal{H}_n}) \cong H^1(\Upsilon_n,\ \mu_{p^\infty})$ which vanishes by Lemma 2.3. By Kummer theory, we know that $\mathcal{H} \cong T_p\mu_{p^\infty}$ as Υ-modules. Therefore,

$$H^1(\mathcal{H}_n,\ E[p^\infty])^{\Upsilon_n} \cong H^1(\mathcal{H}_n,\ \mathbb{Q}_p/\mathbb{Z}_p)^{\Upsilon_n} \cong \mathrm{Hom}(T_p\mu_{p^\infty},\ \mathbb{Q}_p/\mathbb{Z}_p)^{\Upsilon_n};$$

the last of which is easily seen to be finite with p-power order $O(n)$. This proves the proposition when E has multiplicative reduction.

When E does not have complex multiplication and has good ordinary reduction, the dimension of G is 3 (cf. [4, Proposition 2.8]). We have a short exact sequence of G-modules

$$0 \longrightarrow \widehat{E}[p^\infty] \longrightarrow E[p^\infty] \longrightarrow \widetilde{E}[p^\infty] \longrightarrow 0, \tag{1}$$

where $\widehat{E}$ (resp. $\widetilde{E}$) denotes the formal group (resp. reduced curve) of E. Taking G_n-invariance,

$$H^1\left(G_n,\ \widehat{E}[p^\infty]\right) \longrightarrow H^1\left(G_n,\ E[p^\infty]\right) \longrightarrow H^1\left(G_n,\ \widetilde{E}[p^\infty]\right).$$

The discussion in [11, p. 274] implies that $H^1(G_n,\ \widetilde{E}[p^\infty])$ is finite with p-power order $O(n)$. It remains to estimate $H^1(G_n,\ \widehat{E}[p^\infty])$. For this, we further analyse the structure of G. The $\mathrm{Gal}(\bar{K}/K)$-action on $\widetilde{E}[p^\infty]$ induces a group homomorphism $\rho : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}(\widetilde{E}[p^\infty])$. We denote $L_\infty := \bar{K}^{\ker\rho}$ which is a $\mathbb{Z}_p$-extension of K contained in K_∞ (recall that we are assuming that $E[p]$ is realized over K). By definition, $\mathrm{Gal}(\overline{K}/K^{ur})$ acts trivially on $\widetilde{E}[p^\infty]$, where K^{ur} is

the maximal unramified extension of K. Hence, the extension L_∞ is an unramified $\mathbb{Z}_p$-extension of K contained in K_∞. Set $M_\infty = L_\infty(\mu_{p^\infty})$; this is a $\mathbb{Z}_p$-extension of L_∞. We claim that $\widehat{E}[p^\infty]$ is not rational over M_∞. Indeed, since $\widetilde{E}[p^\infty]$ is realized over L_∞, it is also realized over M_∞. If $\widehat{E}[p^\infty]$ is also rational over K_∞, then $E[p^\infty]$ must be rational over M_∞ which in turn implies that $K_\infty = M_\infty$. This contradicts the fact that $G = \mathrm{Gal}(K_\infty/K)$ has dimension 3. By dimension counting, $\mathrm{Gal}(K_\infty/M_\infty)$ is a one-dimensional p-adic Lie group. By enlarging K, we may assume that $\mathrm{Gal}(K_\infty/M_\infty) \cong \mathbb{Z}_p$. For $n \gg 0$, there exists a constant c independent of n such that

$$\mathrm{Gal}\left(K_\infty/M_\infty\right)^{p^n} = \mathrm{Gal}\left(K_\infty \Big/ M_\infty\left(\widehat{E}[p^{n+c}]\right)\right).$$

Now, write $U_n = \mathrm{Gal}(K_\infty/M_\infty)^{p^n}$ and $V_n = \mathrm{Gal}(M_\infty/K)^{p^n}$. For large enough n, the inflation-restriction sequence gives us the following exact sequence

$$0 \longrightarrow H^1\left(V_n,\ \widehat{E}[p^{n+c}]\right) \longrightarrow H^1\left(G_n,\ \widehat{E}[p^\infty]\right) \longrightarrow H^1\left(U_n,\ \widehat{E}[p^\infty]\right)^{V_n}.$$

Since $H^0(U_n,\ \widehat{E}[p^\infty]) = \widehat{E}[p^{n+c}]$ is finite, it follows from an application of Lemma 2.3 that $H^1(U_n,\ \widehat{E}[p^\infty]) = 0$. Now, by appealing to Lemma 2.2, we obtain the required equality,

$$\mathrm{ord}_p\left|H^1\left(G_n,\ \widehat{E}[p^\infty]\right)\right| = \mathrm{ord}_p\left|H^1\left(V_n,\ \widehat{E}[p^{n+c}]\right)\right| \leq 2(n+c) = O(n).$$

We now come to the situation when E does not have complex multiplication and has good supersingular reduction. Under this assumption, the dimension of G is 4 (cf. [41, IV A.2.2]). In particular, it is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. By the discussion in [47, p. 302], and upon enlarging K if necessary, we may assume that $G = Z \times H$, where $Z \cong \mathbb{Z}_p$ and $H = \mathrm{Gal}(K_\infty/K^{\mathrm{cyc}})$. We claim that $E[p^\infty]^{Z_n}$ is finite, where $Z_n = Z^{p^n}$. Suppose for now that the claim holds. Then, by Lemma 2.3, we have $H^1(Z_n,\ E[p^\infty]) = 0$. Therefore, the spectral sequence

$$H^i(H_n,\ H^j(Z_n,\ E[p^\infty])) \Longrightarrow H^{i+j}(G_n,\ E[p^\infty])$$

degenerates to yield

$$H^i\left(H_n,\ E[p^\infty]^{Z_n}\right) \cong H^i\left(G_n,\ E[p^\infty]\right).$$

Writing $L_\infty = K_\infty^Z$, we see that for sufficiently large n, $Z^{p^n} = \mathrm{Gal}\left(K_\infty/L_\infty\left(E[p^{n+c}]\right)\right)$ where c is a constant independent of n. By Lemma 2.1, we see that

$$\mathrm{ord}_p\left|H^1\left(G_n,\ E[p^\infty]\right)\right| = \mathrm{ord}_p\left|H^1\left(H_n,\ E[p^\infty]^{Z_n}\right)\right| \leq 3\,\mathrm{ord}_p\left|E[p^\infty]^{Z_n}\right| = O(n).$$

It therefore remains to verify that $E[p^\infty]^{Z_n}$ is finite. Without loss of generality, it suffices to show that $E[p^\infty]^Z$ is finite. Let T be the Tate module of $E[p^\infty]^Z$. Then $T \otimes \mathbb{Q}_p$ is a $\mathrm{Gal}(\overline{K}/K)$-submodule of $T_pE \otimes \mathbb{Q}_p$. Since E is an elliptic curve without complex multiplication, the latter is an irreducible $\mathrm{Gal}(\overline{K}/K)$-module by [41, IV 2.1]. So, $T \otimes \mathbb{Q}_p$ is either zero or the whole of $T_pE \otimes \mathbb{Q}_p$. As $E[p^\infty]$ is not realized over L_∞, we have $T \otimes \mathbb{Q}_p = 0$; equivalently, $E[p^\infty]^Z$ is finite. □

Finally, we record an estimate on the $\mathbb{Z}_p$-coranks of the first cohomology groups in intermediate extensions of a general p-adic Lie extension. This result is independent of the reduction type of E.

Proposition 4.8. *Let K_∞ be a d-dimensional uniform p-adic Lie extension of K. Then,*

$$\dim_{\mathbb{Z}/p\mathbb{Z}}\left(H^1\left(G_n,\ E\left(K_\infty\right)[p^\infty]\right)[p]\right) = O(1).$$

In particular,

$$\operatorname{corank}_{\mathbb{Z}_p}\left(H^1\left(G_n,\ E\left(K_\infty\right)[p^\infty]\right)\right) = O(1).$$

Proof. This follows from Lemma 2.1 and noting that $h_1(G_n) = d$ for all n. □

5. A General Control Theorem

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Any algebraic (possibly infinite) extension of $\mathbb{Q}$ is then a subfield of this fixed algebraic closure, $\overline{\mathbb{Q}}$. When the subfield is a finite extension of $\mathbb{Q}$, we call it a number field. Let E be an elliptic curve defined over a number field, F, and let S be a finite set of primes containing the primes above p, the primes of bad reduction of E, and the Archimedean primes. Let F_S be the maximal algebraic extension of F unramified outside S. For every (possibly infinite) extension L of F contained in F_S, write $G_S(L) = \operatorname{Gal}(F_S/L)$. Let $S(L)$ be the set of primes of L above S. If L is a finite extension of F and w is a place of L, we write L_w for its completion at w; when L/F is infinite, it is the union of completions of all finite sub-extensions of L.

Over each L, the *p-primary Selmer group* and *p-primary fine Selmer group* are defined as follows

$$0 \longrightarrow \quad \operatorname{Sel}\left(E/L\right) \longrightarrow \quad H^1\left(G_S(L),\ E[p^\infty]\right) \longrightarrow \quad \bigoplus_{w\in S(L)} H^1\left(L_w,\ E\right)[p^\infty],$$

$$0 \longrightarrow \quad R\left(E/L\right) \longrightarrow \quad H^1\left(G_S\left(L\right),\ E[p^\infty]\right) \longrightarrow \quad \bigoplus_{w\in S(L)} H^1\left(L_w,\ E[p^\infty]\right).$$

Using the definition, it is a simple observation that $R(E/L)$ is independent of the choice of S [30, Lemma 4.1]. Indeed, this is because we have the following exact sequence

$$0 \longrightarrow R\left(E/L\right) \longrightarrow \operatorname{Sel}\left(E/L\right) \longrightarrow \bigoplus_{w|p} E(L_w)\otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

A uniform p-adic Lie extension F_∞ of F is one where $\operatorname{Gal}(F_\infty/F)$ is a uniform group. For a given uniform p-adic Lie extension F_∞ contained in F_S, define $R(E/F_\infty) = \varinjlim_L R(E/L)$, where L runs through the finite sub-extensions of F_∞/F. In other words, we have

$$R\left(E/F_\infty\right) \cong \ker\left(H^1\left(G_S\left(F_\infty\right), E[p^\infty]\right) \longrightarrow \bigoplus_{v\in S} K_v^1\left(E/F_\infty\right)\right),$$

where $K_v^1\left(E/F_\infty\right) = \varinjlim_L \bigoplus_{w\in S(L)} H^1\left(L_w,\ E[p^\infty]\right)$. For a finite extension, L/F, we shall sometimes write $K_v^1(E/L) = \bigoplus_{w|v} H^1\left(L_w,\ E[p^\infty]\right)$.

For a finite extension L of F contained in F_∞, we have the following commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & R(E/L) & \longrightarrow & H^1\left(G_S\left(L\right),\ E[p^\infty]\right) & \longrightarrow & \bigoplus_{v\in S} K_v^1(E/L) \\
 & & \downarrow r_L & & \downarrow h_L & & \downarrow g_L \\
0 & \longrightarrow & R\left(E/F_\infty\right)^{\operatorname{Gal}(F_\infty/L)} & \longrightarrow & H^1\left(G_S\left(F_\infty\right),\ E[p^\infty]\right)^{\operatorname{Gal}(F_\infty/L)} & \longrightarrow & \bigoplus_{v\in S} K_v^1\left(E/F_\infty\right)^{\operatorname{Gal}(F_\infty/L)}
\end{array}$$

with exact rows, where the maps h_L and g_L are the restriction maps on cohomology, and r_L is the map induced by these. The above diagram will be the main tool for our discussion. We first prove a general result independent of any hypothesis on the reduction type.

For the remainder of the section, the elliptic curve E will be defined over the number field, F, and F_∞ will be a uniform p-adic Lie extension over F contained in F_S with Galois group, $G = \mathrm{Gal}(F_\infty/F)$. We will write $G_n = G^{p^n}$ and denote by F_n the fixed field of G_n.

Theorem 5.1. *Let E be an elliptic curve defined over F, and let F_∞ be a d-dimensional uniform p-adic Lie extension of F. Then the kernel and cokernel of the restriction map*

$$r_n : R\left(E/F_n\right) \to R\left(E/F_\infty\right)^{G_n}$$

are cofinitely generated over $\mathbb{Z}_p$. Furthermore,

$$\mathrm{corank}_{\mathbb{Z}_p}\left(\ker r_n\right) = O(1) \quad \textit{and} \quad \mathrm{corank}_{\mathbb{Z}_p}\left(\mathrm{coker}\, r_n\right) = O\left(p^{(d-1)n}\right).$$

Proof. Consider the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & R(E/F_n) & \longrightarrow & H^1\left(G_S\left(F_n\right),\ E[p^\infty]\right) & \longrightarrow & \bigoplus_{v_n \in S(F_n)} H^1\left(F_{n,v_n},\ E[p^\infty]\right) \\ & & \downarrow r_n & & \downarrow h_n & & \downarrow g_n \\ 0 & \longrightarrow & R\left(E/F_\infty\right)^{G_n} & \longrightarrow & H^1\left(G_S\left(F_\infty\right),\ E[p^\infty]\right)^{G_n} & \longrightarrow & \bigoplus_{v \in S} K_v^1\left(E/F_\infty\right)^{G_n} \end{array}$$

with exact rows. By the Hochschild-Serre spectral sequence, we have

$$\ker h_n = H^1\left(G_n,\ E(F_\infty)[p^\infty]\right) \quad \text{and} \quad \mathrm{coker}\, h_n \subseteq H^2\left(G_n,\ E(F_\infty)[p^\infty]\right).$$

By Lemma 2.1, we see that $\dim_{\mathbb{Z}/p\mathbb{Z}}\left((\ker h_n)[p]\right) = O(1)$ and $\dim_{\mathbb{Z}/p\mathbb{Z}}\left((\mathrm{coker}\, h_n)[p]\right) = O(1)$. In particular, $\mathrm{corank}_{\mathbb{Z}_p}\left(\ker h_n\right)$ (and hence $\mathrm{corank}_{\mathbb{Z}_p}\left(\ker r_n\right)$) is finite and bounded independent of n.

For the estimate of $\mathrm{coker}\, r_n$, we now study the growth of $\mathrm{corank}_{\mathbb{Z}_p}\left(\ker g_n\right)$. By Shapiro's Lemma,

$$\ker g_n = \bigoplus_{v_n \in S(F_n)} H^1\left(G_{n,v_n},\ E(F_{\infty,v_n})[p^\infty]\right).$$

If v is a prime which splits completely in F_∞/F, then $H^1\left(G_{n,v_n},\ E(F_{\infty,v_n})[p^\infty]\right) = 0$ for every v_n above v. Thus, we consider primes which do not split completely in F_∞/F. By Proposition 4.1, for $v \nmid p$, the group $H^1\left(G_{n,v_n},\ E(F_{\infty,v_n})[p^\infty]\right)$ is finite and has no $\mathbb{Z}_p$-corank contribution. We are reduced to studying $v|p$ which do not split completely in F_∞/F. In this case, the dimension of the decomposition group of G at v is at least 1, so the number of primes of F_n above each v is $O\left(p^{(d-1)n}\right)$. By Proposition 4.8, each $H^1\left(G_{n,v_n},\ E(F_{\infty,v_n})[p^\infty]\right)$ has bounded $\mathbb{Z}_p$-corank growth. It follows that $\mathrm{corank}_{\mathbb{Z}_p}\left(\ker g_n\right) = O\left(p^{(d-1)n}\right)$. This completes the proof of the theorem. □

Corollary 5.2. *Retain the setting of Theorem 5.1. Then,*

$$\left|\mathrm{corank}_{\mathbb{Z}_p}\left(R(E/F_n)\right) - \mathrm{corank}_{\mathbb{Z}_p}\left(R(E/F_\infty)^{G_n}\right)\right| = O\left(p^{(d-1)n}\right).$$

In particular, $R(E/F_\infty)$ is cotorsion over $\mathbb{Z}_p[\![G]\!]$ if and only if $\mathrm{corank}_{\mathbb{Z}_p}\left(R(E/F_n)\right) = O\left(p^{(d-1)n}\right)$.

Proof. The first assertion follows from Theorem 5.1. By Harris' result (see Proposition 3.2),

$$\mathrm{corank}_{\mathbb{Z}_p}\left(R(E/F_\infty)^{G_n}\right) = \mathrm{corank}_{\mathbb{Z}_p[\![G]\!]}\left(R(E/F_\infty)\right)p^{dn} + O\left(p^{(d-1)n}\right).$$

The final assertion is now immediate from this and the above estimate. □

We now consider an analogue of Theorem 5.1 for the p-rank.

Theorem 5.3. *Retain the setting of Theorem 5.1. Then,*

$$\left|\dim_{\mathbb{Z}/p\mathbb{Z}}\left(R(E/F_n)[p]\right) - \dim_{\mathbb{Z}/p\mathbb{Z}}\left(R(E/F_\infty)^{G_n}[p]\right)\right| = O\left(p^{(d-1)n}\right).$$

In particular, the Pontryagin dual of $R(E/F_\infty)$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant if and only if $\dim_{\mathbb{Z}/p\mathbb{Z}}\left(R(E/F_n)[p]\right) = O\left(p^{(d-1)n}\right)$.

Proof. The proof of this estimate is similar to (and easier than) that of Theorem 5.1. Thus,

$$\dim_{\mathbb{Z}/p\mathbb{Z}}\left(R(E/F_n)[p]\right) = O\left(p^{(d-1)n}\right) \Leftrightarrow \dim_{\mathbb{Z}/p\mathbb{Z}}\left(R(E/F_\infty)^{G_n}[p]\right) = O\left(p^{(d-1)n}\right).$$

By Pontryagin duality, the latter is equivalent to $\dim_{\mathbb{Z}/p\mathbb{Z}}\left(\left(R(E/F_\infty)^\vee/p\right)_{G_n}\right) = O\left(p^{(d-1)n}\right)$. In view of Proposition 3.4, this is the same as $\mu_G\left(R(E/F_\infty)^\vee/p\right) = 0$. Equivalently (see Lemma 3.3), $R(E/F_\infty)^\vee$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant. □

When $G = \mathbb{Z}_p$, the conclusion of the theorem was mentioned in [30, Proof of Theorem 5.5]. Thus, Theorem 5.3 is a generalization of the discussion there. This theorem is related to a conjecture of Coates-Sujatha (see [6]) which we now describe.

Conjecture (Conjecture A)**.** *Let F^{cyc} denote the cyclotomic $\mathbb{Z}_p$-extension of F. The fine Selmer group $R(E/F^{\mathrm{cyc}})$ is cofinitely generated over $\mathbb{Z}_p$, i.e., $R(E/F^{\mathrm{cyc}})^\vee$ is a torsion $\mathbb{Z}_p[\![\Gamma]\!]$-module with trivial μ_Γ-invariant, where $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$.*

By Theorem 5.3, Conjecture A holds if and only if $\dim_{\mathbb{Z}/p\mathbb{Z}}\left(R(E/F_n)[p]\right) = O(1)$ (see [30, discussion in the proof of Theorem 5.5]). For a general p-adic Lie extension, the following result holds.

Corollary 5.4. *Let E be an elliptic curve defined over F, and let F_∞ be a d-dimensional uniform p-adic Lie extension of F contained in F_S. Suppose that F_∞ contains F^{cyc}. If Conjecture A of Coates-Sujatha holds, then* $\dim_{\mathbb{Z}/p\mathbb{Z}}\left(R(E/F_n)[p]\right) = O\left(p^{(d-1)n}\right)$.

Proof. If Conjecture A holds, $R(E/F^{\mathrm{cyc}})^\vee$ is finitely generated over $\mathbb{Z}_p$. By [6, Lemma 3.2], this implies $R(E/F_\infty)^\vee$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$ where $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. Applying an observation of Howson [14, Lemma 2.7], we see that $R(E/F_\infty)^\vee$ is torsion over $\mathbb{Z}_p[\![G]\!]$ with trivial μ_G-invariant. The result follows from combining these observations with Theorem 5.3. □

Next, we prove an H-analogue of Theorem 5.1.

Theorem 5.5. *Let E be an elliptic curve defined over F. Let F_∞ be a uniform p-adic Lie extension of F contained in F_S with Galois group, $G = \mathrm{Gal}(F_\infty/F)$ of dimension $d \geq 2$. Suppose that F_∞ contains F^{cyc}. Write $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$ and let $\mathcal{F}_n$ be the fixed field of $H_n := H^{p^n}$. Then the kernel and cokernel of the restriction map*

$$s_n : R\left(E/\mathcal{F}_n\right) \longrightarrow R\left(E/F_\infty\right)^{H_n}$$

are cofinitely generated over $\mathbb{Z}_p$. Furthermore,

$$\mathrm{corank}_{\mathbb{Z}_p}\left(\ker s_n\right) = O(1) \quad \textit{and} \quad \mathrm{corank}_{\mathbb{Z}_p}\left(\mathrm{coker}\, s_n\right) = O\left(p^{(d-2)n}\right).$$

Proof. Consider the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & R(E/\mathcal{F}_n) & \longrightarrow & H^1\left(G_S\left(\mathcal{F}_n\right),\, E[p^\infty]\right) & \longrightarrow & \bigoplus_{v\in S} K_v^1\left(E/\mathcal{F}_n\right) \\ & & \downarrow s_n & & \downarrow \beta_n & & \downarrow \gamma_n \\ 0 & \longrightarrow & R\left(E/F_\infty\right)^{H_n} & \longrightarrow & H^1\left(G_S\left(F_\infty\right),\, E[p^\infty]\right)^{H_n} & \longrightarrow & \bigoplus_{v\in S} K_v^1\left(E/F_\infty\right)^{H_n} \end{array}$$

with exact rows. The kernels and cokernels of the vertical maps are cofinitely generated over $\mathbb{Z}_p$ (see [6, Proof of Lemma 3.2]). By an argument similar to Theorem 5.1, both $\operatorname{corank}_{\mathbb{Z}_p}(\ker\beta_n)$ and $\operatorname{corank}_{\mathbb{Z}_p}(\operatorname{coker}\beta_n)$ are bounded independent of n, and $\operatorname{corank}_{\mathbb{Z}_p}(\ker\gamma_n) = O\left(p^{(d-2)n}\right)$. □

Remark 5.6. *In some special cases more can be said:*

1. *When $E(F_\infty)[p^\infty]$ is finite, both $\ker\beta_n$ and $\operatorname{coker}\beta_n$ are finite and bounded independent of n. In particular, $|\ker s_n| = O(1)$. Indeed, by applying the inflation-restriction sequence $\ker\beta_n = H^1\left(H_n,\, E(F_\infty)[p^\infty]\right)$ and $\operatorname{coker}\beta_n \subseteq H^2\left(H_n,\, E(F_\infty)[p^\infty]\right)$. Since $E(F_\infty)[p^\infty]$ is finite, it follows that $\ker\beta_n$ and $\operatorname{coker}\beta_n$ are finite. Upon noting that $h_1(H_n) = d-1$ for all n, it follows from Lemma 2.2 that the bound is independent of n.*
2. *When $F_\infty = F(E[p^\infty])$, both $\ker\beta_n$ and $\operatorname{coker}\beta_n$ are finite [5, Corollary 6]. Thus, $\ker s_n$ is finite. In fact, $\dim_{\mathbb{Z}/p\mathbb{Z}}(\ker s_n)[p] = O(1)$, but we are unable to estimate $\operatorname{ord}_p|\ker s_n|$.*
3. *If F_∞/F is a p-adic Lie extension such that the primes in S are finitely decomposed, then $\ker\gamma_n$ has finite $\mathbb{Z}_p$-corank bounded independent of n.*

Before continuing any further, we recall another conjecture of Coates-Sujatha [6, Conjecture B].

Conjecture (Conjecture B)**.** *Let F_∞ be a p-adic Lie extension of F containing F^{cyc}, which is unramified outside a finite set of primes, and whose Galois group $G = \operatorname{Gal}(F_\infty/F)$ has dimension ≥ 2. Then $R(E/F_\infty)^\vee$ is a pseudo-null $\mathbb{Z}_p[\![G]\!]$-module.*

This conjecture is very much open. Some examples verifying Conjecture B are given in [3, 17, 23, 25, 36, 43]. As a corollary of Theorem 5.5, we show that Conjecture B can be characterized in terms of the growth of the fine Selmer groups in the intermediate cyclotomic extensions.

Corollary 5.7. *Retain the setting of Theorem 5.5. Suppose that $R(E/F^{\mathrm{cyc}})$ is a cofinitely generated $\mathbb{Z}_p$-module. Then every $R(E/\mathcal{F}_n)$ is cofinitely generated over $\mathbb{Z}_p$ and $R(E/F_\infty)$ is cofinitely generated over $\mathbb{Z}_p[\![H]\!]$. Furthermore,*

$$\left|\operatorname{corank}_{\mathbb{Z}_p}\left(R(E/\mathcal{F}_n)\right) - \operatorname{corank}_{\mathbb{Z}_p}\left(R(E/F_\infty)^{H_n}\right)\right| = O\left(p^{(d-2)n}\right).$$

In particular, $R(E/F_\infty)^\vee$ is pseudo-null over $\mathbb{Z}_p[\![G]\!]$ if and only if $\operatorname{corank}_{\mathbb{Z}_p}\left(R(E/\mathcal{F}_n)\right) = O\left(p^{(d-2)n}\right)$.

Proof. Since $R(E/F^{\mathrm{cyc}})$ is a cofinitely generated $\mathbb{Z}_p$-module, we may apply [6, Lemma 3.2] to conclude that $R(E/F_\infty)$ is cofinitely generated over $\mathbb{Z}_p[\![H]\!]$. Once again applying [6, Lemma 3.2] yields that every $R(E/\mathcal{F}_n)$ is also cofinitely generated over $\mathbb{Z}_p$. This establishes the first assertion. The second assertion on the estimate is an immediate consequence of Theorem 5.5. For the final assertion, we remind the readers of an equivalent definition of pseudo-nullity (due to Venjakob) when $R(E/F_\infty)$ is cofinitely generated over $\mathbb{Z}_p[\![H]\!]$. By [48, Example 2.3 and Proposition 5.4], we know that $R(E/F_\infty)^\vee$ is pseudo-null over $\mathbb{Z}_p[\![G]\!]$ if and only if $R(E/F_\infty)$ is cotorsion over $\mathbb{Z}_p[\![H]\!]$. By the result of Harris (cf. Proposition 3.2),

$$\operatorname{corank}_{\mathbb{Z}_p}\left(R(E/F_\infty)^{H_n}\right) = \operatorname{corank}_{\mathbb{Z}_p[\![H]\!]}\left(R(E/F_\infty)\right)p^{(d-1)n} + O\left(p^{(d-2)n}\right).$$

The final assertion now follows from combining these observations with the estimate of the corollary. □

6. Control Theorem over Certain p-adic Lie Extensions

In this section, we consider specific p-adic Lie extensions and prove sharper Control Theorems for these extensions. These results are then applied to give asymptotic estimates on the growth of non-divisible part of fine Selmer groups in the intermediate subfield of the p-adic Lie extension.

Throughout this section, F is a number field and F_∞ is a uniform p-adic Lie extension of F with Galois group, G. We write $G_n = G^{p^n}$ and denote by F_n the fixed field of G_n. As a start, we record a finiteness result which will be useful for our discussion.

Lemma 6.1. *Let E be an elliptic curve defined over F, and F_∞ be a p-adic Lie extension of F at which $E[p^\infty]$ is not realized over F_∞. Suppose that at least one of the following statements is valid.*

(a) The elliptic curve, E, has no complex multiplication.
(b) The p-adic Lie extension, F_∞, contains the cyclotomic $\mathbb{Z}_p$-extension F^{cyc}.

Then $E(F_\infty)[p^\infty]$ is finite.

Proof. If statement (a) holds, the conclusion follows from [28, Lemma 6.2]. When statement (b) is valid, the conclusion follows from [52, Proposition 10]. □

6.1. **$\mathbb{Z}_p^d$-extensions.** When $d = 1$, the Control Theorem for fine Selmer groups has been studied in [27, 49]. Therefore, we concentrate on the case $d \geq 2$. Pertaining to this, Rubin proved that the kernel and cokernel of the natural restriction map are finite (see [39, Chapter VII, §3]). Here, we refine this result by giving an estimate on the orders of the kernels and cokernels.

Theorem 6.2. *Let E be an elliptic curve defined over F, and F_∞ be a $\mathbb{Z}_p^d$-extension of F, with $d \geq 2$. Then the kernel and cokernel of the restriction map*

$$r_n : R\left(E/F_n\right) \longrightarrow R\left(E/F_\infty\right)^{G_n}$$

are finite. Furthermore,

$$\mathrm{ord}_p|\ker r_n| = O(n) \quad \textit{and} \quad \mathrm{ord}_p|\mathrm{coker}\, r_n| = O\left(p^{(d-1)n}\right).$$

Proof. Consider the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & R(E/F_n) & \longrightarrow & H^1\left(G_S\left(F_n\right),\ E[p^\infty]\right) & \longrightarrow & \bigoplus_{v_n \in S(F_n)} H^1\left(F_{n,v_n},\ E[p^\infty]\right) \\ & & \downarrow r_n & & \downarrow h_n & & \downarrow g_n \\ 0 & \longrightarrow & R\left(E/F_\infty\right)^{G_n} & \longrightarrow & H^1\left(G_S\left(F_\infty\right),\ E[p^\infty]\right)^{G_n} & \longrightarrow & \bigoplus_{v \in S} K_v^1\left(E/F_\infty\right)^{G_n} \end{array}$$

with exact rows. By the Hochschild-Serre spectral sequence, we have

$$\ker h_n = H^1(G_n,\ E(F_\infty)[p^\infty]) \quad \text{and} \quad \mathrm{coker}\, h_n \subseteq H^2(G_n,\ E(F_\infty)[p^\infty]).$$

By using an argument similar to that in Proposition 4.3, we see that both $H^1(G_n,\ E(F_\infty)[p^\infty])$ and $H^2(G_n,\ E(F_\infty)[p^\infty])$ are finite with p-power order $O(n)$. In particular, $\mathrm{ord}_p|\ker r_n| = O(n)$. It remains to estimate $\ker g_n = \bigoplus_{v_n} H^1\left(G_{n,v_n},\ E(F_{\infty,v_n})[p^\infty]\right)$. As in the proof of Theorem 5.1, we only need to consider the primes which do not split completely. Now, if the decomposition group of G at the prime v is at least 2, it follows from Proposition 4.3 that $H^1\left(G_{n,v_n},\ E(F_{\infty,v_n})[p^\infty]\right)$

is finite with p-power order $O(n)$. Since the decomposition group has dimension at least 2, the number of primes above such v grows like $O\left(p^{(d-2)n}\right)$. Hence for such a prime v, we have

$$\operatorname{ord}_p\left|\bigoplus_{v_n|v} H^1\left(G_{n,v_n},\ E\left(F_{\infty,v_n}\right)[p^\infty]\right)\right| = O\left(np^{(d-2)n}\right).$$

If the decomposition group at v has dimension 1, then the number of primes above such a v grows like $O\left(p^{(d-1)n}\right)$. But for these primes, we know that $H^1\left(G_{n,v_n},\ E(F_{\infty,v_n})[p^\infty]\right)$ is finite and the growth is bounded. This is Proposition 4.1(a) when $v \nmid p$ and Remark 4.4 when $v|p$. Hence,

$$\operatorname{ord}_p\left|\bigoplus_{v_n|v} H^1\left(G_{n,v_n},\ E\left(F_{\infty,v_n}\right)[p^\infty]\right)\right| = O\left(p^{(d-1)n}\right).$$

Combining these estimates, we obtain the required estimate for $\ker g_n$ and hence for $\operatorname{coker} r_n$. □

Using a results of Liang and Lim we estimate the growth of $R(E/F_n)^\vee[p^\infty]$.

Corollary 6.3. *Let E/F be an elliptic curve, and F_∞ be a $\mathbb{Z}_p^d$-extension of F, with $d \geq 2$. Then*

$$\operatorname{ord}_p\left(R\left(E/F_n\right)^\vee[p^\infty]\right) = \mu_G\left(R\left(E/F_\infty\right)^\vee\right)p^{dn} + O\left(np^{(d-1)n}\right).$$

If F_∞ contains F^{cyc} and Conjecture A of Coates-Sujatha holds, then

$$\operatorname{ord}_p\left(R\left(E/F_n\right)^\vee[p^\infty]\right) = O\left(np^{(d-1)n}\right).$$

Finally, if F contains F^{cyc} and Conjecture B of Coates-Sujatha is also valid, then

$$\operatorname{ord}_p\left(R\left(E/F_n\right)^\vee[p^\infty]\right) = O\left(p^{(d-1)n}\right).$$

Proof. Since $R\left(E/F_\infty\right)^\vee$ is a finitely generated $\mathbb{Z}_p[\![G]\!]$-module, by a result of Liang-Lim (cf [22, Theorem 2.4.1]) we know that

$$\operatorname{ord}_p\left(\left(R\left(E/F_\infty\right)^\vee\right)_{G_n}[p^\infty]\right) = \mu_G\left(R\left(E/F_\infty\right)^\vee\right)p^{dn} + O\left(np^{(d-1)n}\right).$$

The estimate in the corollary is now immediate from this and Theorem 6.2. For the second assertion, it can be seen from the proof of Corollary 5.4 that if Conjecture A holds, then

$$\mu_G\left(R\left(E/F_\infty\right)^\vee\right) = 0.$$

If both Conjecture A and Conjecture B are valid, we may apply [22, Proposition 2.2.1] to obtain

$$\operatorname{ord}_p\left(\left(R\left(E/F_\infty\right)^\vee\right)_{G_n}[p^\infty]\right) = O\left(p^{(d-1)n}\right).$$

Combining this with Theorem 6.2, we obtain the required estimate. □

We mention another corollary of Theorem 6.2.

Corollary 6.4. *Retain the settings of Theorem 6.2. Suppose that $R(E/F)$ is finite. Then $R(E/F_\infty)^\vee$ is torsion over $\mathbb{Z}_p[\![G]\!]$.*

Proof. By Theorem 6.2 and hypothesis of the corollary, $R(E/F_\infty)^G$ is finite. The conclusion of the corollary now follows from this and the main theorem of [2, pp. 5-6]. □

In view of the above result, we make the following conjecture.

Conjecture (Conjecture Y_d)**.** *Let E be an elliptic curve defined over F, and F_∞ be a $\mathbb{Z}_p^d$-extension of F. Then, $R(E/F_\infty)^\vee$ is torsion over $\mathbb{Z}_p[\![G]\!]$.*

When $d = 1$, the above conjecture is made in [27, Conjecture Y].

6.2. **Multi-False-Tate extensions.** In this subsection, we suppose that the number field, F, contains a primitive p-th root of unity. For $d \geq 2$, consider $F_\infty = F\left(\mu_{p^\infty},\ \sqrt[p^\infty]{\alpha_1}, \ldots,\ \sqrt[p^\infty]{\alpha_{d-1}}\right)$, where $\alpha_1, \ldots, \alpha_{d-1} \in F^\times$ whose image in $F^\times/(F^\times)^p$ are linearly independent over $\mathbb{F}_p$. Then $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p^{d-1} \rtimes \mathbb{Z}_p$ and we call F_∞/F a *multi-false-Tate curve extension of dimension d*. Throughout this subsection, we assume that E has (potential) good reduction at primes above p.

Theorem 6.5. *Let E be an elliptic curve defined over a number field F with potential good reduction at every prime of F above p. Let F_∞/F be a multi-false-Tate curve extension of dimension $d \geq 2$ which is contained in F_S. Then the kernel and cokernel of the natural restriction map*

$$r_n : R\left(E/F_n\right) \longrightarrow R\left(E/F_\infty\right)^{G_n}$$

are finite with $\left|\ker(r_n)\right| = O(1)$ and $\mathrm{ord}_p\left|\mathrm{coker}(r_n)\right| = O\left(p^{(d-1)n}\right)$. If the dimension of the decomposition group of G at every $v \in S$ is at least 2, then $\mathrm{ord}_p\left|\mathrm{coker}(r_n)\right| = O\left(np^{(d-2)n}\right)$.

Proof. As before, we start by considering the following commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & R(E/F_n) & \longrightarrow & H^1\left(G_S\left(F_n\right),\ E[p^\infty]\right) & \longrightarrow & \bigoplus_{v_n \in S(F_n)} H^1\left(F_{n,v_n},\ E[p^\infty]\right) \\ & & \downarrow r_n & & \downarrow h_n & & \downarrow g_n \\ 0 & \longrightarrow & R\left(E/F_\infty\right)^{G_n} & \longrightarrow & H^1\left(G_S\left(F_\infty\right),\ E[p^\infty]\right)^{G_n} & \longrightarrow & \bigoplus_{v \in S} K_v^1\left(E/F_\infty\right)^{G_n} \end{array}$$

By Lemma 6.1, $E\left(F_\infty\right)[p^\infty]$ is finite. Now by applying the inflation-restriction sequence and using Lemma 2.2, we see that $\ker(h_n)$ and $\mathrm{coker}(h_n)$ are finite and bounded independent of n.

We will now estimate $\ker g_n$. For the primes not above p, using Proposition 4.1 we conclude that

$$\mathrm{ord}_p\left|\bigoplus_{v_n|v} H^1\left(G_{n,v_n},\ E\left(F_{\infty,v_n}\right)[p^\infty]\right)\right| = \begin{cases} O\left(p^{(d-1)n}\right), & \text{if the decomposition group at } v \text{ has dimension 1,} \\ O\left(np^{(d-2)n}\right), & \text{if the decomposition group at } v \text{ has dimension 2.} \end{cases}$$

Since we assume that the elliptic curve E has potential good reduction at all primes above p, it follows from Proposition 4.5 that $H^1\left(G_{n,v_n},\ E\left(F_{\infty,v_n}\right)[p^\infty]\right)$ is finite with bounded growth. Thus,

$$\mathrm{ord}_p\left|\bigoplus_{v_n|v} H^1\left(G_{n,v_n},\ E\left(F_{\infty,v_n}\right)[p^\infty]\right)\right| = \begin{cases} O\left(p^{(d-1)n}\right), & \text{if the decomposition group at } v \text{ has dimension 1,} \\ O\left(p^{(d-2)n}\right), & \text{if the decomposition group at } v \text{ has dimension} \geq 2. \end{cases}$$

The assertions of the theorem are now immediate from these estimates. □

Using a result of Perbet (see [37, Théorème 2.1]) we estimate the growth of $R(E/F_n)[p^n]$.

Corollary 6.6. *Let E be an elliptic curve defined over a number field F with potential good reduction at every prime of F above p. Let F_∞/F be a multi-false-Tate curve extension of dimension $d \geq 2$ which is contained in F_S. Then*

$$\mathrm{ord}_p\left(R\left(E/F_n\right)[p^n]\right) = \left(\mathrm{rank}_{\mathbb{Z}_p[\![G]\!]}\left(R\left(E/F_\infty\right)^\vee\right)n + \mu_G\left(R\left(E/F_\infty\right)^\vee\right)\right)p^{dn} + O\left(np^{(d-1)n}\right).$$

If the Conjecture A of Coates-Sujatha holds, then

$$\mathrm{ord}_p\left(R\left(E/F_n\right)[p^n]\right) = O\left(np^{(d-1)n}\right).$$

Proof. Since $R\left(E/F_\infty\right)^\vee$ is a finitely generated $\mathbb{Z}_p[\![G]\!]$-module, the result of Perbet implies that

$$\mathrm{ord}_p\left(\left(R\left(E/F_\infty\right)^\vee\right)_{G_n} \Big/ p^n\right) = \left(\mathrm{rank}_{\mathbb{Z}_p[\![G]\!]}\left(R\left(E/F_\infty\right)^\vee\right) n + \mu_G\left(R\left(E/F_\infty\right)^\vee\right)\right) p^{dn} + O\left(np^{(d-1)n}\right).$$

The estimate is now immediate from Theorem 6.5. For the final remark, one sees that from the proof of Corollary 5.4 that if Conjecture A holds, then

$$\mathrm{rank}_{\mathbb{Z}_p[\![G]\!]}\left(R\left(E/F_\infty\right)^\vee\right) = \mu_G\left(R\left(E/F_\infty\right)^\vee\right) = 0.$$

□

Under the validity of Conjecture B of Coates-Sujatha, we have an even better upper bound.

Corollary 6.7. *Retain the settings of Theorem 6.5. If both Conjecture A and Conjecture B of Coates-Sujatha hold, then*

$$\mathrm{ord}_p\left(R\left(E/F_n\right)[p^n]\right) = O\left(p^{(d-1)n}\right).$$

Proof. Since $R\left(E/F_\infty\right)^\vee$ is a finitely generated $\mathbb{Z}_p[\![H]\!]$-module by the validity of Conjecture A, we may apply [26, Proposition 2.4] to obtain

$$\mathrm{ord}_p\left(\left(R\left(E/F_\infty\right)^\vee\right)_{G_n} \Big/ p^n\right) \leq \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\left(R\left(E/F_\infty\right)^\vee\right) np^{(d-1)n} + O\left(p^{(d-1)n}\right).$$

If Conjecture B holds, then as in the proof of Corollary 5.7, $\mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\left(R\left(E/F_\infty\right)^\vee\right) = 0$. Hence,

$$\mathrm{ord}_p\left(\left(R\left(E/F_\infty\right)^\vee\right)_{G_n} \Big/ p^n\right) = O\left(p^{(d-1)n}\right).$$

Combining this with Theorem 6.5, we obtain the required estimate. □

6.3. **Trivializing Extension.** We now consider the case of the trivializing extension. The case of elliptic curve with and without complex multiplication will be treated separately.

When E has complex multiplication, it is well known that the Galois group $\mathrm{Gal}(F_\infty/F)$ with $F_\infty = F(E[p^\infty])$ contains an open subgroup which is Abelian and isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. In this situation, Theorem 6.2 (with $d = 2$) says that $\mathrm{ord}_p\left(\ker r_n\right) = O(n)$ and $\mathrm{ord}_p\left(\mathrm{coker}\, r_n\right) = O\left(p^n\right)$. In the next theorem, we show that a sharper estimate for the cokernel is possible in this case.

Theorem 6.8. *Let E/F be an elliptic curve with complex multiplication. Suppose that $F_\infty = F\left(E[p^\infty]\right)$ and $G = \mathrm{Gal}(F_\infty/F)$ is uniform. Then the kernel and cokernel of the restriction maps*

$$r_n : R\left(E/F_n\right) \longrightarrow R\left(E/F_\infty\right)^{G_n}$$

are finite. Furthermore, $\mathrm{ord}_p|\ker r_n| = O(n)$ *and* $\mathrm{ord}_p|\mathrm{coker}\, r_n| = O(n)$.

Proof. In view of the proof of Theorem 6.2, it suffices to show that $\mathrm{ord}_p|\mathrm{coker}\, r_n| = O(n)$. This in turn reduces us to showing that $\ker g_n$ has the same growth. Let K be the imaginary quadratic field which gives E the complex multiplication. By base-changing, we may assume that $E[p]$ is realized over F, that $K \subseteq F$, that E has good reduction at every prime of F, and that $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p^2$. Choose S to be the set of primes above p and the infinite primes. From the theory of complex multiplication, we see that F_∞ is the compositum of F and K_∞, where K_∞ is the unique $\mathbb{Z}_p^2$-extension of K. By [21, Théorème 3.2], there are finitely many primes of K_∞ above p. So, there are finitely many primes of F_∞ above p. Combining this latter observation with Proposition 4.3, we see that $\mathrm{ord}_p|\ker g_n| = O(n)$. □

In this situation, Corollary 6.3 (or Theorem 6.8) yields

$$\mathrm{ord}_p\left(R\left(E/F_n\right)^\vee[p^\infty]\right) = \mu_G\left(R\left(E/F_\infty\right)^\vee\right)p^{2n} + O\left(np^n\right).$$

In particular, if Conjecture A of Coates-Sujatha holds, then

$$\mathrm{ord}_p\left(R\left(E/F_n\right)^\vee[p^\infty]\right) = O\left(np^n\right).$$

There is one case where we have the above estimate without assuming Conjecture A holds.

Proposition 6.9. *Let K be an imaginary quadratic field at which the prime p splits completely in K, say $p = \mathfrak{p}\overline{\mathfrak{p}}$. Let F_0 be a finite extension of K which is unramified at $\mathfrak{p}$. Let E be an elliptic curve defined over F_0 which satisfies all the following properties.*

(a) E has complex multiplication given by the ring of integers of K.
(b) E has good ordinary reduction at all primes of F_0 above p.
(c) $F_0(E_{\mathrm{tor}})$ is an Abelian extension of K.

Let $F = F_0(E[p])$ and $F_\infty = F_0(E[p^\infty]) = F(E[p^\infty])$. Then

$$\mathrm{ord}_p\left(R\left(E/F_n\right)^\vee[p^\infty]\right) = O\left(np^n\right).$$

Proof. Indeed, under the hypothesis of the proposition, one can show that $\mu_G\left(R\left(E/F_\infty\right)^\vee\right) = 0$ by appealing to the results of Gillard and Schneps. (For the details of this argument, we refer readers to [31, Proposition 4.1].) Hence it follows from this that we have the estimate as asserted. □

We now come to the case of an elliptic curve without complex multiplication.

Theorem 6.10. *Let E be an elliptic curve defined over F without complex multiplication. Suppose that $F_\infty = F\left(E[p^\infty]\right)$ and $G = \mathrm{Gal}(F_\infty/F)$ is uniform. Then the kernel and cokernel of the restriction maps*

$$r_n : R\left(E/F_n\right) \longrightarrow R\left(E/F_\infty\right)^{G_n}$$

are finite. Furthermore, the power of p in $\ker r_n$ is $O(n)$ and the power of p in $\mathrm{coker}\, r_n$ is $O\left(np^{2n}\right)$.

In [40], Serre proved that $H^i\left(G_n,\ E[p^\infty]\right)$ is finite for every $i \geq 0$. For our purpose, we need to go one step further by analyzing its growth (for $i = 1, 2$), which is the content of the next lemma.

Lemma 6.11. *Retain the setting of Theorem 6.10. Then for $i = 1,\ 2$, the groups $H^i(G_n,\ E[p^\infty])$ are finite and $\mathrm{ord}_p\left|H^i\left(G_n,\ E[p^\infty]\right)\right| = O(n)$.*

Proof. Since E is an elliptic curve without complex multiplication, the group G has dimension 4. By the discussion in [47, p. 302], and enlarging F if necessary, we may assume that $G = Z \times H$, where $Z \cong \mathbb{Z}_p$ and $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. By Lemma 6.1(a), $E[p^\infty]^{Z_n}$ is finite; it follows from Lemma 2.3 that $H^1(Z_n,\ E[p^\infty]) = 0$. Therefore, the spectral sequence

$$H^i(H_n,\ H^j(Z_n,\ E[p^\infty])) \Longrightarrow H^{i+j}(G_n,\ E[p^\infty])$$

degenerates to yield

$$H^i\left(H_n,\ E[p^\infty]^{Z_n}\right) \cong H^i\left(G_n,\ E[p^\infty]\right).$$

Now, applying Lemma 2.1, we see that

$$\mathrm{ord}_p\left|H^1\left(G_n,\ E[p^\infty]\right)\right| = \mathrm{ord}_p\left|H^1\left(H_n,\ E[p^\infty]^{Z_n}\right)\right| \leq 3\,\mathrm{ord}_p\left|E[p^\infty]^{Z_n}\right| = O(n) \quad \text{and}$$

$$\mathrm{ord}_p\left|H^2\left(G_n,\ E[p^\infty]\right)\right| = \mathrm{ord}_p\left|H^2\left(H_n,\ E[p^\infty]^{Z_n}\right)\right| \leq \binom{3}{2}\mathrm{ord}_p\left|E[p^\infty]^{Z_n}\right| = O(n).$$

This completes the proof of the lemma. □

Proof of Theorem 6.10. In view of Lemma 6.11, it remains to study the growth of $\ker g_n$. By base-changing, we may assume that E has no additive reduction outside p. Let S be the set of primes of F consisting of the primes above p, the multiplicative primes of E outside p, and the Archimedean primes. For all $v \in S$, the decomposition group has dimension ≥ 2 (see [4, Lemma 2.8]). The rest of the argument proceeds as before building on Propositions 4.1 and 4.7. □

Remark 6.12. *When the elliptic curve has potential good ordinary reduction at all primes above p, more can be said. Indeed, under this assumption, Greenberg showed (cf. [11, Proposition 5.3]) that the kernel of the restriction map on the classical Selmer groups $s_n : \mathrm{Sel}(E/F_n) \longrightarrow \mathrm{Sel}(E/F_\infty)^{G_n}$ is finite and bounded. Hence, $\ker r_n$ is also bounded in this case.*

Corollary 6.13. *Let E be an elliptic curve defined over a number field F without complex multiplication and F_∞/F be the trivializing extension. Then*

$$\mathrm{ord}_p\left(R\left(E/F_n\right)[p^n]\right) = \mu_G\left(R\left(E/F_\infty\right)^\vee\right)p^{4n} + O\left(np^{3n}\right).$$

If Conjecture A of Coates-Sujatha holds, then

$$\mathrm{ord}_p\left(R\left(E/F_n\right)[p^n]\right) = O\left(np^{3n}\right).$$

Proof. Since F_∞/F is the trivializing extension, it follows from [6, Lemmas 2.4 and 3.1] that $R\left(E/F_\infty\right)^\vee$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module. By [37, Théorème 2.1], we have

$$\mathrm{ord}_p\left(\left(R\left(E/F_\infty\right)^\vee\right)_{G_n}\Big/p^n\right) = \mu_G\left(R\left(E/F_\infty\right)^\vee\right)p^{4n} + O\left(np^{3n}\right).$$

The estimate follows from Theorem 6.10. The final assertion follows from Corollary 5.4. □

Corollary 6.14. *Let E be an elliptic curve defined over a number field F and F_∞/F be the trivializing extension. If both Conjecture A and Conjecture B of Coates-Sujatha hold, then*

(a) $\mathrm{ord}_p\left(R\left(E/F_n\right)[p^\infty]\right) = O\left(p^n\right)$ *if E is an elliptic curve with complex multiplication.*

(b) $\mathrm{ord}_p\left(R\left(E/F_n\right)[p^n]\right) = O\left(p^{3n}\right)$ *if E does not have complex multiplication.*

Proof. In the case when E is an elliptic curve with complex multiplication, the assertion follows from Corollary 6.3 with $d = 2$. When E does not have complex multiplication, the proof of the statement is similar to the argument in Corollary 6.7. □

Remark 6.15. *It is natural to ask if the above growth formula can allow us to estimate the growth of fine Shafarevich-Tate groups (see [50] for the definition) as done for the classical Shafarevich-Tate groups in [10]. A key ingredient used in this proof is the p-divisibility of* $E(F_n)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p$. *However, as the fine Mordell-Weil group need not be p-divisible (see [50, §7]), the torsion part of the Pontryagin dual of the fine Shafarevich-Tate group and* $R(E/F_n)[p^\infty]^\vee$ *need not agree. Therefore, the above asymptotic formula for the fine Selmer group does not carry over to the fine Shafarevich-Tate group automatically. For* $\mathbb{Z}_p$*-extensions, asymptotic growth estimates for the fine Shafarevich-Tate group has been obtained by the second named author in [27] under certain hypotheses. Unfortunately, the results rely on finer aspects of the structure theory of* $\mathbb{Z}_p[\![\Gamma]\!]$*-modules which are not available for more general Iwasawa algebras, and so the techniques of [27] do not carry over.*

7. Examples

Example 7.1. Let E be the elliptic curve defined by $y^2 + y = x^3 - x$. Let $p = 5$. By [12, Example 4.13], we know that $\mathrm{Sel}\left(E/\mathbb{Q}(\mu_{5^\infty},\ \alpha^{-5^\infty})\right) = 0$ for every $\alpha = (\pm 5)^m$. From this, it is then easy to verify that for every finite extension F of $\mathbb{Q}$ contained in $\mathbb{Q}(\mu_{5^\infty}, \alpha^{-5^\infty})$, one has $\mathrm{Sel}(E/F) = 0$ which in turn implies that $R(E/F) = 0$. By Corollary 6.4, it follows that $R(E/F_\infty)$ is cotorsion over $\mathbb{Z}_5[\![\mathrm{Gal}(F_\infty/F)]\!]$ for every multiple $\mathbb{Z}_5$-extension F_∞ of F.

Example 7.2. Let E be the elliptic curve $150a1$ of Cremona's table which is given by

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

Let $p = 5$ and $F = \mathbb{Q}(\mu_5)$. Let S be the set of primes of F lying above $2, 3, 5$, and ∞. Then, E has good ordinary reduction at the unique prime of F above 5 and split multiplicative reduction at the unique primes of F above 2 and 3. By [3, Example 23] and [25, §6], we know that $R(E/F_\infty)^\vee$ is a pseudo-null $\mathbb{Z}_5[\![\mathrm{Gal}(F_\infty/F)]\!]$-module when F_∞ is one of the following 5-adic extension

$$\mathbb{Q}\left(E[5^\infty], 3^{5^{-\infty}}\right),\ \mathbb{Q}\left(E[5^\infty], 2^{5^{-\infty}}, 3^{5^{-\infty}}\right),\ \mathbb{Q}\left(E[5^\infty], 3^{5^{-\infty}}, 5^{5^{-\infty}}\right),\ \mathbb{Q}\left(E[5^\infty], 2^{5^{-\infty}}, 3^{5^{-\infty}}, 5^{5^{-\infty}}\right),$$

$$L_\infty\left(E[5^\infty], 2^{5^{-\infty}}, 3^{5^{-\infty}}\right),\ L_\infty\left(E[5^\infty], 3^{5^{-\infty}}, 5^{5^{-\infty}}\right),\ L_\infty\left(E[5^\infty], 2^{5^{-\infty}}, 3^{5^{-\infty}}, 5^{5^{-\infty}}\right),$$

where L_∞ is any $\mathbb{Z}_5^r$-extension of F for $1 \le r \le 3$. Therefore, Corollary 5.7 applies to yield $\mathrm{corank}_{\mathbb{Z}_5}\left(R(E/\mathcal{F}_n)\right) = O\left(5^{(d-2)n}\right)$, where $\mathcal{F}_n = F_\infty^{\mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})^{5^n}}$.

Example 7.3. Let E be the elliptic curve 79a1 of Cremona's tables given by

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

Let $p = 3$ and $F = \mathbb{Q}(\mu_3)$. Let S be the set of primes of F lying above $3, 79$ and ∞. By [17, p. 362] and [25, §6], we see that $R(E/F_\infty)^\vee$ is a pseudo-null $\mathbb{Z}_3[\![\mathrm{Gal}(F_\infty/F)]\!]$-module when F_∞ is one of the following 3-adic extensions

$$\mathbb{Q}\left(\mu_{3^\infty}, 3^{3^{-\infty}}\right),\ \mathbb{Q}\left(\mu_{3^\infty}, 3^{3^{-\infty}}, 79^{3^{-\infty}}\right).$$

Corollary 6.7 then tells us that $\mathrm{ord}_3\left(R\left(E/F_n\right)[3^n]\right)$ is $O\left(3^n\right)$ and $O\left(3^{2n}\right)$ for the above two extensions respectively.

Example 7.4. Let E be one of the following elliptic curves (with Cremona label): 256a1, 256a2, 256d1, 256d2 with complex multiplication by $\mathbb{Q}(\sqrt{-2})$ or 121b1, 121b2 with complex multiplication by $\mathbb{Q}(\sqrt{-11})$. These elliptic curves have good reduction at $p = 3$. In [1, Theorem 3.11], it was shown that these satisfy Conjecture A for $p = 3$ over the base field $F = \mathbb{Q}(E[3])$ which is non-Abelian over $\mathbb{Q}$. However, it does not seem that the validity of Conjecture B is known for any p-adic Lie extension over F. Nevertheless, we can still apply Corollary 6.6 to obtain

$$\operatorname{ord}_3\left(R\left(E/F_n\right)\left[3^n\right]\right) = O\left(n3^{(d-1)n}\right).$$

for every multi-false-Tate extension, F_∞ of F of dimension $d \geq 2$, and apply Theorem 6.8 to yield

$$\operatorname{ord}_3\left(R\left(E/F_n\right)\left[3^n\right]\right) = O\left(n3^n\right),$$

when $F_\infty = F\left(E[3^\infty]\right)$ is the trivializing extension over F.

Example 7.5. Let E be the elliptic curve 3136u1 from Cremona's table with complex multiplication by $\mathbb{Q}(\sqrt{-1})$. This is given by the equation

$$y^2 = x^3 - 343x.$$

This elliptic curve has good ordinary reduction at all primes satisfying $p \equiv 1 \pmod 4$. For p large, the validity of Conjecture A does not appear to be verified in literature. Nevertheless, when $F_\infty = F\left(E[p^\infty]\right)$ is the trivializing extension over F, we can still apply Proposition 6.9 to obtain

$$\operatorname{ord}_p\left(R\left(E/F_n\right)^\vee\left[p^\infty\right]\right) = O\left(np^n\right).$$

Acknowledgements

The authors thank Prof. Kumar Murty, Prof. John Coates, and Antonio Lei for their interest and comments on an earlier draft. D. Kundu thanks Centre de Recherches Mathématiques (CRM) for their hospitality and support where parts of this work were carried out during the thematic semester "Number Theory - Cohomology in Arithmetic" in Fall 2020. She acknowledges the support of the PIMS Postdoctoral Fellowship. M. F. Lim acknowledges support by the National Natural Science Foundation of China under Grant Nos. 11550110172 and 11771164, and the Fundamental Research Funds for the Central Universities of CCNU under grant CCNU20TD002. We thank the anonymous referee for their comments which helped improve the exposition of the article.

References

[1] C. S. Aribam. On the μ-invariant of fine Selmer groups. *J. Number Theory*, 135:284–300, 2014.
[2] P. Balister and S. Howson. Note on Nakayama's lemma for compact Λ-modules. *Asian J. Math.*, 1(2):224–229, 1997.
[3] A. Bhave. Analogue of Kida's formula for certain strongly admissible extensions. *J. Number Theory*, 122(1):100–120, 2007.
[4] J. Coates. Fragments of the GL_2 Iwasawa theory of elliptic curves without complex multiplication. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, pages 1–50. Lecture Notes in Math., 1716, Springer, Berlin, 1999.
[5] J. Coates and R. Sujatha. Euler-Poincaré characteristics of abelian varieties. *Comptes Rendus de l'Académie des Sciences-Series I-Mathematics*, 329(4):309–313, 1999.
[6] J. Coates and R. Sujatha. Fine Selmer groups of elliptic curves over p-adic Lie extensions. *Math. Ann.*, 331(4):809–839, 2005.

[7] A. A. Cuoco and P. Monsky. Class numbers in $\mathbb{Z}_p^d$-extensions. *Math. Ann.*, 255(2):235–258, 1981.
[8] J. Dixon, M. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1999.
[9] K. R. Goodearl and J. Warfield, R. B. *An introduction to non-commutative Noetherian rings*, volume 61 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, second edition, 2004.
[10] R. Greenberg. Introduction to Iwasawa theory for elliptic curves. Arithmetic algebraic geometry (Park City, UT, 1999). *IAS/Park City Math. Ser*, 9:407–464, 1999.
[11] R. Greenberg. Galois theory for the Selmer group of an abelian variety. *Compos. Math.*, 136(3):255–297, 2003.
[12] Y. Hachimori and O. Venjakob. Completely faithful Selmer groups over Kummer extensions. *Doc. Math., Extra Volume: Kazuya Kato's Fiftieth Birthday*, pages 443–478, 2003.
[13] M. Harris. Correction to p-adic representations arising from descent on abelian varieties. *Compos. Math.*, 121(1):105–108, 2000.
[14] S. Howson. Euler characteristics as invariants of Iwasawa modules. *Proceedings of the London Mathematical Society*, 85(3):634–658, 2002.
[15] S. Howson. Structure of central torsion Iwasawa modules. *Bull. Soc. Math. France*, 130(4):507–535, 2002.
[16] K. Iwasawa. On Γ-extensions of algebraic number fields. *Bull. Am. Math. Soc.*, 65(4):183–226, 1959.
[17] S. Jha. Fine Selmer group of Hida deformations over non-commutative p-adic Lie extensions. *Asian J. Math.*, 16(2):353–365, 2012.
[18] K. Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.
[19] Y. Kubo and Y. Taguchi. A generalization of a theorem of Imai and its applications to Iwasawa theory. *Math. Z.*, 275(3-4):1181–1195, 2013.
[20] T. Y. Lam. *Lectures on modules and rings*, volume 189 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.
[21] A. Lannuzel and T. Nguyen Quang Do. Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres. *Manuscripta Math.*, 102(2):187–209, 2000.
[22] D. Liang and M. F. Lim. On the Iwasawa asymptotic class number formula for $\mathbb{Z}_p^r \rtimes \mathbb{Z}_p$-extensions. *Acta Arithmetica*, 189(2):191–208, 2019.
[23] M. F. Lim. On the pseudo-nullity of the dual fine Selmer groups. *Int. J. Number Theory*, 11(7):2055–2063, 2015.
[24] M. F. Lim. Comparing the π-primary submodules of the dual Selmer groups. *Asian J. Math.*, 21(6):1153–1181, 2017.
[25] M. F. Lim. Notes on the fine Selmer groups. *Asian J. Math.*, 21(2):337–361, 2017.
[26] M. F. Lim. A note on asymptotic class number upper bounds in p-adic Lie extensions. *Acta Math. Sin. (Engl. Ser.)*, 35(9):1481–1490, 2019.
[27] M. F. Lim. On the control theorem for fine Selmer groups and the growth of fine Tate-Shafarevich groups in $\mathbb{Z}_p$-extensions. *Doc. Math.*, 25:2445–2471, 2020.
[28] M. F. Lim and V. K. Murty. The growth of the Selmer group of an elliptic curve with split multiplicative reduction. *Int. J. Number Theory*, 10(3):675–687, 2014.

[29] M. F. Lim and V. K. Murty. Growth of Selmer groups of CM abelian varieties. *Canadian J. Math.*, 67(3):654–666, 2015.

[30] M. F. Lim and V. K. Murty. The growth of fine Selmer groups. *J. Ramanujan Math. Soc. 31, no. 1, 79–94*, 2016.

[31] M. F. Lim and R. Sujatha. On the structure of fine Selmer groups and Selmer groups of CM elliptic curves. to appear in Proceeding of Ropar conference, RMS-Lecture Notes Series.

[32] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18(3-4):183–266, 1972.

[33] J. S. Milne. *Arithmetic duality theorems*. BookSurge, LLC, Charleston, SC, 2006.

[34] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of Fundamental Principles of Mathematical Sciences. Springer-Verlag, Berlin, 2008.

[35] A. Neumann. Completed group algebras without zero divisors. *Arch. Math. (Basel)*, 51(6):496–499, 1988.

[36] Y. Ochi. A remark on the pseudo-nullity conjecture for fine Selmer groups of elliptic curves. *Comment. Math. Univ. St. Pauli*, 58(1):1–7, 2009.

[37] G. Perbet. Sur les invariants d'Iwasawa dans les extensions de Lie p-adiques. *Algebra & Number Theory*, 5(6):819–848, 2012.

[38] K. Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.

[39] K. Rubin. *Euler systems*. Number 147. Princeton University Press, 2000.

[40] J.-P. Serre. Sur les groupes de congruence des variétés abéliennes. II. *Bulletin of the Russian Academy of Sciences. Mathematical series*, 35(4):731–737, 1971.

[41] J.-P. Serre. *Abelian l-adic representations and elliptic curves. With the collaboration of Willem Kuyk and John Labute. Revised reprint of the 1968 original*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998.

[42] J.-P. Serre. *Local Algebra*. Springer Monographs in Mathematics, Spring-Verlag, Berlin, 2000.

[43] S. Shekhar. Comparing the corank of fine Selmer group and Selmer group of elliptic curves. *J. Ramanujan Math. Soc.*, 33(2):205–217, 2018.

[44] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2009.

[45] C. Skinner and E. Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[46] J. Tate. Letter from Tate to Iwasawa on a relation between K_2 and Galois cohomology Algebraic K-theory, II: "Classical" algebraic K-theory and connections with arithmetic (Proc. Conf., Seattle Res. Center, Battelle Memorial Inst., 1972). *Lecture Notes in Math.*, 342:524–527, 1973.

[47] O. Venjakob. On the structure theory of the Iwasawa algebra of a p-adic Lie group. *J. European Math. Soc.*, 4(3):271–311, 2002.

[48] O. Venjakob. A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory. With an appendix by Denis Vogel. *J. Reine Angew. Math.*, 559:153–191, 2003.

[49] C. Wuthrich. *The fine Selmer group and height pairings*. PhD thesis, University of Cambridge, 2004.

[50] C. Wuthrich. The fine Tate-Shafarevich group. *Math. Proc. Camb. Phil. Soc.*, 142(1):1–12, 2007.

[51] C. Wuthrich. Iwasawa theory of the fine Selmer group. *J. Algebraic Geom.*, 16(1):83–109, 2007.

[52] S. L. Zerbes. Selmer groups over p-adic Lie extensions. I. *J. London Math. Soc. (2)*, 70(3):586–608, 2004.

(Kundu) Mathematics Department, 1984, Mathematics Road, University of British Columbia, Vancouver, Canada, V6T1Z2
Email address: dkundu@math.ubc.edu

(Lim) School of Mathematics and Statistics & Hubei Key Laboratory of Mathematical Sciences, Central China Normal University, Wuhan, 430079, P.R.China.
Email address: limmf@mail.ccnu.edu.cn