J. Ramanujan Math. Soc. **36,** No.1 (2021) 1–9

Growth of p-fine Selmer groups and p-fine Shafarevich-Tate groups in $\mathbb{Z}/p\mathbb{Z}$-extensions

Debanjana Kundu

Department of Mathematics, University of Toronto, 40 St. George Street, Toronto, ON, Canada M5S 2E4
email: dkundu@math.toronto.edu

Communicated by: Dr. Anupam Saikia

Received: February 27, 2020

Abstract. In this paper we show that the p-fine Selmer Group can become arbitrarily large as we vary over all $\mathbb{Z}/p\mathbb{Z}$ extensions of a given number field K and find effective estimates on the conductor of such a $\mathbb{Z}/p\mathbb{Z}$-extension. In fact, we show that the p-fine Shafarevich-Tate group can become arbitrarily large on varying over all $\mathbb{Z}/p\mathbb{Z}$ extensions of a given number field. We explore the close relationship in the size of p-fine Selmer groups and p-torsion of ideal class groups in quadratic extensions of number fields.

2000 Mathematics Subject Classification: 11R23.

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. For fixed prime p, it is a folklore result that the p-torsion of the ideal class group can become arbitrarily large in $\mathbb{Z}/p\mathbb{Z}$ extensions of a fixed number field. Varying over all $\mathbb{Z}/p\mathbb{Z}$-extensions of a global field, the p-Selmer group is also known to become arbitrarily large [1].

In [3], the study of the fine Selmer group was initiated. A key idea was to show that the fine Selmer group approximates the ideal class group better than the classical Selmer group. This was made more precise in [5]. Lim-Murty 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 this method of proof, we find effective estimates on the conductor of such a $\mathbb{Z}/p\mathbb{Z}$-extension (see Theorem 3.4). As per the knowledge of the author, such bounds can not be obtained by the method of proof in [1].

It is known 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 [2]. Just like the fine Selmer group, one can define a fine analogue of the classical Shafarevich-Tate group [11]. Lim-Murty asked the natural question whether the p-fine 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 4.5. It would be interesting to give an independent proof of this theorem.

For a fixed number field K, we don't know 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 for $1 < n < p$. Analogous results are conjectured to be true for the p-torsion of the ideal class group. It is believed that such a result should be true for $n = 2$. In Theorem 5.1, we prove these two conjectures are equivalent.

2. Preliminaries

Let K be a fixed number field and p be an odd rational prime. Let 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. 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

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

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

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

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 w.r.t maps induced by 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 that $R_{p^\infty}(A/K)$ is independent of S. 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 [11], 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 $Ш(A/K)[p^k]$. To see this we repeat the argument in [11, Page 3]. Consider the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(K)/p^k & \longrightarrow & \mathrm{Sel}_{p^k}(A/K) & \longrightarrow & Ш(A/K)[p^k] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow 0 & & \\
0 & \longrightarrow & \bigoplus_{v|p} A(K_v)/p^k & \longrightarrow & \bigoplus_{v|p} H^1(K_v, A[p^k]) & \longrightarrow & \bigoplus_{v|p} H^1(K_v, A)[p^k] & \longrightarrow & 0
\end{array}$$

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

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

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 $Ш(A/K)[p^k]$ with quotient in C_{p^k}.

2.1 p-rank

For an Abelian group G, define its p-rank, denoted by $r_p(G)$, as $\dim_{\mathbb{Z}/p\mathbb{Z}} G[p]$.

We record some elementary estimates.

Lemma 2.1 ([5, Lemma 3.2]). *Consider the following short exact sequence of cofinitely generated Abelian groups*

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

Then

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

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

The following lemma is a variant of [5, Lemma 4.3]. The proof is identical. It provides a lower bound for the p-rank of p-fine Selmer group in terms of the p-rank of the S-class group.

Lemma 2.2. *Let A/K be a d-dimensional Abelian variety. 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*

$$r_p(R_p^S(A/K)) \geq r_p(\mathrm{Cl}_S(K))r_p(A(K)[p]) - 2d.$$

Remark 2.3. 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 (see [5, Page 87] or [3, Lemma 3.8] or [9, 6.1]). Therefore

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

3. Unboundedness of p-fine Selmer groups in $\mathbb{Z}/p\mathbb{Z}$-extensions and effective estimates

Recall the Grunwald-Wang theorem [8, Theorem 9.2.8].

Theorem 3.1. *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 [5]. We repeat the proof here because it plays a crucial role in proving our main result.

Proposition 3.2 ([5, 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 [8, 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. □

Remark 3.3. Proposition 3.2 implies the following:

With the same setting as Lemma 2.2,

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

Here sup is over the conductor of L/K.

The above remark shows that the p-fine Selmer group of an Abelian variety A/K becomes arbitrarily large on varying over all $\mathbb{Z}/p\mathbb{Z}$-extensions of K. The proof of Proposition 3.2 suggests that it should be possible to find an effective estimate on the conductor. Indeed, we can prove the following theorem.

Theorem 3.4. *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 $r_p(R_p^S(A/L)) \geq N$.*

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

Theorem 3.5. *Let $A/\mathbb{Q}$ be an Abelian variety of dimension d. 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 $r_p(R_p^S(A/L)) \geq N$.*

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 (see [7, Chapter VII] or [6]).

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 2.2, 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 $S = \{v_1, \ldots, v_k\} \cup S_\infty$ 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 3.2. Here, $r_1 = 1$, $r_2 = 0$ and $\delta = 0$. Therefore we must choose S_n such that $|S_n| = |S| + 1 + n$.

Define $M = \prod_{i=1}^k v_i$. 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 $p_2 \nmid Mp_1$; 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 the set S and the Abelian variety A. $\square$

The computation for proving the general case is similar. We point out some similarities and differences. 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 3.6. By Equation 1, $r_p(\mathrm{Sel}_p(A/K)) \geq r_p(R_p^S(A/K))$. Thus, Theorem 3.4 holds on replacing $r_p(R_p^S(A/K)) \geq N$ by $r_p(\mathrm{Sel}_p(A/K)) \geq N$.

4. 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 [5].

Question 4.1. Let A be an Abelian variety defined over a number field K. Suppose $A(K)[p] \neq 0$. Is

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

For elliptic curves, the answer to this question is precise. It is a corollary of results proved in [2] and [11]. We record these previously known results.

Lemma 4.2 ([11, Lemma 3.1]). *Let $v \mid p$ and $K_v/\mathbb{Q}_p$ be a finite extension of degree n_v. Then*

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

The lemma follows from the observation that $\widehat{E}(\mathfrak{m}_v^a)$ has finite index in $E(K_v)$ 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 [10, Theorem IV.6.4b]. 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 $\mathcal{K}_{p^k}(E/K)$ is contained in the cokernel of the map $E(K)/p \to \oplus_{v|p} E(K_v)/p^k$, denoted by C_{p^k}. Lemma 4.2 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 4.3 ([11, Proposition 3.2]). *The index of $\mathcal{K}_{p^k}(E/K)$ inside $Ш(E/K)[p^k]$ is bounded by*

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

The focus is 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 $w \mid p$ in L. For each $w \mid p$, $\#E(L_w)[p]$ is finite and bounded [10, 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 4.4 ([2]). *Let E/K be an elliptic curve. 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 unbounded.*

The above two results provides a positive answer to Question 4.1.

Theorem 4.5. *Let E be an elliptic curve defined over the number field K. Varying over all $\mathbb{Z}/p\mathbb{Z}$-extensions, L/K, $\mathcal{K}_p(E/L)$ is unbounded.*

Remark 4.6. In the case of elliptic curves, the question asked in [5] does not need the assumption $E(K)[p] \neq 0$.

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

$$\#C_p \leq \prod_{v|p} \#A(K_v)/pA(K_v) \leq \prod_{v|p} \#H^1(K_v, A[p]).$$

The right hand side of the inequality is finite and bounded [8, Theorem 7.1.8(iii)]. The next result now follows immediately.

Proposition 4.7. *Let A be an Abelian variety defined over the number field K. Varying over all $\mathbb{Z}/p\mathbb{Z}$-extensions L/K, $\mathcal{K}_p(A/L)$ is unbounded if and only if $Ш(A/L)[p]$ is unbounded.*

Remark 4.8.

1. Theorem 4.5 is also seen to follow from Proposition 4.7 and the theorem of Clark-Sharif without using the results of [11].
2. In [4], Creutz has proven results on the unboundedness of $Ш(A/L)[p]$.

5. Growth of p-fine Selmer groups in quadratic extensions

We are unable to prove that the p-(fine) Selmer group can be arbitrarily large in quadratic extensions of $\mathbb{Q}$, but there are reasons to believe it should be true. In this section, we prove that this question is equivalent to a well-known conjecture about class groups of quadratic extensions.

Theorem 5.1. *Fix an odd prime p. Let E/K be an elliptic curve such that $E(K)[p] \neq 0$. Let S be a finite set of primes in K containing the primes above p, the primes of bad reduction of E and the Archimedean primes. As we vary over all $\mathbb{Z}/2\mathbb{Z}$-extensions L/K,*

$$\sup\{r_p(R_p^S(E/L)) \mid L/K \textit{ is a quadratic extension}\} = \infty$$

if and only if

$$\sup\{r_p(\mathrm{Cl}(L)) \mid L/K \textit{ is a quadratic extension}\} = \infty.$$

To prove the theorem, we need to first prove some lemmas.

Lemma 5.2. *With the same setting as Theorem 5.1,*

$$r_p(R_p^S(E/L)) \geq r_p(\mathrm{Cl}(L))r_p(E(L)[p]) + O(1).$$

Proof. It follows immediately from Lemma 2.2 upon observing that

$$|r_p(\mathrm{Cl}(L)) - r_p(\mathrm{Cl}_S(L))| = O(1). \tag{4}$$

Indeed, this difference depends only on $|S(L)|$, where $S(L)$ is the set of finite primes of L above the primes of S in K. Note that $|S(L)|$ is finite and bounded, in fact less than $|S|^2$. □

Set $B = E(L)[p]$. Define $R_p^S(B/L)$ by replacing $E[p]$ with $E(L)[p]$ in the definition of the p-fine Selmer group (see (1)).

Lemma 5.3. *With the setting as Theorem 5.1,*

$$|r_p(R_p^S(B/L)) - r_p(R_p^S(E/L))| \leq r_p(\mathrm{Cl}_S(L)) + O(1).$$

Proof. If $B = E(L)[p] = E[p]$, there is nothing to prove. So, assume $B \neq E[p]$. Consider the following commutative diagram

$$\begin{array}{ccccccc} 0 & \to & R_p^S(B/L) & \to & H^1(G_S(L),\ B) & \to & \bigoplus_\upsilon H^1(L_\upsilon,\ B) \\ & & \downarrow s & & \downarrow f & & \downarrow g \\ 0 & \to & R_p^S(E/L) & \to & H^1(G_S(L),\ E[p]) & \to & \bigoplus_\upsilon H^1(L_\upsilon,\ E[p]) \end{array}$$

where υ runs over all the primes in the finite set $S(L)$.

By hypothesis, E has an L-rational p-torsion point. This gives the short exact sequence

$$0 \to B \to E[p] \to \mu_p \to 0. \tag{5}$$

This is because, if E has an L-rational p-torsion point, this point gives an injection $\mathbb{Z}/p\mathbb{Z} \hookrightarrow E[p]$. Therefore,

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to M \to 0.$$

By Cartier duality and the Weil pairing, the short exact sequence turns into

$$0 \to M^\vee \to E[p] \to \mu_p \to 0,$$

where μ_p is viewed as a quotient of $E[p]$. Since the Weil pairing is alternating, the orthogonal complement of $\mathbb{Z}/p\mathbb{Z}$ is $\mathbb{Z}/p\mathbb{Z}$, thus $M^\vee = \mathbb{Z}/p\mathbb{Z}$ as a subgroup of $E[p]$.

Taking the $G_S(L)$-cohomology of (5), $\ker(f) = H^0(G_S(L), \mu_p)$. As $|\mu_p|$ is finite and bounded, $r_p(\ker(s)) \leq r_p(\ker(f)) = O(1)$. A similar argument for the local cohomology yields $r_p(\ker(g)) = O(1)$.

Therefore, to prove the lemma, it suffices to prove

$$r_p(\mathrm{coker}(s)) \leq r_p(\mathrm{coker}(f)) + O(1) \leq r_p(\mathrm{Cl}_S(L)) + O(1).$$

Indeed, by Lemma 2.1 applied to the map s,

$$\begin{aligned} |r_p(R_p^S(B/L)) - r_p(R_p^S(E/L))| &\leq 2r_p(\ker(s)) + r_p(\mathrm{coker}(s)) \\ &= r_p(\mathrm{coker}(s)) + O(1). \end{aligned}$$

Let $\mathcal{O}_S^\times$ be the set of S-units of L_S, the maximal unramified outside S extension of L. We know $\mu_p \subseteq \mathcal{O}_S^\times$ and there exists a short exact sequence [8, Theorem 8.3.18]

$$0 \to \mu_p \to \mathcal{O}_S^\times \xrightarrow{p} \mathcal{O}_S^\times \to 0.$$

This yields a long exact sequence which can be rewritten as

$$0 \to \mathcal{O}_{L,S}^{\times}/(\mathcal{O}_{L,S}^{\times})^p \to H^1(G_S(L), \mu_p) \to \mathrm{Cl}_S(L)[p] \to 0, \tag{6}$$

where $\mathcal{O}_{L,S}^{\times}$ is the notation for the S-units of L. We remark, (6) follows from standard results $H^0(G_S(L), \mathcal{O}_S^{\times}) \simeq \mathcal{O}_{L,S}^{\times}$ and $H^1(G_S(L), \mathcal{O}_S^{\times}) \simeq \mathrm{Cl}_S(L)$ [8, Theorem 8.3.11]. Therefore, (p-rank of) $\mathrm{coker}(f) = H^1(G_S(L), \mu_p)$ is finite. Furthermore,

$$|r_p(\mathrm{coker}(f)) - r_p(\mathrm{Cl}_S(L))| \leq r_p(\mathcal{O}_{L,S}^{\times}/(\mathcal{O}_{L,S}^{\times})^p).$$

Since $|S(L)|$ is bounded by an absolute constant, the S-units analogue of Dirichlet's Unit Theorem yields

$$|r_p(\mathrm{coker}(f)) - r_p(\mathrm{Cl}_S(L))| = O(1).$$

Equivalently,

$$r_p(\mathrm{coker}(f)) = r_p(\mathrm{Cl}_S(L)) + O(1).$$

Therefore,

$$|r_p(R_p^S(B/L)) - r_p(R_p^S(E/L))| \leq r_p(\mathrm{Cl}_S(L)) + O(1).$$

This finishes the proof. □

Proof of Theorem 5.1. In Lemma 5.2, we showed

$$r_p(R_p^S(E/L)) \geq r_p(\mathrm{Cl}(L)) r_p(E(L)[p]) + O(1).$$

This proves: if $r_p(\mathrm{Cl}(L))$ is arbitrarily large then so is the $r_p(R_p^S(E/L))$. Equivalently, if $r_p(R_p^S(E/L))$ is bounded then so is $r_p(\mathrm{Cl}(L))$.

We now prove the other direction.

Claim. If $r_p(\mathrm{Cl}(L))$ is bounded, the same is true for the $r_p(R_p^S(E/L))$.

Justification. Suppose $r_p(\mathrm{Cl}(L)) = O(1)$. By Equation 4, $r_p(\mathrm{Cl}(L))$ is bounded if and only if $r_p(\mathrm{Cl}_S(L))$ is bounded.

By hypothesis, the Galois action of $G_S(L)$ on $E(L)[p]$ is trivial; the argument in Remark 2.3 yields

$$r_p(R_p^S(B/L)) \leq 2 r_p(\mathrm{Cl}_S(L)) = O(1).$$

By Lemma 5.3, if $r_p(\mathrm{Cl}_S(L))$ is bounded,

$$|r_p(R_p^S(B/L)) - r_p(R_p^S(E/L))| \leq O(1).$$

From the above two inequalities, the claim follows. This finishes the proof. □

Acknowledgement

We thank Kumar Murty for helpful discussions and his encouragement. We thank all past and present members of the GANITA Lab for listening to the details over and over again. We extend our gratitude 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. We are grateful to the referee for a careful reading of this paper and for their helpful comments and corrections.

References

[1] Kęstutis Česnavičius, p-Selmer growth in extensions of degree p, *J. London Math. Soc.*, **95** (2017) no. 3, 833–852.
[2] Pete L. Clark and Shahed Sharif, Period, index and potential Sha, *Algebra & Number Theory*, **4** no. 2, (2010) 151–174.
[3] John Coates and Ramdorai Sujatha, Fine Selmer groups of elliptic curves over p-adic Lie extensions, *Math. Annalen*, **331** no. 4, (2005) 809–839.
[4] Brendan Creutz, Potential Sha for abelian varieties, *J. Number Theory*, **131** no. 11, (2011) 2162–2174.
[5] Meng Fai Lim and V. Kumar Murty, The growth of fine Selmer groups, *J. Ramanujan Math. Society*, **31** no. 1, (2016) 79–94.
[6] Vijaya Kumar Murty and John Scherk, Effective versions of the Chebotarev density theorem for function fields, Comptes rendus de l'Académie des sciences, *Série 1, Mathématique*, **319** no. 6 (1994), 523–528.
[7] Jürgen Neukirch, Algebraic number theory, vol. 322, Springer (2013).
[8] Jürgen Neukirch, Alexander Schmidt and Kay Wingberg, Cohomology of number fields (2008).
[9] Karl Rubin, Euler systems, No. 147, Princeton University Press (2000).
[10] Joseph H. Silverman, The arithmetic of elliptic curves, vol. 106, Springer (2009).
[11] Christian Wuthrich, The fine Tate-Shafarevich group, *Math. Proc. Camb. Phil. Soc.*, vol. 142 (2007) 1–12.