GROWTH OF p-FINE SELMER GROUPS AND p-FINE SHAFAREVICH-TATE GROUPS IN $\mathbb{Z}/p\mathbb{Z}$ EXTENSIONS

DEBANJANA KUNDU

Abstract. In this paper we investigate the growth of the p-rank of the fine Selmer group and the fine Shafarevich-Tate group. In particular, we show that the p-fine Selmer Group and the p-fine Shafarevich-Tate group can become unbounded as we vary over all $\mathbb{Z}/p\mathbb{Z}$ extensions of a given number field, K.

1. Introduction

Using genus theory, Gauss proved that the 2-torsion of the ideal class group of a quadratic number field can be arbitrarily large. There is a known analogy between the growth of ideal class groups and growth of Selmer groups of Abelian varieties. This question was studied in detail in [Česl5]. If p is a fixed prime, it is a folklore result that the p-torsion of the ideal class group can become unbounded in $\mathbb{Z}/p\mathbb{Z}$ extensions of a fixed number field. In [Čes17], Česnavičius proved that the p-Selmer group can be arbitrarily large when one varies over all $\mathbb{Z}/p\mathbb{Z}$-extensions of a global field.

In [CS05], Coates and Sujatha initiated the study of a subgroup of the Selmer group called the fine Selmer group. They showed that the fine Selmer group approximates the ideal class group better than the classical Selmer group. This was made more precise in [LM16]. They proved that the p^∞-fine Selmer group of an Abelian variety has unbounded growth on varying over all $\mathbb{Z}/p\mathbb{Z}$-extensions of a fixed number field.

Using methods similar to [LM16], it is possible to show that the p-fine Selmer group of an Abelian variety has unbounded growth as one varies over $\mathbb{Z}/p\mathbb{Z}$ extensions of a fixed number field. This is recorded in Proposition 4.2. Using this method of proof, we find effective estimates on the conductor of such a $\mathbb{Z}/p\mathbb{Z}$-extension. As per the knowledge of the author, such bounds can not be obtained by the method of proof in [Čes17].

These results will imply the results of Lim-Murty and also of Česnavičius (for the number field case). Indeed, this is because the p-fine Selmer group is contained in the p^∞-fine Selmer group and is a subgroup of the p-Selmer group.

In [CS10], Clark and Sharif have proven that the p-torsion of the classical Shafarevich-Tate group of an elliptic curve has unbounded growth in $\mathbb{Z}/p\mathbb{Z}$-extensions of a fixed number field. Just like the fine Selmer group, one can define a fine analogue of the classical Shafarevich-Tate group. These objects were defined and studied in [Wut07]. Lim-Murty asked the natural question whether the p-fine

Date: October 9, 2019.
2010 *Mathematics Subject Classification.* Primary 11R23.
Key words and phrases. Iwasawa Theory, Fine Selmer groups, Class groups, p-rank.

Shafarevich-Tate group has unbounded growth in $\mathbb{Z}/p\mathbb{Z}$-extensions. Using the unboundedness result of Clark-Sharif, we provide an affirmative answer to their question, for the case of elliptic curves in Theorem 5.3. It would be interesting to give an independent proof of this theorem.

For a fixed number field K, we don't know at present how to show that the p-fine Selmer group has unbounded growth as one varies over all $\mathbb{Z}/n\mathbb{Z}$-extensions of K where $1 < n < p$. Analogous results are conjectured to be true for the p-torsion of the ideal class group. It is conjectured that such a result should be true for $n = 2$.

2. Preliminaries

Let K be a fixed number field and p be an odd rational prime. Let A be an Abelian variety defined over K of dimension, d. Let S be a finite set of primes of K including the infinite primes, the primes where A has bad reduction and the primes above p. Fix an algebraic closure $\overline{K}/K$ and denote the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ by G_K. Use the notation K_S for the maximal subfield of $\overline{K}$ containing K which is unramified outside S. Write $G_S(K) = \mathrm{Gal}(K_S/K)$.

The p^k-Selmer group of an Abelian variety is defined as,

$$\mathrm{Sel}_{p^k}(A/K) = \ker\left(H^1(G_S(K), A[p^k]) \to \bigoplus_{v\in S} H^1(K_v, A)[p^k]\right)$$

Here, $H^*(K_v, M)$ is the Galois cohomology of the decomposition group at v for any G-module, M.

The p^k-fine Selmer group is defined as

$$R^S_{p^k}(A/K) = \ker\left(H^1(G_S(K), A[p^k]) \to \bigoplus_{v\in S} H^1(K_v, A[p^k])\right).$$

For any number field K, one has the following exact sequence

$$0 \to R^S_{p^k}(A/K) \to \mathrm{Sel}_{p^k}(A/K) \to \bigoplus_{v\in S} H^1(K_v, A[p^k]). \tag{1}$$

Consider the limit versions of the above defined objects. Define

$$\mathrm{Sel}_{p^\infty}(A/K) := \varinjlim \mathrm{Sel}_{p^k}(A/K) = \ker\left(H^1(G_S(K), A[p^\infty]) \to \bigoplus_{v\in S} H^1(K_v, A)[p^\infty]\right)$$

where the limit is with respect to maps induced by the inclusions $A[p^k] \hookrightarrow A[p^{k+1}]$. It has a subgroup, the discrete fine Selmer group

$$R_{p^\infty}(A/K) := \varinjlim R^S_{p^k}(A/K).$$

Note $R_{p^\infty}(A/K)$ is independent of S. This follows from the short exact sequence

$$0 \to R_{p^\infty}(A/K) \to \mathrm{Sel}_{p^\infty}(A/K) \to \bigoplus_{v|p} A(K_v)\otimes \mathbb{Q}_p/\mathbb{Z}_p$$

upon noting that $A(K_v)\otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ for $v \nmid p$. However, $R^S_p(A/K)$ is not.

For the classical Selmer group, one has the short exact sequence

$$0 \to A(K)/p^k \to \mathrm{Sel}_{p^k}(A/K) \to Ш(A/K)[p^k] \to 0$$

where $A(K)$ is the Mordell-Weil group. In [Wut07], a fine subgroup of the Mordell-Weil group is defined; it is the following kernel

$$0 \to M_{p^k}(A/K) \to A(K)/p^k \to \bigoplus_{v|p} A(K_v)/p^k.$$

It is now natural to define the fine Shafarevich-Tate group by the exact sequence,

$$0 \to M_{p^k}(A/K) \to R^S_{p^k}(A/K) \to \text{Ж}_{p^k}(A/K) \to 0.$$

One can view $\text{Ж}_{p^k}(A/K)$ as a subgroup of $\text{Ш}(A/K)[p^k]$. To see this we repeat the argument in [Wut07, Page 3]. Consider the following diagram

$$\begin{tikzcd}
0 \arrow[r] & A(K)/p^k \arrow[r] \arrow[d] & \mathrm{Sel}_{p^k}(A/K) \arrow[r] \arrow[d] & \text{Ш}(A/K)[p^k] \arrow[r] \arrow[d, "0"] & 0 \\
0 \arrow[r] & \bigoplus_{v|p} A(K_v)/p^k \arrow[r] & \bigoplus_{v|p} H^1(K_v, A[p^k]) \arrow[r] & \bigoplus_{v|p} H^1(K_v, A)[p^k] \arrow[r] & 0
\end{tikzcd}$$

From the above diagram, by an application of the snake lemma, one obtains the following exact sequence

$$0 \to M_{p^k}(A/K) \to R^S_{p^k}(A/K) \to \text{Ш}(A/K)[p^k] \to C_{p^k}$$

where C_{p^k} is the cokernel of the left vertical map in the above diagram. Thus, $\text{Ж}_{p^k}(A/K)$ is a subgroup of $\text{Ш}(A/K)[p^k]$ with quotient in C_{p^k}.

3. p-rank

For an Abelian group, G, define its p-rank, $r_p(G)$, as $\dim_{\mathbb{Z}/p\mathbb{Z}} G[p]$. When G is a pro-p group, use the notation $h_i(G) = r_p(H^i(G, \mathbb{Z}/p\mathbb{Z}))$.

We start by recording an estimate of the p-rank of the first cohomology group.

Lemma 3.1. *[LM15, Lemma 3.2] Let G be a pro-p group, and M be a discrete G-module cofinitely generated over $\mathbb{Z}_p$. If $h_1(G)$ is finite, then $r_p(H^1(G, M))$ is finite and*

$$\begin{aligned} h_1(G) r_p(M^G) - r_p((M/M^G)^G) &\le r_p(H^1(G, M)) \\ &\le h_1(G)(\mathrm{corank}_{\mathbb{Z}_p}(M) + \log_p |M/M_{\mathrm{div}}|) \end{aligned}$$

Moreover, when M is a trivial G-module,

$$r_p(H^1(G, M)) = h_1(G) r_p(M).$$

Denote the p-Hilbert S-class field of K by $H_S(K)$ or even H_S. It is the maximal Abelian unramified p-extension of K in which all primes in S split completely.

In the following lemma we give a lower bound for the p-rank of p-fine Selmer group in terms of the p-rank of the S-class group.

Lemma 3.2. *Let A be an Abelian variety of dimension, d, defined over a number field K. Let S be a finite set of primes of K including the infinite primes, the primes where A has bad reduction and the primes above p. Suppose $A(K)[p] \neq 0$. Then*

$$r_p(R^S_p(A/K)) \ge r_p(\mathrm{Cl}_S(K)) r_p(A(K)[p]) - 2d.$$

Proof. Consider the following diagram with exact rows.

$$\begin{array}{ccccccc}
0 & \longrightarrow & R_p^S(A/K) & \longrightarrow & H^1(G_S(K), A[p]) & \longrightarrow & \bigoplus_{v\in S} H^1(K_v, A[p]) \\
 & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\
0 & \longrightarrow & R_p^S(A/H_S) & \longrightarrow & H^1(G_S(H_S), A[p]) & \longrightarrow & \bigoplus_{v\in S}\bigoplus_{w\mid v} H^1(H_{S,w}, A[p])
\end{array}$$

The vertical maps are given by restriction maps. Write $\gamma = \oplus_v \gamma_v$ with

$$\gamma_v : H^1(K_v, A[p]) \to \bigoplus_{w\mid v} H^1(H_{S,w}, A[p]).$$

From the inflation-restriction sequence one gets that $\ker \gamma_v = H^1(G_v, A[p])$ where G_v is the decomposition group of $\mathrm{Gal}(H_S/K)$ at v. By the definition of the p-Hilbert S-class field, all the primes of K in S split completely in H_S and hence $G_v = 1$. This forces $\ker\gamma$ to be trivial.

The inflation-restriction sequence also gives $\ker\beta = H^1\left(\mathrm{Gal}(H_S/K), A(H_S)[p]\right)$. This gives the injection

$$H^1(\mathrm{Gal}(H_S/K), A(H_S)[p]) \hookrightarrow R_p^S(A/K).$$

This implies

$$r_p\left(R_p^S(A/K)\right) \geq r_p\left(H^1(\mathrm{Gal}(H_S/K), A(H_S)[p])\right).$$

Lemma 3.1 implies that

$$r_p\left(H^1(\mathrm{Gal}(H_S/K), A(H_S)[p])\right) \geq h_1(\mathrm{Gal}(H_S)/K) r_p(A(K)[p]) - 2d.$$

From class field theory, $\mathrm{Gal}(H_S/K) \simeq \mathrm{Cl}_S(K)$. The result follows since the class group (and hence the S-class group) is always finite; thus

$$h_1\left(\mathrm{Gal}(H_S/K)\right) = r_p\left(\mathrm{Cl}_S(K)\right).$$

□

Remark 3.3. Under the slightly stronger assumption that $A[p] \subseteq A(K)$, we can get better estimates. This assumption forces $A[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{2d}$ as $G_S(K)$-modules. Now, $G_S(K)$ acts trivially on $A[p]$ and hence we have

$$H^1(G_S(K), A[p]) = \mathrm{Hom}(G_S(K), A[p]).$$

We have similar equalities for the local cohomology groups as well. Thus,

$$R_p^S(A/K) = \mathrm{Hom}(\mathrm{Cl}_S(K), A[p]) \simeq \mathrm{Cl}_S(K)[p]^{2d}$$

as Abelian groups. Therefore

$$r_p(R_p^S(A/K)) = 2d r_p(\mathrm{Cl}_S(K)).$$

4. Unboundedness of p-fine Selmer groups in $\mathbb{Z}/p\mathbb{Z}$-extensions

In this section, we first improve upon a result of [LM16]. Recall the Grunwald-Wang theorem (cf Theorem 9.2.8 and the remark following it in [NSW08]).

Theorem. *Let S be a finite set of primes of a global field K and let G be a finite Abelian group. For all $\mathfrak{p} \in S$, let the finite Abelian extensions $\mathcal{K}_\mathfrak{p} \mid K_\mathfrak{p}$ be given such that* $\mathrm{Gal}(\mathcal{K}_\mathfrak{p} \mid K_\mathfrak{p})$ *may be embedded into G. Then there exists a global Abelian extension $\mathcal{K} \mid K$ with Galois group G such that $\mathcal{K}$ has the given completions $\mathcal{K}_\mathfrak{p}$ for all $\mathfrak{p} \in S$.*

The following proposition is proved in [LM16]. We repeat the proof here because it plays a crucial role in proving our main result.

Proposition 4.1. *[LM16, Proposition 6.1] Let S be a finite set of primes of K containing the Archimedean primes. Then there exists a sequence $\{L_n\}$ of distinct number fields such that each L_n is a $\mathbb{Z}/p\mathbb{Z}$ extension of K and such that for every $n \geq 1$,*

$$r_p(\mathrm{Cl}_S(L_n)) \geq n.$$

Proof. Set r_1 and r_2 to denote the number of real and the number of pairs of complex places of K. Let S_1 be a set of primes of K containing S such that

$$|S_1| = |S| + r_1 + r_2 + \delta + 1$$

where $\delta = 1$ if K contains a primitive p-root of unity, and is 0 otherwise.

By the Grunwald-Wang theorem, there exists a $\mathbb{Z}/p\mathbb{Z}$ extension L_1/K such that it is ramified at all finite places of S_1 and is unramified outside of it. Using [NSW08, Proposition 10.10.3],

$$r_p(\mathrm{Cl}_S(L_1)) \geq |S_1| - |S| - r_1 - r_2 - \delta = 1.$$

Repeat the above process; choose a set S_2 containing S_1 with the property

$$|S_2| = |S_1| + 1 = |S| + r_1 + r_2 + \delta + 2.$$

By Grunwald-Wang theorem, there exists a $\mathbb{Z}/p\mathbb{Z}$-extension L_2/Kramified at all the finite places of S_2 and unramified outside of it. L_2 is distinct from L_1 by construction. For this field,

$$r_p(\mathrm{Cl}_S(L_2)) \geq 2.$$

Since K has infinitely many primes, we can continue this process indefinitely. Each of the L_i's are distinct by construction. This proves the proposition. ☐

The above proposition combined with Lemma 3.2 proves the following improvement of [LM16, Theorem 6.2].

Proposition 4.2. *Let K be a number field and A be a d-dimensional Abelian variety defined over K. Let S be a finite set of primes of K including the infinite primes, the primes where A has bad reduction and the primes above p. Suppose $A(K)[p] \neq 0$. Then*

$$\sup\{r_p\left(R_p^S(A/L)\right) \mid L/K \textit{ is a cyclic extension of degree } p\} = \infty.$$

Here sup *is over the conductor of L/K.*

When $A(K)[p] = 0$, one gets a weaker statement.

Corollary 4.3. *Let K be a number field and A be an Abelian variety of dimension, d, defined over K. If $A(K)[p] = 0$, define*

$$m = \min\{[F : K] \mid A(F)[p] \neq 0\}.$$

Then

$$\sup\{r_p(R_p^S(A/L)) \mid L/K \textit{ is an extension of degree } pm\} = \infty.$$

Remark 4.4. In [LM16], it is shown that $m \leq p^{2d} - 1$.

In Proposition 4.2, we saw that the p-fine Selmer group of an Abelian variety, A defined over K becomes unbounded as we vary over all $\mathbb{Z}/p\mathbb{Z}$-extensions of K. The proof of Proposition 4.1 suggests that it should be possible to find an effective estimate on the conductor. Indeed, we can prove the following theorem.

Theorem 4.5. *Let A be an Abelian variety of dimension d, defined over a number field, K. Let S be a finite set of primes as defined above. Suppose $A(K)[p] \neq 0$. Given a non-negative integer N, there exists a $\mathbb{Z}/p\mathbb{Z}$ extension L/K with norm of the conductor, $N_{K/\mathbb{Q}}(\mathfrak{f}(L/K)) \sim \kappa^N$ where κ is a constant depending on S, A and K, such that $r_p(R_p^S(A/K)) \geq N$.*

When $K = \mathbb{Q}$, the notation simplifies considerably. We prove the above theorem in detail for the special case $K = \mathbb{Q}$.

Theorem 4.6. *Let A be an Abelian variety of dimension d defined over $\mathbb{Q}$. Let S be a finite set of primes containing the Archimedean primes, the primes above p, and the primes of bad reduction of A. Suppose $A(\mathbb{Q})[p] \neq 0$. Given a non-negative integer N, there exists a $\mathbb{Z}/p\mathbb{Z}$ extension $L/\mathbb{Q}$ of conductor $\mathfrak{f}(L/\mathbb{Q}) \sim \kappa^N$ where κ is a constant depending on S and A, such that $r_p(R_p^S(A/\mathbb{Q})) \geq N$.*

Proof. Let $L/\mathbb{Q}$ be a $\mathbb{Z}/p\mathbb{Z}$-extension and let P be the set of rational primes which ramify in L. Since $L/\mathbb{Q}$ is a Galois extension, there is a unique $\mathfrak{p}$ above p, if p is ramified in L. The conductor, $\mathfrak{f}(L/\mathbb{Q}) = \prod_{q \in P} \mathfrak{f}_q$ where

$$\mathfrak{f}_q = \begin{cases} q^{p-1}, & \text{when } (q,p) = 1 \\ p^{p-1+\mathfrak{s}_{\mathfrak{p}|p}}, & \text{otherwise.} \end{cases}$$

Here, $1 \leq \mathfrak{s}_{\mathfrak{p}|p} \leq \mathrm{val}_{\mathfrak{p}}(p) = p$. The first case is called tame ramification, and the second is the case of wild ramification.

Taking natural log,

$$\log(\mathfrak{f}(L/\mathbb{Q})) = (p-1) \sum_{q \in P} \log q + \mathfrak{s}_{\mathfrak{p}|p} \log p. \tag{2}$$

The goal is to find the minimal conductor of L for which $r_p(R_p^S(A/L))$ is unbounded, i.e. $r_p(R_p^S(A/L)) \geq N$ for any given non-negative integer, N. From Lemma 3.2, it is enough to find a $\mathbb{Z}/p\mathbb{Z}$-extension $L_{n(N)}/\mathbb{Q}$ such that

$$r_p(\mathrm{Cl}_S(L_n)) \geq \frac{2d + N}{r_p(A(L_n)[p])} =: n(N) = n.$$

Note that $r_p(A(L_n)[p])$ is a positive constant, less than or equal to $2d$.

Let $S = \{v_1, \dots, v_k\} \cup S_\infty$ be the finite set of primes containing the Archimedean primes, the primes above p, and the primes of bad reduction of A. We construct S_n as in the proof of Proposition 4.1. Here, $r_1 = 1$, $r_2 = 0$ and $\delta = 0$. Therefore we must choose S_n such that $|S_n| = |S| + 1 + n$.

Define $M = \prod_{i=1}^k v_i$. Then $\log M \sim k \log k$. To construct S_n from the given set S, we need to add $n+1$ many primes. Choose the first prime $p_1 \nmid M$. By the Prime Number Theorem we know that we can find $p_1 \sim \log M$. Now choose $p_2 \nmid M p_1$; here $p_2 \sim \log(M \log M)$. We have $S \cup \{p_1, p_2\} = S_1$. We continue to choose, in the same way, as many primes as required to form S_n. Using Equation 2, as $n \to \infty$,

$$\log(\mathfrak{f}(L_n/K)) \sim (p-1) n \log \log M.$$

Equivalently, $\mathfrak{f}(L_n/\mathbb{Q}) \sim c^N$ with c a constant that depends on the given set S. By definition of $n(N)$, $\mathfrak{f}(L_{n(N)}/\mathbb{Q}) \sim \kappa^N$ for a constant κ that depends on S. $\square$

For proving the general case, the computation is similar. We point out some similarities and differences one needs to keep in mind. Consider the tower of number fields, $L \supset K \supset \mathbb{Q}$ where $[L : K] = p$. By hypothesis, L/K is Galois. If $\mathfrak{q} \mid q$ is a prime in K that ramifies in L, there will be a unique prime $\mathfrak{Q}|\mathfrak{q}$. The definition of the conductor carries through. But now, we are interested in the $N_{K/\mathbb{Q}}(\mathfrak{f}(L/K))$ so as to be able to do estimates. Define $M = \prod_i N(v_i)$ and construct S_n from S by adding $r_1 + r_2 + \delta + n$ many primes. Choose $p_1 \nmid M$ as before and the required element of S_n is $\mathfrak{p}_1 \mid p_1$. From here, the proof follows as before.

Remark 4.7. From Equation 1, $r_p\left(\mathrm{Sel}_p(A/K)\right) \geq r_p\left(R_p^S(A/K)\right)$. It follows that Theorem 4.5 holds if we replace $r_p(R_p^S(A/K)) \geq N$ by $r_p(\mathrm{Sel}_p(A/K)) \geq N$.

5. Unboundedness of the fine Shafarevich-Tate group in $\mathbb{Z}/p\mathbb{Z}$-extensions

In this section, we provide answers to the following question asked in [LM16].

Question. Let A be an Abelian variety defined over a number field K. Suppose $A(K)[p] \neq 0$. Is

$$\sup\{r_p\left(Ж_{p^\infty}(A/L)\right) \mid \ L/K \text{ is a cyclic extension of degree } p\} = \infty?$$

For elliptic curves, the answer to this question is precise. It is a corollary of results proved in [CS10] and [Wut07]. We record these previously known results.

Lemma 5.1. *[Wut07, Lemma 3.1] Let $v \mid p$ and $K_v/\mathbb{Q}_p$ be a finite extension of degree n_v. Then*

$$\#\left(E(K_v)/p^k\right) = p^{k\cdot n_v} \cdot \#\left(E(K_v)[p^k]\right).$$

The lemma follows from the observation that $E(K_v)$ has finite index in $\widehat{E}(\mathfrak{m}_v^a)$ where, $\widehat{E}$ stands for the formal group associated to E and $\mathfrak{m}_v^a$ is any power of the maximal ideal in the ring of integers in K_v. Therefore,

$$\frac{\#E(K_v)/p^k}{\#E(K_v)[p^k]} = \frac{\#\widehat{E}(\mathfrak{m}_v^a)/p^k}{\#\widehat{E}(\mathfrak{m}_v^a)[p^k]}.$$

For sufficiently large a, $\widehat{E}(\mathfrak{m}_v^a) \simeq \mathfrak{m}_v^a$ where the isomorphism is given by the formal logarithm (Theorem IV.6.4b, [Sil09]). The lemma follows since $\widehat{E}(\mathfrak{m}_v^a)[p^k] = 0$ and $\widehat{E}(\mathfrak{m}_v^a)/p^k = p^{k\cdot n_v}$.

Recall that the quotient of $Ш(E/K)[p^k]$ and $Ж_{p^k}(E/K)$ is contained in the cokernel of the map $E(K)/p \to \oplus_{v|p} E(K_v)/p^k$, denoted C_{p^k}. Lemma 5.1 shows that the codomain of this map has size bounded by $p^{k[K:\mathbb{Q}]} \prod_{v|p} \#E(K_v)[p^k]$. Thus,

Proposition 5.2. *[Wut07, Proposition 3.2] The index of $Ж_{p^k}(E/K)$ inside $Ш(E/K)[p^k]$ is bounded by*

$$[Ш(E/K)[p^k] : Ж_{p^k}(E/K)] \leq p^{k[K:\mathbb{Q}]} \prod_{v|p} \#E(K_v)[p^k] \tag{3}$$

The focus is once again on the case $k = 1$, ie the p-fine Shafarevich-Tate group. When E is an elliptic curve defined over a number field, K, and L/K is a degree p-extension, there are only finitely many $w|p$ in L. For each $w|p$, $\#E(L_w)[p]$ is finite and bounded [Sil09, Corollary III.6.4b]. Therefore, $\#\prod_{w|p} E(L_w)[p]$ is finite and bounded as we vary over all $\mathbb{Z}/p\mathbb{Z}$-extensions, L/K.

Theorem. *[CS10] Let E/K be an elliptic curve. Given M, for any positive integer r, there exists $\mathbb{Z}/p\mathbb{Z}$ field extensions L/K such that $Ш(E/L)$ contains at least r elements of order p i.e. there exists a $\mathbb{Z}/p\mathbb{Z}$ field extension L/K such that $Ш(E/L)[p]$ is greater than M.*

Combining the above two results we obtain a positive answer to the question.

Theorem 5.3. *Let E be an elliptic curve defined over the number field K. Varying over all $\mathbb{Z}/p\mathbb{Z}$-extensions L/K, for which $E(L)[p] \neq 0$, $Ӿ_p(E/L)$ is unbounded.*

Remark 5.4. In the case of elliptic curves, it appears that the question asked in [LM16] does not need the assumption $E(K)[p] \neq 0$.

In general, we know that $Ӿ_p(A/K)$ is a subgroup of $Ш(A/K)[p]$ with quotient in C_p. We have

$$\#C_p \leq \#A(K_v)/pA(K_v) \leq \#H^1(K_v, A[p]).$$

The right hand side of the inequality is finite and bounded [NSW08, Theorem 7.1.8(iii)]. It follows

Proposition 5.5. *Let A be an Abelian variety defined over the number field K. Varying over all $\mathbb{Z}/p\mathbb{Z}$-extensions, L/K, $Ӿ_p(A/L)$ is unbounded if and only if $Ш(A/L)[p]$ is unbounded.*

Remark 5.6.
(1) Theorem 5.3 is also seen to follow from Proposition 5.5 and the theorem of Clark-Sharif.
(2) In [Cre11], Creutz has proven results on the unboundedness of $Ш(A/L)[p]$.

Acknowledgement

The author thanks Kumar Murty for helpful discussions and his encouragement. Thanks are due to all members of the GANITA Lab for listening to the details over and over again. Much thanks also to Kęstutis Česnavičius for his comments on an earlier draft, and to Arul Shankar for answering innumerable questions on weekends when no one else was in the department.

References

[Čes15] Kęstutis Česnavičius. Selmer groups and class groups. *Compos. Math.*, 151(3):416–434, 2015.

[Čes17] Kęstutis Česnavičius. p-Selmer growth in extensions of degree p. *J. London Math. Soc.*, 95(3):833–852, 2017.

[Cre11] Brendan Creutz. Potential Sha for abelian varieties. *J. Number Theory*, 131(11):2162–2174, 2011.

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

[CS10] Pete L Clark and Shahed Sharif. Period, index and potential Sha. *Algebra & Number Theory*, 4(2):151–174, 2010.

[LM15] Meng Fai Lim and V Kumar Murty. Growth of Selmer groups of CM abelian varieties. *Canadian Journal of Mathematics*, 67(3):654–666, 2015.

[LM16] Meng Fai Lim and V Kumar Murty. The growth of fine Selmer groups. *J. Ramanujan Math. Society*, 31(1):79–94, 2016.

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

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[Wut07] Christian Wuthrich. The fine Tate–Shafarevich group. In *Math. Proc. Camb. Phil. Soc.*, volume 142, pages 1–12, 2007.

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