GROWTH OF SELMER GROUPS AND FINE SELMER GROUPS IN UNIFORM PRO-p EXTENSIONS

DEBANJANA KUNDU

Abstract. In this article, we study the growth of (fine) Selmer groups of elliptic curves in certain infinite Galois extensions where the Galois group G, is a uniform, pro-p, p-adic Lie group. By comparing the growth of (fine) Selmer groups with that of class groups, we show that it is possible for the μ-invariant of the (fine) Selmer group to become arbitrarily large in a certain class of nilpotent, uniform, pro-p Lie extension. We also study the growth of fine Selmer groups in false Tate curve extensions.

Dans cet article, nous étudions la croissance de groupes de Selmer (fins) de courbes elliptiques dans certaines extensions infinies de Galois oú le groupe de Galois G est un groupe de Lie uniforme, pro-p, p-adique. En comparant la croissance des groupes (fins) de Selmer avec celle des groupes de classes, nous montrons qu'il est possible que l'invariant μ du groupe (fin) de Selmer devienne arbitrairement grand dans une certaine classe de nilpotents, uniformes, pro-p Lie extension. Nous étudions également la croissance de groupes de Selmer fins dans de fausses extensions de courbe de Tate.

1. Introduction

Iwasawa theory began as the study of ideal class groups over infinite towers of number fields. Kenkichi Iwasawa introduced the notion of a μ-invariant to study the growth of (p-ranks) of ideal class groups in $\mathbb{Z}_p$-extensions. In [13], he constructed $\mathbb{Z}_p$-extensions over number fields with arbitrarily large μ-invariants. This notion of a μ-invariant was later generalized to all uniform pro-p groups [12], [30]. In [10], Hajir and Maire investigated uniform pro-p groups which are realisable as Galois groups of extensions of number fields with arbitrarily large μ-invariant.

In the study of rational points on Abelian varieties, the Selmer group plays an important role. In [21], exploiting the intimate connection between class groups and Selmer groups, Mazur developed an analogous theory to study the growth of Selmer groups of Abelian varieties in $\mathbb{Z}_p$-extensions. He showed that the Selmer groups of Abelian varieties and ideal class groups have *similar* growth patterns in $\mathbb{Z}_p$-extensions. When the Abelian variety has good ordinary reduction at p, it is possible to associate a μ-invariant to the Selmer group. In [3], Coates and Sujatha showed that the *fine* Selmer group has even stronger finiteness properties than the classical Selmer group. They showed that the growth of fine Selmer groups mimics the growth of ideal class group in a general p-adic analytic extension containing the *cyclotomic* $\mathbb{Z}_p$-extension. In [20], this was further investigated by Lim and Murty wherein they extended this analogy to some non p-adic analytic extensions as well. In [16], the author showed that there exist non-cyclotomic $\mathbb{Z}_p$-extensions

Date: October 18, 2020.

2010 *Mathematics Subject Classification.* Primary 11R23.

Key words and phrases. Selmer groups, Fine Selmer groups, Class groups, p-rank.

over number fields where the μ-invariant associated to the fine Selmer group can be made arbitrarily large. In this article, the goal is to extend these methods and investigate the growth of Selmer groups and fine Selmer groups of Abelian varieties (and their associated μ-invariants) in extensions of the kind studied by Hajir-Maire.

In Section 3, we develop a general strategy to show that the μ-invariant of (fine) Selmer groups can be arbitrarily large in extensions where it is known that the μ-invariant associated to the class group is arbitrarily large. We give explicit examples of nilpotent, uniform, pro-p, p-adic Lie extensions of number fields with arbitrarily large μ-invariant of (fine) Selmer groups. In Section 4, we study the growth of fine Selmer groups in metabelian extensions (in particular, false Tate curve extensions). All the results we prove in this paper are for elliptic curves, but can be easily generalized to Abelian varieties.

2. Preliminaries

Throughout this article, p is an odd prime.

2.1. **Selmer Groups and Fine Selmer Groups [2], [3], [32].**

Let E be an elliptic curve defined over a fixed number field F. Let S be a finite set of primes in F containing the Archimedean primes, the primes above p, and the primes of bad reduction of E; for short write $S \supseteq S_\infty \cup S_p \cup S_{\text{bad}}$. For any (finite or infinite) extension L/F, denote by L_S the maximal extension of L unramified outside S; for the Galois group $\text{Gal}(L_S/L)$, set the notation $G_S(L)$. For a $G_S(L)$-module M, its i-th Galois cohomology group is denoted by $H^i\left(G_S(L),\ M\right)$. If w is a place of L, 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. For local fields, the cohomology group $H^i(L_w,\ M)$ is with respect to the absolute Galois group of L_w. For an Abelian group A, we use the notation $A[p]$ to denote its p-torsion points and $A(p)$ to denote its p-primary part.

The p-**primary Selmer group** fits into an exact sequence

$$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \text{Sel}(E/F) \to \text{Ш}(E/F)(p) \to 0$$

where $E(F)$ is the group of F-rational points called the **Mordell-Weil group** and $\text{Ш}(E/F)$ is the **Shafarevich-Tate group**.

The *fine Selmer group* is a subgroup of the classical Selmer group obtained by imposing stronger conditions at primes above p. The p-**primary fine Selmer Group** is defined by the following kernel

$$0 \to R\left(E/F\right) \to \text{Sel}\left(E/F\right) \to \bigoplus_{v|p} H^1\left(F_v,\ E[p^\infty]\right),$$

where $E[p^\infty]$ is the set of all the p-power division points of the elliptic curve.

For an infinite Galois extension $\mathcal{L}/F$, the p-primary Selmer group, $\text{Sel}\left(E/\mathcal{L}\right)$, and the p-primary fine Selmer group, $R\left(E/\mathcal{L}\right)$, are defined as follows

$$0 \to \text{Sel}\left(E/\mathcal{L}\right) \to H^1\left(G_S(\mathcal{L}),\ E[p^\infty]\right) \to \bigoplus_{v\in S}\left(\varinjlim_{L}\bigoplus_{w|v} H^1\left(L_w,\ E\right)(p)\right),$$

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

The inductive limit is taken with respect to the restriction maps and L runs over all finite extensions of F contained in $\mathcal{L}$. Also, note that

$$\begin{aligned}\operatorname{Sel}\left(E/\mathcal{L}\right) &= \varinjlim_{L} \operatorname{Sel}\left(E/L\right),\\ R\left(E/\mathcal{L}\right) &= \varinjlim_{L} R\left(E/L\right).\end{aligned}$$

2.1.1. Control Theorem. Let F be a number field and $\mathcal{L}/F$ be a p-adic analytic extension with Galois group $\operatorname{Gal}(\mathcal{L}/F) \simeq G$. Let E be an elliptic curve defined over F. The study of the natural restriction map

$$s_{\mathcal{L}/F} : \operatorname{Sel}\left(E/F\right) \to \operatorname{Sel}\left(E/\mathcal{L}\right)^G$$

is called the **control problem**. Mazur proved the following result.

Theorem 2.1 (Control Theorem [21]). *Let $\mathcal{L}/F$ be a $\mathbb{Z}_p$-extension and let E be an elliptic curve defined over F with good ordinary reduction at primes above p. Then both $\ker(s_{\mathcal{L}/L})$ and $\operatorname{coker}(s_{\mathcal{L}/L})$ are finite and bounded as L/F varies over all finite extensions inside $\mathcal{L}$.*

In [7], Greenberg formulated a general plan to attack this problem. He proved generalizations of Mazur's Control Theorem stated below.

Set $E(\mathcal{L})[p^\infty]$ to denote all the p-power torsion points in $\mathcal{L}$, $\mathfrak{g}$ be the Lie algebra of $\operatorname{Gal}(\mathcal{L}/F) \simeq G$, and $\mathfrak{d}_{\mathfrak{p}}$ (resp. $\mathfrak{i}_{\mathfrak{p}}$) be the Lie algebra of the decomposition group (resp. inertia subgroup) at $\mathfrak{p}$. For any Lie algebra $\mathfrak{l}$, denote by $\mathfrak{l}'$, the derived Lie subalgebra.

Theorem 2.2 (Greenberg [7]). *Assume E has potentially ordinary reduction at all primes of F lying over p. Assume that $\mathcal{L}/F$ is a p-adic Lie extension satisfying the property that $\mathfrak{d}_{\mathfrak{p}}' = \mathfrak{i}_{\mathfrak{p}}'$ for all primes $\mathfrak{p}$ above p. Further suppose that $\mathfrak{g}$ is reductive or $E(\mathcal{L})[p^\infty]$ is finite. Then both $\ker(s_{\mathcal{L}/L})$ and $\operatorname{coker}(s_{\mathcal{L}/L})$ are finite as L varies over all finite extensions of F inside $\mathcal{L}$.*

Some examples of p-adic Lie extensions $\mathcal{L}/F$, where the property $\mathfrak{d}_{\mathfrak{p}}' = \mathfrak{i}_{\mathfrak{p}}'$ holds for all primes $\mathfrak{p} \mid p$, include:

1. when G is Abelian.
2. when the inertia subgroup has finite index in G for all $\mathfrak{p} \mid p$.
3. when G admits a faithful, finite-dimensional p-adic representation of Hodge-Tate type at $\mathfrak{p} \mid p$.

With the same setting as above, for the fine Selmer group, there is an analogous control problem. It involves studying the natural restriction map

$$r_{\mathcal{L}/F} : R\left(E/F\right) \to R\left(E/\mathcal{L}\right)^G.$$

The following result is known.

Theorem 2.3 (Control theorem for fine Selmer groups [26, Chapter VII, Section 4]). *Let F be a number field and E be an elliptic curve defined over F. Let $\mathcal{L}/F$ be a $\mathbb{Z}_p^d$-extension where $d \geq 1$, and suppose all primes in S are finitely decomposed. Then both $\ker(r_{\mathcal{L}/L})$ and $\operatorname{coker}(r_{\mathcal{L}/L})$ are finite as L varies over all finite extensions of F inside $\mathcal{L}$.*

Remark 2.4. (1) The Control Theorem for fine Selmer groups is independent of the reduction type at p.

(2) When $d = 1$, the Control Theorem is proved for *all* $\mathbb{Z}_p$-extensions [32]. Moreover, the order of $\ker(r_{\mathcal{L}/L})$ and $\operatorname{coker}(r_{\mathcal{L}/L})$ are bounded independent of L.

2.2. **Iwasawa Theory of Uniform pro-p Groups [4], [12], [30].** Let G be a finitely generated pro-p group. For two elements $x,\ y \in G$, define the commutator $[x,\ y] := x^{-1}y^{-1}xy$. For closed subgroups $H_1,\ H_2$ of G, let $[H_1,\ H_2]$ be the closed subgroup generated by all commutators $[x_1,\ x_2]$ with $x_i \in H_i$.

Definition 2.5. *A profinite group G, is **uniform** if it is topologically finitely generated by d generators, and there exists a (unique) filtration by the p-descending central series of G. In other words, we have*

$$G = G_0 \supset G_1 \supset \dots G_n \supset \dots$$

such that each G_{n+1} is normal in G_n, and $G_n/G_{n+1} \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^d$. In particular, a uniform p-adic analytic group is always pro-p.

For a d-dimensional uniform pro-p group G, one has $[G :\ G_n] = p^{dn}$, for all n. A well-known and important fact is the following.

Theorem 2.6 ([4, Theorem II.8.32])**.** *Every p-adic analytic pro-p group is a closed subgroup of $\mathrm{GL}_m(\mathbb{Z}_p)$ for some integer m and contains an open uniform subgroup.*

Let $\Lambda(G) = \mathbb{Z}_p[\![G]\!] := \varprojlim_H \mathbb{Z}_p[G/H]$ be the **completed Iwasawa algebra** of G, where H runs over all open normal subgroups of G. Set $\Omega(G) = \mathbb{F}_p[\![G]\!] = \mathbb{Z}_p[\![G]\!]/p$. Both $\Omega(G)$ and $\Lambda(G)$ are local, Noetherian rings without zero divisors [4, Chapter 7] (see also [12]). Denote by $\mathcal{Q}\left(\Omega\left(G\right)\right)$ the fraction skew field of $\Omega(G)$. If M is a finitely generated $\Omega(G)$-module, the **rank** of M, written as $\operatorname{rank}_{\Omega(G)}(M)$, is the $\mathcal{Q}\left(\Omega\left(G\right)\right)$-dimension of $M \otimes_{\left(\Omega(G)\right)} \mathcal{Q}(\Omega(G))$.

Definition 2.7. *Let M be a finitely generated $\Lambda(G)$-module. Set*

$$r(M) = \operatorname{rank}_{\Omega(G)}\left(M[p]\right); \qquad \mu(M) = \sum_{i\geq 0} \operatorname{rank}_{\Omega(G)}\left(M[p^{i+1}]/M[p^i]\right)$$

where $M[p^i]$ denotes the p^i-torsion points of M for all $i \in \mathbb{Z}^{\geq 0}$.

It follows that $\mu(M) \geq r(M)$ and $r(M) = 0$ if and only if $\mu(M) = 0$.

Recall that for any G-module M, the co-invariant M_G is the largest quotient of M on which G acts trivially. When M is a discrete p-primary Abelian group or a compact pro-p Abelian group, define its **Pontryagin dual** $M^\vee := \operatorname{Hom}_{\mathrm{cont}}(M,\ \mathbb{Q}_p/\mathbb{Z}_p)$. The following result of Perbet measures the growth of finitely generated $\Lambda(G)$-modules where G is a uniform, pro-p, p-adic Lie group.

Theorem 2.8 (Perbet [24])**.** *Let G be a uniform pro-p group of dimension d and M be a $\Lambda(G)$-module of rank $\rho(M)$. Then for sufficiently large n,*

$$\dim_{\mathbb{F}_p}\left(M_{G_n}/p\right) = \left(\rho(M) + r(M)\right)p^{dn} + O\left(p^{n(d-1)}\right),$$
$$\#\left(M_{G_n}/p^n\right) = p^{\left(\rho(M)+\mu(M)\right)p^{dn} + O\left(np^{n(d-1)}\right)}.$$

2.3. **Growth of Class Groups in Uniform pro-p Lie Extensions.** Let p be an odd prime and let F be a number field. Let $\mathcal{L}/F$ be a uniform pro-p Lie extension, i.e. $\mathrm{Gal}(\mathcal{L}/F) \simeq G$ where G is a uniform, pro-p, p-adic Lie group. Let L/F be a finite subextension of $\mathcal{L}/F$. Denote by $\mathrm{Cl}(F)_p$ the p-Sylow subgroup of the class group of F. Define the Iwasawa module

$$X\left(\mathcal{L}/F\right) := \varprojlim_{L} \mathrm{Cl}(L)_p$$

where the inverse limit is taken over all number fields L in $\mathcal{L}/F$ with respect to the norm map. By a Nakayama's Lemma argument, it is known that $X(\mathcal{L}/F)$ is a torsion $\Lambda(G)$-module [1](see also [11]). Set $\mu_{\mathcal{L}/F} = \mu\left(X\left(\mathcal{L}/F\right)\right)$ and $r_{\mathcal{L}/F} = r\left(X\left(\mathcal{L}/F\right)\right)$. Perbet proved the following result by classical descent.

Theorem 2.9 (Perbet [24])**.** *Let $X(\mathcal{L}/F)$ be as defined above. Then for sufficiently large n,*

$$r_p\left(\mathrm{Cl}(F_n)\right) = r_{\mathcal{L}/F}p^{dn} + O\left(p^{n(d-1)}\right),$$

$$\log\left|\mathrm{Cl}(F_n)_p/p^n\right| = \mu_{\mathcal{L}/F}p^{dn}\log p + O\left(np^{d(n-1)}\right),$$

where for any Abelian group A, the p-rank $r_p(A) := \dim_{\mathbb{F}_p}(A[p])$.

Remark 2.10. In [18], Lei obtained a more precise version of the above result when G is a metabelian extension.

2.4. **p-Rational Fields.** Let p be an odd prime. Let F be a number field and let $\mathcal{F}_{S_p}$ denote the maximal pro-p extension of F unramified outside S_p, i.e. the primes above p. The number field F is called **p-rational** if $\mathrm{Gal}(\mathcal{F}_{S_p}/F)$ is pro-p free.

Theorem 2.11 ([6, Theorem IV.3.5])**.** *Let F be a number field that contains a primitive p-th root of unity. Then, F is p-rational if and only if there exists a unique prime $\mathfrak{p}$ above p and the p-part of the $\mathfrak{p}$-class group of F is trivial.*

Remark 2.12.
1. It is believed that given any number field, it should be p-rational for all primes p outside a set of density zero [8, Page 99].
2. Let F be a p-rational number field which is Galois over $\mathbb{Q}$. Suppose $\mathfrak{p}$ is the unique prime above p in F, $p \nmid \left|\mathrm{Cl}(F)\right|$, and $p-1 \mid [F:\mathbb{Q}]$. Then, $\mathfrak{p}$ is totally ramified in $\mathcal{F}_{S_p}/F$ [8, Remark 6.4].

2.5. **False Tate Curve Extensions.** Let p be a fixed odd prime and let F be a number field containing the group of p-th roots of unity, denoted by μ_p. The **false Tate curve extension**, denoted by $\mathcal{F}_\infty$, is obtained by adjoining the p-power roots of a fixed integer $m > 1$ to the cyclotomic $\mathbb{Z}_p$-extension of F, which in turn is written as F_{cyc}. Therefore,

$$\mathcal{F}_\infty = F\left(\mu_{p^\infty},\ m^{\frac{1}{p^n}} : n = 1, 2, \dots\right).$$

The Galois group, $G = \mathrm{Gal}\left(\mathcal{F}_\infty/F\right) \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$, is a solvable group with no element of finite order. This is a non-Abelian pro-p p-adic Lie extension of cohomological dimension 2 [28]. Set $H = \mathrm{Gal}\left(\mathcal{F}_\infty/F_{\mathrm{cyc}}\right) \simeq \mathbb{Z}_p$. The extension $\mathcal{F}_\infty/F$ is contained in $G_S(F)$ where S is a finite set of primes in F containing the Archimedean primes, the primes above p, the primes of bad reduction of E and primes dividing m. For short we write, $S \supseteq S_\infty \cup S_p \cup S_{\mathrm{bad}} \cup S_m$.

3. Growth of Selmer Groups in Uniform pro-p Extensions

3.1. **Brief Review of the Result of Hajir-Maire [10, Section 4].** Given a uniform pro-p group G, Hajir-Maire developed a general strategy to construct G-extensions of number fields with arbitrarily large μ-invariant.

Proposition 3.1 ([10, Proposition 4.1]). *Suppose G is a uniform pro-p group and $\mathcal{L}/\mathbb{M}$ is a Galois extension of a number field such that*

(1) $\mathrm{Gal}(\mathcal{L}/\mathbb{M}) \simeq G$;

(2) there are finitely many primes that are ramified in $\mathcal{L}/\mathbb{M}$;

(3) there are infinitely many primes of $\mathbb{M}$ that split completely in $\mathcal{L}/\mathbb{M}$.

Then, there exist G-extension of number fields with arbitrarily large associated μ-invariant.

The main theorem they prove is the following.

Theorem 3.2 ([10, Theorem 4.8]). *Let G be a uniform pro-p group having an automorphism τ of order m with fixed-point-free action, where m is coprime to p. Suppose F_0 is a totally imaginary field admitting a cyclic extension F/F_0 of degree m such that F is p-rational. Then there exists a finite p-extension K/F unramified outside p and a G-extension $\mathcal{L}/K$ such that for any given integer N, there exists a cyclic degree p extension K' over $K(\mu_p)$ and a G-extension $\mathcal{L}'/K'$ where $\mathcal{L}' = \mathcal{L}K'$ whose associated μ-invariant is greater than N.*

3.1.1. *Construction/Discussion:* Let G be a uniform pro-p group having an automorphism τ of order m with fixed-point-free action, where m is coprime to p. If $m = 2$, then $G \simeq \mathbb{Z}_p^d$ for some $d \geq 1$ [25, Corollary 4.6.10].

Suppose F_0 is a totally imaginary field admitting a cyclic extension F/F_0 of degree m such that F is p-rational. For n sufficiently large, set K_0 (resp. K) to be the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of F_0 (resp. F). It follows that K is p-rational. By construction, K/K_0 is a cyclic extension of degree m.

Let $\mathcal{K}_{S_p}$ be the maximal, pro-p, unramified outside S_p extension of K. Then, there exists an intermediate field $K \subset \mathcal{L} \subset \mathcal{K}_{S_p}$ with $\mathrm{Gal}(\mathcal{L}/K_0) \simeq G \rtimes \langle\tau\rangle$ [10, Proposition 4.6]. The conjugation action of τ is fixed-point-free by assumption; equivalently the action of $\langle\tau\rangle$ is fixed-point-free, if m is a prime (not equal to p). Under this additional assumption, $G \rtimes \langle\tau\rangle$ is a Frobenius group [25, Theorem 4.6.1(d)]. Hence G is a nilpotent uniform pro-p group [25, Corollary 4.6.10].

Every place $\mathfrak{q}$ which is totally inert in K/K_0 and is not ramified in $\mathcal{L}/K$ splits completely in this extension [10, Proposition 4.7]. By the Chebotarev density theorem, there are infinitely many primes that remain totally inert in the Galois extension K/K_0.

Without loss of generality assume K contains μ_p (otherwise replace K by $K(\mu_p)$ in this paragraph). Choose an integer $t \geq 1$, and primes $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ in $\mathcal{O}_K$ which split completely in $\mathcal{L}/K$. There exists a $\mathbb{Z}/p\mathbb{Z}$-extension, K'/K in which each of these $\mathfrak{q}_i$ ramify. Indeed, let $\mathfrak{q}_0$ be a prime ideal coprime to $\mathfrak{q}_1 \cdots \mathfrak{q}_t$ which is in the inverse of $\mathfrak{q}_1 \cdots \mathfrak{q}_t$, i.e. $\mathfrak{q}_0\mathfrak{q}_1 \cdots \mathfrak{q}_t$ is a principal ideal generated by α (say). Then $K' := K(\alpha^{1/p})$ is a cyclic degree p extension of K where $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ ramify.

3.2. **Strategy to Extend the Above Result.** To extend Theorem 3.2 to (fine) Selmer groups of elliptic curves, we adopt the following strategy. We write it down for Selmer groups. For fine Selmer groups, the strategy is identical.

Step 1: Let G be a d-dimensional uniform pro-p p-adic Lie group. Let K be a number field that admits an infinite extension $\mathcal{L}/K$ with $\mathrm{Gal}(\mathcal{L}/K) \simeq G$ such that the associated μ-invariant in this extension is arbitrarily large. Recall that $[G : G_n] \simeq (\mathbb{Z}/p\mathbb{Z})^{nd}$. Let K_n/K be the field fixed by G_n. Let E/K be an elliptic curve such that $E(K)[p] \neq 0$. Then, the first task is to show

$$r_p\left(\mathrm{Sel}\left(E/K_n\right)\right) \geq r_p\left(\mathrm{Cl}(K_n)\right) r_p\left(E(K_n)[p]\right) - 2. \tag{1}$$

This is a consequence of the following lemma.

Lemma 3.3 ([19, Proposition 4.1(i)]). *Let $\mathbb{M}$ be a number field and E be an elliptic curve with good reduction everywhere over $\mathbb{M}$ and $E(\mathbb{M})[p] \neq 0$. Then,*

$$r_p\left(\mathrm{Sel}\left(E/\mathbb{M}\right)\right) \geq r_p\left(\mathrm{Cl}(\mathbb{M})\right) r_p\left(E(\mathbb{M})[p]\right) - 2. \tag{2}$$

Step 2: With notation as in *Step 1*, we construct a cyclic extension K_n'/K_n such that $r_p\left(\mathrm{Sel}\left(E/K_n'\right)\right)$ can be made arbitrarily large.

A key ingredient in this step is the following result from genus theory.

Theorem 3.4 ([27]). *Let $\mathbb{M}$ be a number field and $\mathbb{L}/\mathbb{M}$ be a $\mathbb{Z}/p\mathbb{Z}$-extension. Let t be the number of primes that ramify in $\mathbb{L}/\mathbb{M}$. Then,*

$$r_p\left(\mathrm{Cl}(\mathbb{L})\right) \geq t - 1 - r_p\left(\mathcal{O}_{\mathbb{M}}^{\times}\right).$$

Let K be the number field considered in *Step 1*. Suppose there exists a $\mathbb{Z}/p\mathbb{Z}$-extension K'/K such that the number of primes t that ramify in K'/K can be made arbitrarily large. Further, suppose these primes split completely in the G-extension $\mathcal{L}/K$. Set $\mathcal{L}' = \mathcal{L}K'$; then $K_n' = K_nK'$ is the field fixed by G_n in $\mathcal{L}'/K'$.

By (the K_n'-version of) Inequality 1 and Theorem 3.4, both $r_p\left(\mathrm{Cl}(K_n')\right)$ and $r_p\left(\mathrm{Sel}\left(E/K_n'\right)\right)$ can be made arbitrarily large. In fact [10, Page 609],

$$r_p\left(\mathrm{Sel}(E/K_n')\right) \geq [K_n' : K]\left(t - r_2(K') - 1\right) - 2 \tag{3}$$

where r_2 denotes the number of pairs of complex embeddings of the number field. In obtaining the above inequality we have used that $r_p\left(E(K_n')[p]\right) \geq 1$.

Remark 3.5. When G is a uniform pro-p group having an automorphism τ of order m with fixed-point-free action, and m is coprime to p, the number fields K and K' exist by the work of Hajir-Maire. They are constructed as in Theorem 3.2 (see Section 3.1.1 for the details).

Step 3: We apply Greenberg's Control Theorem (Theorem 2.2). This allows the comparison of the growth estimate obtained from genus theory (in Inequality 3) and that obtained from the theorem of Perbet (Theorem 2.8).

Recall that the Pontryagin dual of the Selmer group (and hence the Pontryagin dual of the fine Selmer group) is *always* a finitely generated $\Lambda(G)$-module where G is a uniform pro-p group. This is a consequence of the Nakayama's Lemma in this setting [1].

In our setting, Perbet's theorem can be applied. It gives the following equality.

$$r_p\left(\mathrm{Sel}\left(E/\mathcal{L}'\right)^{G_n}\right) = \left(\rho(\mathfrak{X}') + r(\mathfrak{X}')\right)p^{dn} + O(p^{n(d-1)}) \tag{4}$$

where $\rho(\mathfrak{X}')$ (resp. $r(\mathfrak{X}')$) is the $\Lambda(G)$-rank (resp. $\Omega(G)$-rank) of the dual Selmer group $\mathfrak{X}(E/\mathcal{L}') = \mathfrak{X}'$. By construction, $\mathrm{Gal}(\mathcal{L}'/K') \simeq G$. If $\mathcal{L}'/K'$ is such that

Greenberg's Control Theorem is applicable and the p-ranks of the kernel and cokernel of the restriction map are finite and bounded (see for example [7, Proposition 3.4]), then for an elliptic curve E with (potentially) ordinary reduction at K',

$$r_p\left(\operatorname{Sel}\left(E/\mathcal{L}'\right)^{G_n}\right) = r_p\left(\operatorname{Sel}\left(E/K'_n\right)\right) + O(1).$$

This allows the comparison of the leading terms of Inequality 3 and Equation 4. We get

$$\rho(\mathfrak{X}') + r(\mathfrak{X}') \geq pt - pr_2(K') - p.$$

In *Step 2*, it was guaranteed by construction that t can be made arbitrarily large. It follows that $\rho(\mathfrak{X}') + r(\mathfrak{X}')$ (and hence $\rho(\mathfrak{X}') + \mu(\mathfrak{X}')$) can be made arbitrarily large. If $\mathfrak{X}'$ is $\Lambda(G)$-torsion then $\rho(\mathfrak{X}') = 0$. Hence, $\mu(\mathfrak{X}')$ can be made arbitrarily large.

3.3. **Growth of Selmer groups when G is Abelian.** When G is an Abelian pro-p group, i.e. $G \simeq \mathbb{Z}_p^d$ (for $d \geq 1$), the result of Hajir-Maire can be applied (with $m = 2$) and Greenberg's Control Theorem holds.

With notation as before, invoking the strategy described in Section 3.2, the following result is immediate.

Theorem 3.6. *Let $G \simeq \mathbb{Z}_p^d$ where $d \geq 1$. Suppose F_0 is a totally imaginary field. Let E/F_0 be an elliptic curve with good reduction everywhere over F_0 and ordinary reduction at primes above p. Further suppose $E(F_0)[p] \neq 0$. Let F/F_0 be a cyclic extension of degree coprime to p such that F is p-rational. Given any integer $N > 0$, there exists a number field K'/F and a $\mathbb{Z}_p^d$-extension $\mathcal{L}'/K'$ such that $\rho(\mathfrak{X}') + \mu(\mathfrak{X}') \geq N$. If further, $\mathfrak{X}'$ is $\Lambda(G)$-torsion, then $\mu(\mathfrak{X}') \geq N$.*

Remark 3.7. If E/F_0 is an elliptic curve with complex multiplication (CM) by an imaginary quadratic field contained which is a subfield of F_0, then E acquires good reduction everywhere over $F_0(E[p])$ [29]. If $p \geq 5$, $[F_0(E[p]) : F_0]$ is coprime to p and by the Weil pairing $F_0(E[p]) \supseteq F_0(\mu_p)$.

3.4. **Growth of Selmer groups when G is a non-Abelian nilpotent uniform pro-p group.** Throughout this section, let $p \geq 5$.

The nilpotent uniform pro-p groups of dimension ≤ 2 are always Abelian. This follows from the fact that every 2-dimensional nilpotent Lie algebra is Abelian. In this section, we work with a specific example of a non-Abelian nilpotent uniform pro-p group of dimension 3 considered in [10].

In [5, Theorem 7.4], González-Sánchez and Klopsch proved that up to isomorphism, every non-Abelian, nilpotent, uniform, pro-p group of dimension 3 is parametrized by $s \in \mathbb{N}$ and represented by

$$G(s) = \left\langle x,\ y,\ z \mid [x,\ z] = [y,\ z] = 1,\ [x,\ y] = z^{p^s} \right\rangle.$$

The center of $G(s)$ is pro-cyclic and there exists a short exact sequence

$$1 \to \mathbb{Z}_p \to G(s) \to \mathbb{Z}_p^2 \to 1.$$

These groups were studied by Hajir-Maire. They proved that $G(s)$ is a uniform pro-p group having an automorphism τ of order 3 with fixed-point-free action when $p \equiv 1 \pmod 3$ [10, Proposition 5.1]. The following result is known about growth of class groups (and the associated μ-invariant) in $G(s)$-extensions of number fields.

Theorem 3.8 ([10, Corollary 5.3])**.** *Suppose p is a regular prime, i.e. $p \nmid \left|\mathrm{Cl}(\mathbb{Q}(\mu_p))\right|$ and satisfy the additional property $p \equiv 1 \pmod 3$. For each $s \in \mathbb{N}$, there exist $G(s)$-extensions of number fields with arbitrarily large μ-invariants.*

In this section, we prove the following result.

Theorem 3.9. *Let $s \in \mathbb{N}$ and $G \simeq G(s)$. Suppose p is a fixed regular prime with $p \equiv 1 \pmod 3$. Suppose F_0 is a totally imaginary field containing μ_p and E/F_0 is an elliptic curve without CM with good reduction everywhere, ordinary reduction at p, and $E(F_0)[p] \neq 0$. Let F/F_0 be a cyclic $\mathbb{Z}/3\mathbb{Z}$ such that F is p-rational, Galois over $\mathbb{Q}$, and $p \nmid \left|\mathrm{Cl}(F)\right|$. Given any integer $N > 0$, there exists a number field K'/F and a $G(s)$-extension $\mathcal{L}'/K'$ such that $\rho(\mathfrak{X}') + \mu(\mathfrak{X}') \geq N$. If further, $\mathfrak{X}'$ is $\Lambda(G)$-torsion, then $\mu(\mathfrak{X}') \geq N$.*

Remark 3.10. Since $G(s)$ is a non-Abelian, nilpotent, uniform pro-p group, the corresponding Lie algebra *can not* be reductive.

To prove the theorem, we adopt the general strategy developed in Section 3.2. We need to verify that Greenberg's Control Theorem is in fact applicable to this extension. For this, we need the following lemmas.

Lemma 3.11. *Let the number field K' and a $G(s)$-extension $\mathcal{L}'/K'$ with arbitrarily large μ-invariant be constructed as in Theorem 3.2. Let E/K' be an elliptic curve without CM. Then, $E(\mathcal{L}')[p^\infty]$ is finite.*

To prove the lemma, recall the following result of Zarhin.

Theorem 3.12 ([33, Main Theorem])**.** *Let X be a g-dimensional Abelian variety over a number field $\mathbb{M}$. Assume that the Hodge group of X is semi-simple. If $\mathcal{L}/\mathbb{M}$ is an infinite extension such that its intersection with $\mathbb{M}_{\mathrm{cyc}}/\mathbb{M}$ is of finite degree over $\mathbb{M}$, then $X(\mathcal{L})_{\mathrm{tors}}$ is finite.*

Proof of Lemma 3.11. When E is an elliptic curve without CM, it is known that its Hodge group is SL_2, and therefore semi-simple [22, Section 2]. Further, the intersection of the $G(s)$-extension $\mathcal{L}'/K'$ and K'_{cyc}/K' is necessarily of finite degree over K'. This is because by construction of $\mathcal{L}'/K'$, there are infinitely many primes that are not finitely decomposed in $\mathcal{L}'/K'$. However, in K'_{cyc}/K' all primes are finitely decomposed. Thus, for a non-CM elliptic curve E/K', Theorem 3.12 implies that $E(\mathcal{L}')[p^\infty]$ is finite. □

Lemma 3.13. *Keep the notation as in Theorem 3.9. Let the number field K' and a $G(s)$-extension $\mathcal{L}'/K'$ with arbitrarily large μ-invariant be constructed as in Theorem 3.2. Let E/K' be an elliptic curve. The inertia subgroup has finite index in $G(s)$ for all primes above p in K'.*

Proof. Recall that by construction, K is the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of F. Therefore, K/F is p-rational number field containing μ_p such that $\mathcal{K}_{S_p} \subseteq \mathcal{F}_{S_p}$. There is a unique prime $\mathfrak{p}$ above p in K (see Theorem 2.11), i.e. $S_p = \{\mathfrak{p}\}$. Recall that the p-adic Lie extension $\mathcal{L}/K$ with $\mathrm{Gal}(\mathcal{L}/K) \simeq G(s)$ is contained in $\mathcal{K}_{S_p}$. Since K/F is a p-power extension and $p \nmid \left|\mathrm{Cl}(F)\right|$, it follows that $p \nmid \left|\mathrm{Cl}(K)\right|$ [31, Theorem 10.4(1)]. By Remark 2.12(2), the unique prime $\mathfrak{p} \mid p$ is totally ramified in $\mathcal{F}_{S_p}/F$. Hence, the unique prime above p in K is totally ramified in $\mathcal{K}_{S_p}/K$; the inertia subgroup of $G(s) \simeq \mathrm{Gal}(\mathcal{L}/K)$ is maximal (in this case, of dimension 3). Upon performing a base change to K'/K, for every prime above $\mathfrak{p}$

in K', the dimension of the inertia subgroup is still 3, i.e. the inertia subgroup has finite index in the $G(s)$-extension over K'. □

Proof of Theorem 3.9. Given F_0 as in the statement of the theorem, construct K'/F_0 as in Theorem 3.2 and let $\mathcal{L}'/K'$ be a $G(s)$-extension with arbitrarily large μ-invariant. Such a $G(s)$-extension $\mathcal{L}'/K'$ exists by the proof of Theorem 3.8.

By hypothesis, E/K' has good reduction everywhere and good ordinary reduction at primes above p. To apply Greenberg's Control Theorem, the following two properties need to be verified.

(i) $E(\mathcal{L}')[p^\infty]$ is finite.
(ii) The inertia subgroup has finite index in $G(s)$ for all primes $\mathfrak{p} \mid p$.

The first property is verified in Lemma 3.11. This guarantees that the kernel of the restriction map is finite and bounded [7, Proposition 3.1]. The second property is verified in Lemma 3.13. This guarantees that the cokernel is also finite and bounded [7, Proposition 4.4]. The general strategy developed in Section 3.2 proves the theorem. □

Remark 3.14. If p is a regular prime and m is an odd divisor of $p-1$, then for any $k \geq 1$, the cyclotomic field $\mathbb{Q}(\mu_{p^k})$ admits a $\mathbb{Z}/m\mathbb{Z}$ extension $K/\mathbb{Q}(\mu_{p^k})$ which is p-rational (see discussion following [10, Theorem 1.1]).

3.5. **Growth of fine Selmer groups when G is Abelian.** When $G \simeq \mathbb{Z}_p^d$ (for $d \geq 1$), it is possible to prove an analogue of Theorem 3.6 for the fine Selmer groups. The difficulty lies in the fact that the *control problem* for fine Selmer groups is less understood. Set the notation $\mathfrak{Y} = \mathfrak{Y}(E/\mathcal{L})$ (resp. $\mathfrak{Y}' = \mathfrak{Y}(E/\mathcal{L}')$) to denote the Pontryagin dual of the fine Selmer group over $\mathcal{L}$ (resp. $\mathcal{L}'$).

Theorem 3.15. *Let $G \simeq \mathbb{Z}_p^d$ where $d \geq 1$. Suppose F_0 is a totally imaginary field containing μ_p. Let E/F_0 be an elliptic curve with good reduction everywhere and $E(F_0)[p] \neq 0$. Let F/F_0 be a cyclic extension of degree coprime to p such that F is p-rational and $p \nmid \mathrm{Cl}(F)$. Given any integer $N > 0$, there exists a number field K'/F and a $\mathbb{Z}_p^d$-extension $\mathcal{L}'/K'$ such that $\rho(\mathfrak{Y}') + \mu(\mathfrak{Y}') \geq N$. If further, $\mathfrak{Y}'$ is $\Lambda(G)$-torsion, then $\mu(\mathfrak{Y}') \geq N$.*

Remark 3.16. (1) The definition of the fine Selmer group is independent of the choice of the set S. By hypothesis, E has good reduction everywhere. Hence, choose $S = S_p \cup S_\infty$. In our setting, the unique prime $\mathfrak{p} \mid p$ is totally ramified in $\mathcal{L}/K$. Observe that the prime(s) above p in K' are finitely decomposed in the $\mathbb{Z}_p^d$-extension $\mathcal{L}'/K'$.
(2) When $d = 1$, Wuthrich proved the Control Theorem for all $\mathbb{Z}_p$-extensions. As will be clear from the proof, in this case there is no hypothesis on the reduction type [16].
(3) It is always possible to choose $S = S_p \cup S_{\text{bad}} \cup S_\infty$. If all the bad primes in S are finitely decomposed in $\mathcal{L}'/K'$, we need not assume E/F_0 has good reduction everywhere.

Definition 3.17. *Let $H_S(\mathbb{M})$ be the maximal Abelian unramified extension of $\mathbb{M}$ such that all the primes in S split completely in $H_S(\mathbb{M})$. By class field theory, the Galois group* $\mathrm{Gal}\left(H_S(\mathbb{M})/\mathbb{M}\right) \simeq \mathrm{Cl}_S(\mathbb{M})$ *where* $\mathrm{Cl}_S(\mathbb{M})$ *is the S-class group of* $\mathbb{M}$.

We begin by recording two elementary estimates.

Lemma 3.18 ([19, Lemma 3.2])**.** *Let G be a pro-p group and let M be a discrete G-module that is cofinitely generated over $\mathbb{Z}_p$. If $r_p\left(H^1\left(G,\ \mathbb{Z}/p\mathbb{Z}\right)\right)$ is finite then*

$$r_p\left(H^1\left(G,\ M\right)\right) \leq r_p\left(H^1\left(G,\ \mathbb{Z}/p\mathbb{Z}\right)\right)\left(\operatorname{corank}_{\mathbb{Z}_p} M + \log_p\left(\left|M/M_{\text{div}}\right|\right)\right).$$

Lemma 3.19 ([20, Lemma 3.2])**.** *Consider the following short exact sequence of cofinitely generated Abelian groups*

$$P \to Q \to R \to S.$$

Then

$$\left|r_p\left(Q\right) - r_p\left(R\right)\right| \leq 2r_p\left(P\right) + r_p\left(S\right).$$

To prove Theorem 3.15, we will apply the general strategy. To complete *Step 1* of the general strategy, we need the following lemmas.

Lemma 3.20. *Let $\mathcal{L}$ be any $\mathbb{Z}_p^d$ extension of a number field $\mathbb{M}$. Let $S(\mathbb{M})$ be a finite set of primes in $\mathbb{M}$ containing the primes above p and the Archimedean primes. Let s_0 be the number of non-Archimedean primes in $S(\mathbb{M})$. Let $\mathbb{M}_n$ be the subfield of $\mathcal{L}$ such that $[\mathbb{M} : \mathbb{M}_n] = p^{dn}$. Then*

$$\left|r_p\left(\mathrm{Cl}\left(\mathbb{M}_n\right)\right) - r_p\left(\mathrm{Cl}_S\left(\mathbb{M}_n\right)\right)\right| \leq 2s_0p^{dn}.$$

Proof. Let $S(\mathbb{M}_n)$ denote the primes in $\mathbb{M}_n$ above the primes in $S(\mathbb{M})$. Set $S_f(\mathbb{M}_n)$ to denote all the non-Archimedean primes of $S(\mathbb{M}_n)$. Consider the following short exact sequence for all n [23, Lemma 10.3.12],

$$\mathbb{Z}^{\left|S_f(\mathbb{M}_n)\right|} \to \mathrm{Cl}(\mathbb{M}_n) \xrightarrow{\alpha_n} \mathrm{Cl}_S(\mathbb{M}_n) \to 0.$$

Observe that $\ker(\alpha_n)$ is finite because the class group is always finite. Note that $r_p\left(\ker\left(\alpha_n\right)\right) \leq \left|S_f\left(\mathbb{M}_n\right)\right|$ and by finiteness it follows that $r_p\left(\ker\left(\alpha_n\right)/p\right) \leq \left|S_f\left(\mathbb{M}_n\right)\right|$. Using Lemma 3.19, compare the p-ranks in this short exact sequence; this gives

$$\left|r_p\left(\mathrm{Cl}\left(\mathbb{M}_n\right)\right) - r_p\left(\mathrm{Cl}_S\left(\mathbb{M}_n\right)\right)\right| \leq 2\left|S_f(\mathbb{M}_n)\right| \leq 2s_0p^{dn}.$$

The last inequality follows from the fact that if *all* the non-Archimedean primes in $S(\mathbb{M})$ undergo complete splitting in $\mathbb{M}_n$, there are s_0p^{dn} finite primes in $S(\mathbb{M}_n)$. □

Lemma 3.21 ([20, Lemma 4.3])**.** *Let E be an elliptic curve defined over the number field $\mathbb{M}$ with $E(\mathbb{M})[p] \neq 0$. Let S be a finite set of primes in $\mathbb{M}$ containing the primes above p, the primes of bad reduction, and the Archimedean primes. Then,*

$$r_p\left(R\left(E/\mathbb{M}\right)\right) \geq r_p\left(\mathrm{Cl}_S(\mathbb{M})\right) r_p\left(E(\mathbb{M})[p]\right) - 2.$$

We can now prove Theorem 3.15. The proof involves invoking the strategy in Section 3.2. We briefly explain some of the differences.

Proof of Theorem 3.15. Let F_0 be as in the statement. Construct K and K' as in Theorem 3.2. Let t be the number of primes that are inert in K/K_0 and totally split completely in $\mathcal{L}/K$. By construction, these primes ramify in K'/K. Since E/F_0 has good reduction everywhere, set $S = S_p \cup S_\infty$. Recall that the prime(s) above p in K' are finitely decomposed in $\mathcal{L}'$. It follows that for n sufficiently large,

$\Big| r_p\left(\mathrm{Cl}\left(\mathbb{M}_n\right)\right) - r_p\left(\mathrm{Cl}_S\left(\mathbb{M}_n\right)\right)\Big|$ is finite and bounded. Over the n-th layer of the $\mathbb{Z}_p^d$ extension $\mathcal{L}'/K'$, we have

$$r_p\left(R\left(E/K_n'\right)\right) \geq r_p\left(\mathrm{Cl}_S\left(K_n'\right)\right) r_p\left(E\left(K_n'\right)[p]\right) - 2 \tag{5}$$

$$= \left(r_p\left(\mathrm{Cl}\left(K_n'\right)\right) + O(1)\right) r_p\left(E\left(K_n'\right)[p]\right) - 2 \tag{6}$$

$$\geq \left(pt - r_2\left(K'\right) - p\right) p^{dn} + O(1). \tag{7}$$

The first inequality is an application of Lemma 3.21. The equality in the second line follows from Lemma 3.20. The last inequality is obtained by an application of Theorem 3.4 and noting that $r_p\left(E\left(K_n'\right)[p]\right) \geq 1$. By Theorem 2.8,

$$r_p\left(R\left(E/\mathcal{L}'\right)^{G_n}\right) = \left(\rho(\mathfrak{Y}') + r(\mathfrak{Y}')\right) p^{dn} + O(p^{n(d-1)}). \tag{8}$$

Step 3 of the general strategy can now be carried out. The Control Theorem for fine Selmer groups holds when G is Abelian and primes in S are finitely decomposed (Theorem 2.3). This is independent of the reduction type at primes above p. The p-rank of the kernel and cokernel of the (global) restriction map

$$h_{\mathcal{L}'/K_n'} : H^1\left(K_n',\ E[p^\infty]\right) \to H^1\left(\mathcal{L}',\ E[p^\infty]\right)^{G_n}$$

is known to be finite and bounded independent of n [7, Proposition 3.4]. Therefore, the p-rank of ker $\left(r_{\mathcal{L}'/K_n'}\right)$ enjoys the same properties. The above mentioned result of Greenberg also ensures that coker $\left(r_{\mathcal{L}'/K_n'}\right)$ is finite and bounded independent of n, if the same holds for the p-rank of the kernel of the local restriction map. But the latter follows from Lemma 3.18 upon observing that $r_p\left(H^1\left(G_{n,v}, \mathbb{Z}/p\mathbb{Z}\right)\right)$ is bounded independent of n. Now by Lemma 3.19, it is possible to compare the leading terms of Inequality 7 and Equation 8. By construction, t can be made arbitrarily large. This proves the theorem. □

Remark 3.22. At this point, we are unable to prove a Control Theorem for fine Selmer groups in $G(s)$-extensions. This prevents us from completing *Step 3* of the general strategy and proving an analogue of Theorem 3.9 for fine Selmer groups.

Remark 3.23. It was only after this paper was published, while discussing with Meng Fai Lim on another problem, we realized that the strategy developed in Subsection 3.2 can be extended to all p-adic Lie extensions. Indeed, the strategy works whenever the p-rank of $\ker(r_{\mathcal{L}'/K'})$ has bounded p-rank which is trivially true for p-adic Lie extensions.

4. Growth of Fine Selmer Groups in False Tate Curve Extensions

We will use the notation introduced in Section 2.5. In this section, the goal is to prove a non-commutative version of results in [20, Section 5] and [16, Section 3.3]. We prove our results for the false Tate curve extension $\mathcal{F}_\infty/F$ with Galois group $G = \mathrm{Gal}(\mathcal{F}_\infty/F) \simeq H \rtimes \Gamma$ where both H and Γ are isomorphic to $\mathbb{Z}_p$. The action of Γ on H is non-trivial; hence G is non-Abelian. Note that G is a solvable uniform pro-p group which is *not* nilpotent. This is because all nilpotent uniform pro-p groups of dimension ≤ 2 are Abelian. Thus, we do not expect that the results proved in Section 3 will extended easily to the false Tate curve extension.

Consider the setting described in Section 2.5. Let p be a fixed odd prime and for simplicity, set $F = \mathbb{Q}(\mu_p)$. Throughout this section, we make either of the following hypothesis on m:

(1) let m be an integer which is not a p-th power *or*
(2) let $p \mid m$.

In either of the cases, it is guaranteed that the unique prime above p is totally ramified in $\mathcal{F}_\infty/F$ (see [9, Lemma 3.9(ii)] or [17]).

By a deep result of Kato, for a modular elliptic curve, an analogue of the Weak Leopoldt Conjecture (WLC) holds over the cyclotomic extension F_{cyc}/F, i.e. $H^2\Big(G_S\left(F_{\text{cyc}}\right),\ E_{p^\infty}\Big)$ is trivial [14]. By a Hochschild-Serre spectral seqeunce argument it follows that $H^2\left(G_S\left(\mathcal{F}_\infty\right),\ E_{p^\infty}\right) = 0$. Thus, the elliptic curve analogue of the WLC is true over this false Tate curve extension [9, Remark 2.2].

In the main theorem of this section, we relate the growth of fine Selmer groups and class groups in the false Tate curve extension.

Theorem 4.1. *Let E be an elliptic curve defined over a number field F. Let $\mathcal{F}_\infty$ be the false Tate curve extension such that primes of bad reduction of E divide m. Further assume $E[p] \subseteq E(F)$. Then,*

$$\left| r_p\Big(R\left(E/F_n\right)\Big) - 2r_p\left(\mathrm{Cl}\left(F_n\right)\right)\right| = O(1).$$

Remark 4.2. (1) It should be possible to weaken the hypothesis $E[p] \subseteq E(F)$ slightly, i.e. the above theorem should hold under the weaker hypothesis $E(F)[p] \neq 0$ (see [15]).
(2) It should be possible to generalize this result to any metabelian extension considered in [18].

To prove the theorem, we need a series of lemmas. In the first lemma we prove that the class group and S-class group have the same order of growth in the false Tate curve extension. Recall that $S \supseteq S_p \cup S_{\text{bad}} \cup S_m \cup S_\infty$.

Lemma 4.3. *Let $\mathcal{F}_\infty/F$ be the false Tate curve extension of F. Let F_n be the n-th layer of this false Tate curve extension, i.e.*

$$F_n = \mathbb{Q}\left(\mu_{p^n},\ \sqrt[p^n]{m}\right),$$

where either $p \mid m$ or m is an integer that is not a p-th power. Then for sufficiently large n,

$$\Big| r_p\left(\mathrm{Cl}(F_n)\right) - r_p\left(\mathrm{Cl}_S(F_n)\right)\Big| = O(1).$$

The proof is similar to Lemma 3.20 (see also [20, Lemma 5.2]).

Proof. As in the proof of Lemma 3.20, we obtain

$$\Big| r_p\left(\mathrm{Cl}\left(F_n\right)\right) - r_p\left(\mathrm{Cl}_S\left(F_n\right)\right)\Big| \leq 2\big|S_f(F_n)\big| = O(1).$$

By the hypothesis on m, the last equality follows from the fact that primes in S are finitely decomposed in the false Tate curve extension $\mathcal{F}_\infty/F$ [9, Lemmas 3.9]. □

We now define the p-fine Selmer group of an elliptic curve. Let S be a finite set of primes containing the primes above p, the primes of bad reduction of E, the primes above m, and the Archimedean primes. Define

$$R_S\left(E[p]/F\right) = \ker\left(H^1\left(G_S\left(F\right),\ E[p]\right) \to \bigoplus_{v\in S} H^1\left(F_v,\ E[p]\right)\right).$$

The next lemma is the fine Selmer group analogue of Lemma 4.3. As will be shown in the proof of Theorem 4.1, the p-fine Selmer group indeed depends on the set S.

Lemma 4.4. *Let $\mathcal{F}_\infty/F$ be the false Tate curve extension of F. Let F_n be the n-th layer of this false Tate curve extension, i.e.*

$$F_n = \mathbb{Q}\left(\mu_{p^n},\ \sqrt[p^n]{m}\right).$$

Let E be an elliptic curve defined over F satisfying the additional property that $\prod_{v\in S_{bad}} v$ divides m. Then for sufficiently large n,

$$\left| r_p\left(R\left(E/F_n\right)\right) - r_p\left(R_S\left(E[p]/F_n\right)\right)\right| = O(1).$$

Proof. Consider the commutative diagram below.

$$\begin{tikzcd}
0 \arrow[r] & R_S(E[p]/F_n) \arrow[r] \arrow[d, "s_n"] & H^1\left(G_S\left(F_n\right),\ E[p]\right) \arrow[r] \arrow[d, "f_n"] & \bigoplus_{v\in S(F_n)} H^1\left(F_{n,v_n},\ E[p]\right) \arrow[d, "\gamma_n"] \\
0 \arrow[r] & R\left(E/F_n\right)[p] \arrow[r] & H^1\left(G_S\left(F_n\right),\ E[p^\infty]\right)[p] \arrow[r] & \bigoplus_{v_n\in S(F_n)} H^1\left(F_{n,v_n},\ E[p^\infty]\right)[p]
\end{tikzcd}$$

Both f_n and γ_n are surjective. The kernel of these maps are

$$\ker(f_n) = E(F_n)[p^\infty]/p$$
$$\ker(\gamma_n) = \bigoplus_{v_n\in S(F_n)} E(F_{n,v_n})[p^\infty]/p.$$

Observe that $r_p\left(\ker\left(s_n\right)\right) \leq r_p\left(\ker\left(f_n\right)\right) \leq 2$. Also, $r_p\left(\ker\left(\gamma_n\right)\right) \leq 2\left|S_f(F_n)\right|$. By assuming that $\prod_{v\in S_{bad}} v$ divides m, it is guaranteed that all primes are finitely decomposed in the false Tate curve extension [9, Lemma 3.11], i.e. for n sufficiently large, $\left|S_f(F_n)\right| = O(1)$. By an application of the Snake Lemma, it follows that $r_p\left(\text{coker}\left(s_n\right)\right)$ is finite and bounded. Applying Lemma 3.19 to the map s_n gives the desired result. □

We are now in a position to prove the theorem.

Proof of Theorem 4.1. Let S be a finite set of primes containing the primes above p, the primes above m and the Archimedean primes. By hypothesis, it is not needed to assume that S also contains the primes of bad reduction of E. Since $E[p] \subseteq E(F)$, we have the following isomorphism (as $G_S(F_n)$-modules)

$$E[p] \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Since the action of $G_S(F_n)$ is trivial, the following equality holds

$$H^1\left(G_S\left(F_n\right),\ E[p]\right) = \text{Hom}\left(G_S\left(F_n\right),\ E[p]\right).$$

There are similar identifications for the local cohomology groups. It follows that (see [3, Lemma 3.8] or [26, Chapter I 6.1])

$$R_S\left(E[p]/F_n\right) = \operatorname{Hom}\left(\mathrm{Cl}_S\left(F_n\right),\ E[p]\right) \simeq \left(\mathrm{Cl}_S\left(F_n\right)[p]\right)^2.$$

Thus, $r_p\Big(R_S\left(E[p]/F_n\right)\Big) = 2r_p\left(\mathrm{Cl}_S\left(F_n\right)[p]\right)$. Combined with Lemmas 4.3 and 4.4, the proof of the theorem is complete. □

Acknowledgements

We thank Kumar Murty for his continued support and all members of the GANITA Lab for listening to the details. We extend our gratitude to Prof. Sujatha Ramdorai, Prof. Christian Maire, Prof. Karl Rubin, Meng Fai Lim and Jishnu Ray for answering many questions along the way. We thank Prof. Antonio Lei for his comments on an earlier draft of this article. Finally, we thank the referee for a careful reading of the article which helped improve the exposition.

References

[1] P. Balister and S. Howson. Note on Nakayama's lemma for compact Λ-modules. *Asian Journal of Mathematics*, 1(2):224–229, 1997.

[2] J. Coates and R. Sujatha. *Galois cohomology of elliptic curves*, volume 88. Narosa Publishing House New Delhi, 2000.

[3] J. Coates and R. Sujatha. Fine Selmer groups of elliptic curves over p-adic Lie extensions. *Math. Ann.*, 331(4):809–839, 2005.

[4] J. D. Dixon, M. P. Du Sautoy, D. Segal, and A. Mann. *Analytic pro-p groups*, volume 61. Cambridge University Press, 2003.

[5] J. González-Sánchez and B. Klopsch. Analytic pro-p groups of small dimensions. *Journal of Group Theory*, 12(5):711–734, 2009.

[6] G. Gras. *Class Field Theory: from theory to practice.* Springer Science & Business Media, 2013.

[7] R. Greenberg. Galois theory for the Selmer group of an abelian variety. *Compositio Mathematica*, 136(3):255–297, 2003.

[8] R. Greenberg. Galois representations with open image. *Annales mathématiques du Québec*, 40(1):83–119, 2016.

[9] Y. Hachimori and O. Venjakob. Completely faithful Selmer groups over Kummer extensions. *Documenta Math., Extra Volume: Kazuya Kato's Fiftieth Birthday*, pages 443–478, 2003.

[10] F. Hajir and C. Maire. Prime decomposition and the Iwasawa μ-invariant. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 166, pages 599–617. Cambridge University Press, 2019.

[11] M. Harris. Correction to p-adic representations arising from descent on abelian varieties. *Compositio Mathematica*, 121(1):105–108, 2000.

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

[13] K. Iwasawa. On the μ-invariants of $\mathbb{Z}_\ell$-extensions. *Algebraic Geometry and Commutative Algebra*, pages 1–11, 1973.

[14] K. Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.

[15] D. Kundu. *Iwasawa theory of fine Selmer groups.* PhD thesis, University of Toronto, 2020.

[16] D. Kundu. Growth of fine Selmer groups in infinite towers. *Canadian Mathematical Bulletin*, page 1–15, 2020 to appear.

[17] C.-Y. Lee. Non-commutative Iwasawa theory of elliptic curves at primes of multiplicative reduction. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 154, pages 303–324. Cambridge University Press, 2013.

[18] A. Lei. Estimating class numbers over metabelian extensions. *Acta Arithmetica*, 180:347–364, 2017.

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

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

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

[22] D. Mumford. A note of Shimura's paper: Discontinuous groups and abelian varieties. *Math. Ann.*, 181:345–351, 1969.

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

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

[25] L. Ribes and P. Zalesskii. Profinite groups. In *Profinite Groups*. Springer, 2000.

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

[27] R. Schoof. Infinite class field towers of quadratic fields. *J. Reine Angew. Math.*, 1:209–220, 1986.

[28] J.-P. Serre. Sur la dimension cohomologique des groupes profinis. *Topology*, 3(4):413–420, 1965.

[29] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math.(2)*, 88(492-517):2, 1968.

[30] O. 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.

[31] L. C. Washington. *Introduction to cyclotomic fields*, volume 83. Springer, 1997.

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

[33] Y. G. Zarhin. Torsion of abelian varieties, Weil classes and cyclotomic extensions. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 126, pages 1–15. Cambridge University Press, 1999.

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