ACTA ARITHMETICA
Online First version

The non-p-part of the fine Selmer group in a $\mathbb{Z}_p$-extension

by

Adithya Chakravarthy (Toronto)

Abstract. Fix two distinct primes p and ℓ. Let A be an abelian variety over $\mathbb{Q}(\zeta_\ell)$, the cyclotomic field of ℓth roots of unity. Suppose that $A(\mathbb{Q}(\zeta_\ell))[\ell] \neq 0$. We show that there exists a number field L and a $\mathbb{Z}_p$-extension L_∞/L where the ℓ-primary fine Selmer group of A grows arbitrarily quickly. This is a fine Selmer group analogue of a theorem of Washington that there are certain (non-cyclotomic) $\mathbb{Z}_p$-extensions where the ℓ-part of the class group can grow arbitrarily quickly. We also prove this for a wide class of non-commutative p-adic Lie extensions. Finally, we include several examples to illustrate this theorem.

1. Introduction. We begin with a fundamental theorem of Iwasawa, which serves as the starting point of Iwasawa theory. Let K be a number field and let K_∞/K be a $\mathbb{Z}_p$-extension: a Galois extension with Galois group isomorphic to the additive group $\mathbb{Z}_p$ of p-adic integers. For such an extension K_∞/K, there exists a unique sequence of fields

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty$$

such that each K_n/K is a cyclic extension of degree p^n. Iwasawa [Iwa59] proved the following now famous theorem about the growth of class numbers in such towers.

Theorem (Iwasawa). *Let K be a number field and let K_∞/K be a $\mathbb{Z}_p$-extension with layers K_n. Suppose that p^{e_n} is the exact power of p dividing the class number of K_n. Then there exist integers μ, λ, ν such that*

$$e_n = \mu p^n + \lambda n + \nu$$

for all sufficiently large values of n.

A large part of classical Iwasawa theory is devoted to studying the invariants μ and λ in the above formula. In a beautiful paper, Iwasawa showed

2020 *Mathematics Subject Classification*: Primary 11G05; Secondary 11R23, 11R29.
Key words and phrases: Iwasawa theory, fine Selmer groups, abelian varieties, number theory, Selmer groups, elliptic curves.
Received 24 April 2023; revised 8 October 2023.
Published online 8 April 2024.

DOI: 10.4064/aa230424-15-1

[Iwa73, Theorem 1] that there are $\mathbb{Z}_p$-extensions for which the μ-invariant can be *arbitrarily* large.

THEOREM 1.1 (Iwasawa). *Let $N \geq 1$. There exists a number field L and a $\mathbb{Z}_p$-extension L_∞/L such that $\mu \geq N$.*

Now that we have discussed the p-part of the class group in a $\mathbb{Z}_p$-extension, we turns to its ℓ-part, where $\ell \neq p$ are *distinct* primes. The fundamental theorem in this area is due to Washington [Was78]:

THEOREM 1.2 (Washington). *Let $\ell \neq p$ be primes. Let K be an abelian extension of the field $\mathbb{Q}$ of rational numbers. Let K^{cyc}/K be the cyclotomic $\mathbb{Z}_p$-extension of K and let ℓ^{e_n} be the exact power of ℓ dividing the class number of K_n. Then e_n is bounded as $n \to \infty$.*

Based on this, one might reasonably guess that the ℓ-part of the class group is bounded in an *arbitrary* $\mathbb{Z}_p$-extension. But this turns out to be false, as proven in [Was75, Theorem 6].

THEOREM 1.3 (Washington). *Let $N \geq 1$. There exists a number field L and a $\mathbb{Z}_p$-extension L_∞/L such that*

$$e_n \geq Np^n,$$

where ℓ^{e_n} is the exact power of ℓ dividing the class number of L_n.

The purpose of this article is to discuss analogues of Theorems 1.1 and 1.3 for fine Selmer groups of elliptic curves. Let E be an elliptic curve over a number field F. The Mordell–Weil Theorem says the group $E(F)$ of rational points is a finitely generated abelian group. This arithmetic of this group is essentially controlled by the Selmer group of E/F. In [Maz72], Mazur introduced the Iwasawa theory of Selmer groups in $\mathbb{Z}_p$-extensions of F. The notion of the fine Selmer group was formally introduced by Coates and Sujatha in [CS05], even though it had been studied by Rubin [Rub00] and Perrin-Riou [PR93, PR95] under various guises in the late 80's and early 90's. In [CS05], Coates and Sujatha showed that these fine Selmer groups have stronger finiteness properties than classical Selmer groups.

In [Kun20, Theorem 4.2], Kundu proved an analogue of Theorem 1.1 for fine Selmer groups: If A is an abelian variety and $N \geq 1$ is an integer, then there exists a number field L and a $\mathbb{Z}_p$-extension L_∞/L such that the μ-invariant of the fine Selmer group of A over L_∞ is at least N. In other words, μ-invariants of fine Selmer groups can be arbitrarily large. And in [KL23, Theorem B], Kundu and Lei proved a fine Selmer group analogue of Theorem 1.2: In the *cyclotomic* $\mathbb{Z}_p$-extension, the ℓ-part of the fine Selmer group of A stabilizes.

The purpose of the present paper is to prove a fine Selmer group analogue of Theorem 1.3. If ℓ is a prime and A is an abelian variety over a number

field F, let $R_{\ell^\infty}(A/F)$ denote the ℓ-primary fine Selmer group of A over F. (See Section 5.1 for the precise definition.) If G is an abelian group, the *ℓ-rank* of G is defined by $r_\ell(G) = \dim_{\mathbb{Z}/\ell\mathbb{Z}} G[\ell]$. Note that it is possible to have $r_\ell(G) = \infty$; this is true for example if G contains infinitely many copies of $\mathbb{Z}/\ell\mathbb{Z}$. (See [LM16, Section 3] as a reference for this definition.) Here is our main result:

THEOREM 1.4. *Let $\ell \neq p$ be primes. Let $\mathbb{Q}(\zeta_\ell)$ be the cyclotomic field of ℓth roots of unity and let A be an abelian variety over $\mathbb{Q}(\zeta_\ell)$. Suppose that $A(\mathbb{Q}(\zeta_\ell))[\ell] \neq 0$. For every integer $N \geq 1$, there exists a finite extension $L/\mathbb{Q}(\zeta_\ell)$ and a $\mathbb{Z}_p$-extension L_∞/L such that*

$$r_\ell(R_{\ell^\infty}(A/L_n)) \geq Nq^n$$

for all $n \geq 0$, where $q = \min\{\ell, p\}$. In particular, $r_\ell(R_{\ell^\infty}(A/L_n)) \to \infty$ as $n \to \infty$.

More generally, we can also prove this theorem for many non-commutative p-adic Lie extensions. The relevant statement requires a definition:

DEFINITION 1.5. A pro-p group Γ is *uniform of dimension d* if it is topologically finitely generated by d generators and there exists a unique filtration by the p-descending central series of Γ. In other words, we have

$$\Gamma = \Gamma_0 \supset \Gamma_1 \supset \cdots$$

such that each Γ_{n+1} is normal in Γ_n and $\Gamma_n/\Gamma_{n+1} \simeq (\mathbb{Z}/p\mathbb{Z})^d$.

If F is a number field and $\mathfrak{p}$ is a prime ideal of F, then the *$\mathfrak{p}$-class group* of F is the quotient of $\mathrm{Cl}(F)$ by the subgroup generated by the ideal class of $\mathfrak{p}$.

ASSUMPTION 1. Let Γ be a uniform pro-p group with a fixed-point-free automorphism of order m, where $m > 2$ is a prime different from p. Assume that:

(1) there exists a $\mathbb{Z}/m\mathbb{Z}$-extension of number fields F/F_0, where F_0 is totally imaginary,
(2) the field F contains the pth roots of unity,
(3) there is a unique prime $\mathfrak{p}$ of F lying over the rational prime p,
(4) the p-part of the $\mathfrak{p}$-class group of F is trivial.

THEOREM 1.6. *Let $\ell \neq p$ be primes. Let $\mathbb{Q}(\zeta_\ell)$ be the cyclotomic field of ℓth roots of unity and let A be an abelian variety over $\mathbb{Q}(\zeta_\ell)$. Suppose that $A(\mathbb{Q}(\zeta_\ell))[\ell] \neq 0$. Let Γ be a uniform pro-p group with a fixed-point-free automorphism of order m. If $m > 2$, suppose that Assumption 1 holds.*

Then for every integer $N \geq 1$, there exists a finite extension $L/\mathbb{Q}(\zeta_\ell)$ and a Γ-extension L_∞/L such that

$$r_\ell(R_{\ell^\infty}(A/L_n)) \geq Nq^n$$

for all $n \geq 0$, where $q = \min\{\ell, p\}$. In particular, $r_\ell(R_{\ell^\infty}(A/L_n)) \to \infty$ as $n \to \infty$.

Let $\mathrm{Sel}_{\ell^\infty}(A/F)$ denote the ℓ-primary (usual) Selmer group of A over F. (See Section 5.1 for the precise definition.) Since the fine Selmer group is a subgroup of the usual Selmer group, we have the following

COROLLARY 1.7. *Retain the notations and assumptions of Theorem* 1.6. *For every integer $N \geq 1$, there exists a finite extension $L/\mathbb{Q}(\zeta_\ell)$ and a Γ-extension L_∞/L such that*

$$r_\ell(\mathrm{Sel}_{\ell^\infty}(A/L_n)) \geq Nq^n$$

for all $n \geq 0$, where $q = \min\{\ell, p\}$. In particular, $r_\ell(\mathrm{Sel}_{\ell^\infty}(A/L_n)) \to \infty$ as $n \to \infty$.

We give several numerical examples at the end of the paper to show that Assumption 1 often holds.

Strategy. We follow Iwasawa's approach in [Iwa73], which inspired Washington's approach in [Was75, Section VI]. We construct a $\mathbb{Z}_p^d$-extension L_∞/L where the ℓ-rank of the *class group* is unbounded.

THEOREM 1.8. *Let $\ell \neq p$ be primes. Let Γ be a uniform pro-p group. If $m > 2$, then suppose Assumption* 1 *holds. For every integer $N \geq 1$, there exists a finite extension $L/\mathbb{Q}(\zeta_\ell)$ and a Γ-extension L_∞/L such that for all $n \geq 0$*

$$r_\ell(\mathrm{Cl}(L_n)) \geq Np^n.$$

In particular, $r_\ell(\mathrm{Cl}(L_n)) \to \infty$ as $n \to \infty$.

We then use results of Lim–Murty [LM16] to show that the ℓ-rank of the fine Selmer group is close in size to the ℓ-rank of the class group. Putting these two results together, we conclude that the ℓ-part of the fine Selmer group is unbounded in L_∞/L, proving Theorem 1.6.

2. Construction of the Γ-extension K_∞/K.

In this section we will construct a Γ-extension K_∞/K where infinitely many primes split completely. Here Γ will be a uniform pro-p group with a fixed-point-free automorphism τ of order m. The construction proceeds differently in the cases $m = 2$ and $m > 2$.

2.1. The case $m = 2$.

By [RZ00, Corolary 4.6.10], if Γ is a uniform pro-p group with a fixed-point-free automorphism τ of order $m = 2$, then $\Gamma \simeq \mathbb{Z}_p^d$ for some $d \geq 1$.

To motivate the next proposition, recall that if K is an imaginary quadratic field, then there is a $\mathbb{Z}_p$-extension K_∞/K called the *anticyclotomic $\mathbb{Z}_p$-extension* of K. This extension has the property that infinitely many

primes of K split completely in K_∞. The next proposition generalizes this to $\mathbb{Z}_p^d$-extensions for $d \geq 1$.

PROPOSITION 2.1. *Let K be a CM field such that $K/\mathbb{Q}$ is a $\mathbb{Z}/2d\mathbb{Z}$-extension. Suppose that there is only one prime in K lying over p. Then there is a $\mathbb{Z}_p^d$-extension K_∞/K such that infinitely many primes of K split completely in K_∞.*

Proof. This fact is well-known, but for lack of a reference we sketch the proof here. The construction below is reproduced from [Lon12, Section 2]. Let K^+ be the maximal totally real subfield of K. For any integral ideal $\mathfrak{c} \subseteq \mathcal{O}_{K^+}$, let $\mathcal{O}_\mathfrak{c} = \mathcal{O}_{K^+} + \mathfrak{c}\mathcal{O}_K$ be the order of conductor $\mathfrak{c}$ in K. The *ring class field* $K[\mathfrak{c}]/K$ of K of conductor $\mathfrak{c}$ is the Galois extension of K such that there is an isomorphism via the Artin map:

$$\mathrm{Gal}(K[c]/K) \simeq \mathrm{Cl}(\mathcal{O}_\mathfrak{c}).$$

Let $\mathfrak{p}$ be the unique prime of K^+ lying over p. Put $K[\mathfrak{p}^\infty] = \bigcup_{n=1}^\infty K[\mathfrak{p}^n]$. Define K_∞ to be the unique subfield of $K[\mathfrak{p}^\infty]$ satisfying

$$\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p^{[K_\mathfrak{p}^+:\mathbb{Q}_p]} = \mathbb{Z}_p^d.$$

Suppose that ℓ is a rational prime which is inert in K. Then the ideal class of ℓ is trivial in $\mathrm{Cl}(K)$ and hence class field theory shows that ℓ splits completely in any ring class field $K[\mathfrak{c}]$ of conductor coprime to ℓ. (See [Nek07, Section 2.6.3].) In particular, if ℓ is inert in $K/\mathbb{Q}$ and ℓ is coprime to p then ℓ splits completely in K_∞. By the Chebotarev density theorem, there are infinitely many such primes. ∎

2.2. The case $m > 2$. Here is the main result:

PROPOSITION 2.2. *Let Γ be a uniform pro-p group. Suppose Assumption 1 holds. Then there exists a Galois extension K/F and a Γ-extension K_∞/K such that infinitely many primes of K split completely in K_∞.*

Now let F be a number field and let $F_{\max,p}$ be the maximal pro-p extension of F unramified outside the primes above p. The number field F is called *p-rational* if $\mathrm{Gal}(F_{\max,p}/F)$ is pro-p free.

LEMMA 2.3. *Let F be a number field with a primitive pth 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.*

Proof. This is part of [Gra, Theorem IV.3.5]. ∎

LEMMA 2.4. *Keep the notations and assumptions from Proposition 2.2. Let n be an integer such that $[F_0 : \mathbb{Q}]p^n \geq 2d$ and let K_0 (resp. K) be the nth layer of the cyclotomic $\mathbb{Z}_p$-extension of F_0 (resp. F). Then there exists an intermediate field $K \subset K_\infty \subset K_{\max,\,p}$ such that K_∞ is Galois over K_0*

with Galois group $\Gamma \rtimes \langle\tau\rangle$. Suppose τ acts fixed-point-freely on Γ. Then every place of K_0 which is inert in K/K_0 splits completely in K_∞/K.

Proof. This follows from [HM19, Propositions 3.6 and 3.7] if F is p-rational. But Lemma 2.3 gives conditions for F to be p-rational and F satisfies those conditions. ∎

Proposition 2.2 now follows from Lemma 2.4, because by the Chebotarev density theorem there are infinitely many primes that are inert in the cyclic extension K/K_0.

3. Construction of the Γ-extension L_∞/L. Fix $N \geq 1$. In this section we will construct a Γ-extension L_∞/L with the properties in Theorem 1.8, i.e. such that

$$r_\ell(\mathrm{Cl}(L_n)) \geq Np^n \quad \text{for all } n \geq 0.$$

PROPOSITION 3.1. *Let $N \geq 1$ be an integer. Let Γ be a uniform pro-p group of dimension d with a fixed-point-free automorphism of order m. If $m > 2$, suppose Assumption 1 holds. Let K_∞/K denote the Γ-extension from Proposition 2.1 (resp. Proposition 2.2) if $m = 2$ (resp. $m > 2$). There exists a finite extension L/K and a Γ-extension L_∞/L satisfying the following:*

(1) *The extension L_∞ contains K_∞. Furthermore, for all $n \geq 0$, the number of primes ramifying in L_n/K_n is at least*

$$(N + md\ell(\ell-1))p^n.$$

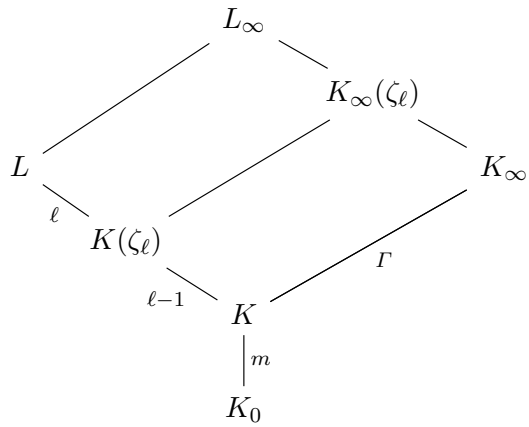
(2) *We have $[L_n : \mathbb{Q}] \geq m\ell(\ell-1)dp^n$ for all $n \geq 0$.*

Proof. We only prove the case $m > 2$; the proof for $m = 2$ is identical and left to the reader. By Proposition 2.2, infinitely many primes of K split completely in K_∞/K. Let $t \geq 1$ be an integer (to be chosen later) and let $v_1, \ldots, v_t$ be primes in K that split completely in K_∞/K.

CLAIM 3.2. *There exists $\alpha \in K$ such that $\mathrm{ord}_{v_i}(\alpha) = 1$ for all $i = 1, \ldots, t$.*

Proof of claim. Consider the ideal class $I = [v_1 \cdot \ldots \cdot v_t] \in \mathrm{Cl}(K)$. Then II^{-1} is trivial in $\mathrm{Cl}(K)$ so there exists a fractional ideal w of K such that $v_1 \cdot \ldots \cdot v_t \cdot w$ is a principal ideal; write $v_1 \cdot \ldots \cdot v_t \cdot w = (\alpha)$ for some $\alpha \in K$. Then $\mathrm{ord}_{v_i}(\alpha) \geq 1$ for all $i = 1, \ldots, t$. We can ensure that $\mathrm{ord}_{v_i}(\alpha)$ is *exactly* 1 by dividing w through by v_i if necessary. This proves the claim. ∎

Now let $\alpha \in K$ be such that $\mathrm{ord}_{v_i}(\alpha) = 1$ for all $i = 1, \ldots, t$. Put $L = K(\alpha^{1/\ell}, \zeta_\ell)$. Then $L/K(\zeta_\ell)$ is a cyclic degree ℓ extension where $v_1, \ldots, v_t$ ramify. Put $L_\infty = K_\infty L$. Then L_∞/L is a Γ-extension. We summarize this in a diagram:



Let K_n (resp. L_n) be the nth layer of the Γ-extension K_∞ (resp. L_∞). The primes $v_1, \dots, v_t$ ramify in L/K. Furthermore, all the primes of K_n lying over $v_1, \dots, v_t$ must ramify in L_n as well. Since each v_i splits completely, there are tp^n such primes of K_n. Therefore, the number of primes of L_n/K_n that ramify is at least tp^n. Now set

$$t := N + md\ell(\ell - 1).$$

This proves property (1).

To prove property (2), we just count degrees in the above field diagram, noting that $[L_n : L] = dp^n$. This completes the proof of Proposition 3.1. ∎

4. Growth of class groups in L_∞/L: the proof of Theorem 1.8. We want to show that the ℓ-part of the class group in the Γ-extension L_∞/L is unbounded. Our main tool to do this is the so-called *ambiguous class number formula*.

Definition 4.1. Let ℓ be a prime. Let K be a number field and L/K be a cyclic $\mathbb{Z}/\ell\mathbb{Z}$-extension. Let $\sigma \in \mathrm{Gal}(L/K)$ be a generator. An ideal class $[\mathfrak{a}] \in \mathrm{Cl}(L)$ is called *strongly ambiguous* if $[\mathfrak{a}]^{\sigma-1} = (1)$.

The subgroup of $\mathrm{Cl}(L)$ consisting of strongly ambiguous classes is denoted by $\mathrm{Am}_{\mathrm{st}}(L/K)$.

The following is given in [Kun20, Proposition 4.5].

Proposition 4.2 (Ambiguous class number formula). *Let ℓ be a prime. Let K be a number field and L/K be a cyclic $\mathbb{Z}/\ell\mathbb{Z}$-extension such that σ is a generator of the Galois group* $\mathrm{Gal}(L/K)$. *Then*

$$r_\ell(\mathrm{Am}_{\mathrm{st}}(L/K)) \geq T - [L : \mathbb{Q}],$$

where T is the number of ramified primes in L/K.

Proof of Theorem 1.8. Observe that for each $n \geq 1$, the extension L_n/K_n is cyclic of degree ℓ. Applying Proposition 4.2 to L_n/K_n, we have

$$r_\ell(\mathrm{Am}_{\mathrm{st}}(L_n/K_n)) \geq T - [L_n : \mathbb{Q}],$$

and the number of primes ramifying in L_n/K_n is at least

$$(N + 2d\ell(\ell-1))p^n.$$

We have $[L_n : \mathbb{Q}] \geq m\ell(\ell-1)dp^n$ for all $n \geq 0$.

By Proposition 3.1(2), we have $T \geq (N + md\ell(\ell-1))p^n$ and $[L_n : \mathbb{Q}] \geq md\ell(\ell-1)p^n$. And since $\mathrm{Am}_{\mathrm{st}}(L_n/K_n)$ is a subgroup of $\mathrm{Cl}(L_n)$, we have

$$r_\ell(\mathrm{Cl}(L_n)) \geq r_\ell(\mathrm{Am}_{\mathrm{st}}(L_n/K_n)).$$

Combining these, we obtain

$$\begin{aligned} r_\ell(\mathrm{Cl}(L_n)) &\geq r_\ell(\mathrm{Am}_{\mathrm{st}}(L_n/K_n)) \geq T - [L_n : \mathbb{Q}] \\ &\geq (N + md\ell(\ell-1))p^n - md\ell(\ell-1)p^n = Np^n \end{aligned}$$

for all $n \geq 0$. This completes the proof of Theorem 1.8. ∎

5. Application to fine Selmer groups: the proof of Theorems 1.6

5.1. Review of fine Selmer group. Let F be a number field and p be a prime. Let A be an abelian variety over F and let S be a finite set of primes containing $S_p \cup S_{\mathrm{bad}} \cup S_\infty$. Denote by F_S the maximal extension of F unramified outside S.

The usual p^∞-*Selmer group* of A is defined by

$$\mathrm{Sel}_{p^\infty}(A/F) = \ker\Big(\sum H^1(F, A[p^\infty]) \to \prod_v H^1(F_v, A)[p^\infty]\Big).$$

Here v runs through all the primes of F. The *fine Selmer group* of A is defined by the exact sequence

$$0 \to R_{p^\infty}(A/F) \to \mathrm{Sel}_{p^\infty}(A/F) \to \bigoplus_{v|p} A(F_v) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p.$$

5.2. Proof of Theorem 1.6. Let F be a number field and S a finite set of places of F. The *S-class group* of F, denoted $\mathrm{Cl}_S(F)$, is the quotient of $\mathrm{Cl}(F)$ by the subgroup generated by the ideal classes of prime ideals in S. The following proposition is proven in [LM16, Lemma 4.3].

Proposition 5.1. *Let A be an abelian variety over a number field F. Let S be a finite set of primes containing $S_\ell \cup S_{\mathrm{bad}} \cup S_\infty$. Suppose that $A(F)[\ell] \neq 0$. Then*

$$r_\ell(R_{\ell^\infty}(A/F)) \geq r_\ell(\mathrm{Cl}_S(F)) \cdot r_\ell(A(F)[\ell]) - 2\dim(A),$$

where $\dim(A)$ *denotes the dimension of the abelian variety A.*

We will first relate the S-class group of F to the class group of F.

LEMMA 5.2. *Let L be a number field and let ℓ be a rational prime. Let S be a finite set of places of L containing the primes above ℓ. Let s_0 be the number of finite primes in S. Then for all n,*

$$|r_\ell(\mathrm{Cl}(L_n)) - r_\ell(\mathrm{Cl}_S(L_n))| \geq 2s_0\ell^n.$$

Proof. We reproduce this proof from [Kun20, Lemma 4.6, Step A]. Let s_n be the number of finite primes of L_n lying over a prime of S. Consider the following short exact sequence for all n [NSW13, Lemma 10.3.12]:

$$\mathbb{Z}^{s_0} \to \mathrm{Cl}(L_n) \to \mathrm{Cl}_S(L_n).$$

Taking ℓ-ranks of this sequence, by [LM16, Lemma 3.2] we obtain

$$|r_\ell(\mathrm{Cl}(L_n)) - r_\ell(\mathrm{Cl}_S(L_n))| \geq 2s_0\ell^n. \quad \blacksquare$$

Proof of Theorem 1.6. Recall that we have primes $\ell \neq p$ and an abelian variety A defined over $\mathbb{Q}(\zeta_\ell)$. Let $S = S_p \cup S_{\mathrm{bad}} \cup S_\infty$. Let s_0 be the number of finite places of S. We can apply Theorem 1.8 (replacing N with $N + 2s_0$) to construct a Γ-extension L_∞/L such that

$$r_\ell(\mathrm{Cl}(L_n)) \geq (N + 2s_0)p^n$$

for all $n \geq 0$. Proposition 5.1 tells us that for all $n \geq 0$,

$$r_\ell(R_{\ell^\infty}(A/L_n)) \geq r_\ell(\mathrm{Cl}_S(L_n)) \cdot r_\ell(A(L_n)[\ell]) - 2\dim(A).$$

Since we have assumed $A(\zeta_\ell)[\ell] \neq 0$, it follows that $r_\ell(A(L_n)[\ell]) \geq 1$ for all $n \geq 1$. This gives us

$$r_\ell(R_{\ell^\infty}(A/L_n)) \geq r_\ell(\mathrm{Cl}_S(L_n)) - 2\dim(A).$$

Applying Lemma 5.2, we get

$$r_\ell(R_{\ell^\infty}(A/L_n)) \geq (r_\ell(\mathrm{Cl}(L_n)) - 2s_0\ell^n) - 2d \geq N + 2s_0p^n - 2s_0\ell^n - 2\dim(A).$$

Suppose $\ell < p$. Then we have

$$r_\ell(R_{\ell^\infty}(A/L_n)) \geq N + 2s_0\ell^n - 2s_0\ell^n - 2d = N\ell^n - 2\dim(A).$$

Now suppose $\ell > p$. Then

$$r_\ell(R_{\ell^\infty}(A/L_n)) \geq N + 2s_0p^n - 2s_0p^n - 2d = Np^n - 2\dim(A).$$

Either way, we get

$$r_\ell(R_{\ell^\infty}(A/L_n)) \geq Nq^n - 2\dim(A) \geq Nq^n,$$

where $q = \min\{\ell, p\}$. This completes the proof of Theorem 1.6. $\blacksquare$

6. Examples

EXAMPLE 1. Let $E = 11a1$. Then $E(\mathbb{Q}(\zeta_5))[5] \neq 0$, so we can pick $\ell = 5$ and $p = 3$. Let $N = 2$. We will construct a $\Gamma = \mathbb{Z}_3$-extension L_∞/L such that

$$r_5(R_{5^\infty}(E/L_n)) \geq 2 \cdot 3^n \quad \text{for all } n \geq 0.$$

We pick $K = \mathbb{Q}(\zeta_3)$ because there is a unique prime of F lying over $p = 3$. Let K_∞/K be the anticyclotomic $\mathbb{Z}_3$-extension of K. We have $t = N + 2d\ell(\ell-1) = 42$. We want to find $t = 42$ primes $v_1, \ldots, v_t$ of F that split completely in K_∞. It is enough to find 42 primes different from $p = 3$ that are inert in $\mathbb{Q}(\zeta_3)$. We list these primes below:

$2, 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101, 107, 113, 131, 137, 149, 167, 173, 179, 191,$
$197, 227, 233, 239, 251, 257, 263, 269, 281, 293, 311, 317, 347, 353, 359, 383, 389, 401, 419.$

Let α be the product of these 42 primes,

$$\alpha = 5564821300878169567266781038470220470547296829866818046142810483994789051955010075838675 10.$$

Now put $L = K(\zeta_5, \sqrt[5]{\alpha})$, and let $L_\infty = K_\infty L$. Then L_∞/L is a $\mathbb{Z}_3$-extension. Theorem 1.8 says that

$$r_5(\mathrm{Cl}(L_n)) \geq 2 \cdot 3^n \quad \text{for all } n \geq 0.$$

And Theorem 1.4 says that

$$r_5(R_{5\infty}(E/L_n)) \geq 2 \cdot 3^n \quad \text{for all } n \geq 0.$$

Example 2. We now look at $\mathbb{Z}_p^d$-extensions for $d = 3$. As in the previous example, let $E = 11a1$, $\ell = 5$ and $p = 3$. Set $N = 10$. We will construct a $\mathbb{Z}_3^3$-extension L_∞/L such that

$$r_\ell(R_{\ell\infty}(E/L_n)) \geq 10 \cdot 3^n \quad \text{for all } n \geq 0.$$

Consider the CM field $K = \mathbb{Q}(\zeta_9)$. Let K_∞ be the $\mathbb{Z}_3^3$-extension of K given in Proposition 2.1. We have $t = N + 2d\ell(\ell-1) = 90$. We want to find $t = 90$ primes $v_1, \ldots, v_t$ that are inert in K. By the well-known splitting laws for primes in cyclotomic fields, every rational prime which is $\equiv 2, 5$ modulo 9 is inert in K. Here is a list of 90 such primes:

$2, 5, 11, 23, 29, 41, 47, 59, 83, 101, 113, 131, 137, 149, 167, 173, 191, 227, 239, 257, 263, 281,$
$293, 311, 317, 347, 353, 383, 389, 401, 419, 443, 461, 479, 491, 509, 563, 569, 587, 599, 617, 641,$
$653, 659, 677, 743, 761, 797, 821, 839, 857, 887, 911, 929, 941, 947, 977, 983, 1013, 1019, 1031,$
$1049, 1091, 1103, 1109, 1163, 1181, 1193, 1217, 1229, 1283, 1289, 1301, 1307, 1319, 1361,$
$1373, 1409, 1427, 1433, 1451, 1481, 1487, 1499, 1523, 1553, 1559, 1571, 1607, 1613.$

Let α be the product of these primes:

$$\alpha = 3026691567190856771201105872323454284465474656097714712640878306872219738 23946203120683121105279988012699117394288474908858414443287091308966386167902242957859532761609270923483095428112544069874627622945451584053107032 9013191741865236750170.$$

Now put $L = K(\zeta_5, \sqrt[5]{\alpha})$ and let $L_\infty = K_\infty L$. Then L_∞/L is a $\mathbb{Z}_3^2$-extension. Theorem 1.8 says that

$$r_5(\mathrm{Cl}(L_n)) \geq 10 \cdot 3^n \quad \text{for all } n \geq 0.$$

And Theorem 1.6 says that

$$r_5(R_{5^\infty}(E/L_n)) \geq 10 \cdot 3^n \quad \text{for all } n \geq 0.$$

Example 3. We discuss a non-commutative example of Γ. The nilpotent uniform groups of dimension $d = 3$ are parametrized, up to isomorphism, by a number $s \in \mathbb{N}$. They are given by (see [GSK09, Section 7, Theorem 7.4])

$$\Gamma(s) = \langle x, y, z : [x, z] = [y, z] = 1,\ [x, y] = z^{p^s} \rangle.$$

The groups $\Gamma(s)$ are non-abelian; they fit in the exact sequence

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

If $p \equiv 1$ modulo 3, the group $\Gamma(1)$ has an automorphism τ of order 3 which has no fixed points (see [HM19, Proposition 4.1]). Therefore $m = 3$.

Put $\Gamma = \Gamma(1)$. Let $E = 19a1$. Since $E(\mathbb{Q})[3] \neq 0$, let $\ell = 3$, and $p = 7$. Let $N = 6$. We will construct a Γ-extension L_∞/L such that

$$r_5(R_{5^\infty}(E/L_n)) \geq 6 \cdot 3^n \quad \text{for all } n \geq 0.$$

We construct a degree $m = 3$ extension F/F_0 as in Assumption 1. Let $F_0 = \mathbb{Q}(\zeta_7)$. Let $F = F_0(\theta)$, where θ is a root of the irreducible cubic polynomial

$$x^3 - x^2 - 4x - 1.$$

Then F/F_0 is a degree 3 cyclic extension. According to the LMFDB database [LMF23], the class number of F is 13 and there is a unique prime $\mathfrak{p}$ lying over $p = 7$. In particular, the p-part of the $\mathfrak{p}$-class group of F is trivial so F is p-rational. Therefore, F/F_0 satisfies the hypotheses of Proposition 3.1.

Set $t := N + md\ell(\ell-1) = 6+3\cdot 3\cdot 3\cdot 2 = 60$. We need to find 60 primes of $F_0 = \mathbb{Q}(\zeta_7)$ which are inert in F. Consider the following 10 rational primes:

$$43, 127, 491, 673, 953, 1499, 1583, 2129, 2311, 2591. \tag{1}$$

By a calculation in Sage, each of these 10 rational primes splits completely in F_0 into 6 factors and each of these factors is inert in F. For example, 43 factors in F_0 as

$$\begin{aligned} 43 = {} & (\zeta_7^5 + 2\zeta_7^3 + \zeta_7^2 + 1) \cdot (\zeta_7^5 + \zeta_7^4 + 2\zeta_7^2 + \zeta_7) \\ & \cdot (2\zeta_7^5 + \zeta_7^4 + 2\zeta_7^3 + \zeta_7^2 + 2\zeta_7 + 1) \cdot (-2\zeta_7^5 - \zeta_7^4 - \zeta_7^3 - 2\zeta_7^2 - 2\zeta_7 - 1) \\ & \cdot (2\zeta_7^4 + \zeta_7^3 + \zeta_7^2 + \zeta_7) \cdot (\zeta_7^5 + \zeta_7^4 + \zeta_7^3 + 2\zeta_7^2), \end{aligned}$$

and each of the factors is inert in F. In total, there are $10 \cdot 6 = 60$ primes of F_0 lying over the 10 rational primes (1), each of which is inert in F.

Let α be the product of these 60 primes:

$$\begin{aligned} \alpha = {} & 784025037792166554050235760891167382653206060626833429989912309772985 94 \\ & 366840200239211889414161610945783214748072276266387591561420797021082 39 \\ & 313497652801991067685041337071171617321114788409671453358754013644971. \end{aligned}$$

We apply Lemma 2.4. Since $[F_0 : \mathbb{Q}] = 6 \geq 2d$, we set $n = 0$, so that $K_0 = F_0$ and $K = F$. The lemma says that there exists a Γ-extension K_∞/K such that every inert prime in K/K_0 splits completely in K_∞.

Put $L = K(\alpha^{1/3}, \zeta_3)$ and $L_\infty = LK_\infty$. Then L_∞/L is a Γ-extension. Theorem 1.8 says that

$$r_5(\mathrm{Cl}(L_n)) \geq 6 \cdot 3^n \quad \text{for all } n \geq 0.$$

And Theorem 1.6 says that

$$r_5(R_{5^\infty}(E/L_n)) \geq 6 \cdot 3^n \quad \text{for all } n \geq 0.$$

Acknowledgements. I want to thank Debanjana Kundu for guiding me through my first steps in Iwasawa theory, and also for suggesting this problem to me. This paper would not have been possible without your support, so thank you! I would also like to thank Professor Kumar Murty and members of the GANITA lab for patiently listening to me present the proofs in this paper. Finally, I thank the anonymous referee for their comments which greatly improved the paper's content and exposition.

References

[CS05] J. Coates and R. Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. 331 (2005), 809–839.

[GSK09] J. Gonzálo-Sánchez and B. Klopsch, *Analytic pro-p groups of small dimensions*, J. Group Theory 12 (2009), 711–734.

[Gra] G. Gras, *Class Field Theory: From Theory to Practice*, Springer, 2003.

[HM19] F. Hajir and C. Maire, *Prime decomposition and the Iwasawa MU-invariant*, Math. Proc. Cambridge Philos. Soc. 166 (2019), 599–617.

[Iwa59] K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. 65 (1959), 183–226.

[Iwa73] K. Iwasawa, *On the μ-invariants of $\mathbb{Z}_\ell$-extensions*, in: Number Theory, Algebraic Geometry and Commutative Algebra, Kinokuniya, 1973, 1–11.

[Kun20] D. Kundu, *Growth of fine Selmer groups in infinite towers*, Canad. Math. Bull. 63 (2020), 921–936.

[KL23] D. Kundu and A. Lei, *Growth of p-parts of ideal class groups and fine Selmer groups in $\mathbb{Z}_q$-extensions with $p \neq q$*, Acta Arith. 207 (2023), 297–313.

[LM16] M. F. Lim and V. K. Murty, *The growth of fine Selmer groups*, J. Ramanujan Math. Soc. 31 (2016), 79–94.

[LMF23] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, https://www.lmfdb.org/NumberField/18.0.110609092182866440454328583.1, 2023.

[Lon12] M. Longo, *Anticyclotomic Iwasawa's Main Conjecture for Hilbert modular forms*, Comment. Math. Helv. 87 (2012), 303–353.

[Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. 18 (1972), 183–266.

[Nek07] J. Nekovář, *The Euler system method for CM points on Shimura curves*, in: *L*-Functions and Galois Representations, London Math. Soc. Lecture Note Ser. 320, Cambridge Univ. Press, 2007, 471–547.

[NSW13] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Grundlehren Math. Wiss. 323, Springer, 2013.

[PR93] B. Perrin-Riou, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble) 43 (1993), 945–995.

[PR95] B. Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques*, Astérisque 229 (1995), 198 pp.

[RZ00] L. Ribes and P. Zalesskii, *Profinite Groups*, Ergeb. Math. Grenzgeb. (3) 40, Springer, 2000.

[Rub00] K. Rubin, *Euler Systems*, Ann. of Math. Stud. 147, Princeton Univ. Press, 2000.

[Was75] L. C. Washington, *Class numbers and $\mathbb{Z}_p$-extensions*, Math. Ann. 214 (1975), 177–193.

[Was78] L. C. Washington, *The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension*, Invent. Math. 49 (1978), 87–97.

Adithya Chakravarthy
University of Toronto
Toronto, ON, M5S 2E4, Canada
E-mail: adithyachakra21@gmail.com