Canad. J. Math. Vol. 67 (3), 2015 pp. 654–666
http://dx.doi.org/10.4153/CJM-2014-041-1

Growth of Selmer Groups of CM Abelian Varieties

Meng Fai Lim and V. Kumar Murty

Abstract. Let p be an odd prime. We study the variation of the p-rank of the Selmer groups of Abelian varieties with complex multiplication in certain towers of number fields.

1 Introduction

Let A be an Abelian variety defined over a number field F. The Mordell–Weil group, that is, the group of rational points $A(F)$, has been an object of much study in arithmetic. One of the main approaches towards studying it is via the Selmer groups. More precisely, one looks at the p-primary component of the Selmer groups (for a choice of a prime number p).

Let p be an odd prime. In this paper, we are interested in the variation of the p-rank of the Selmer groups of Abelian varieties with complex multiplication in certain families of number fields. We first establish a lower bound for this rank with respect to a p-power degree isogeny (see Corollaries 4.3 and 4.4) under some mild assumptions on the prime p. Our proof utilizes the techniques developed in [4, 9] and a property of Abelian varieties with complex multiplication as observed in [16].

Our lower bound is somewhat in the spirit of the papers of Mazur and Rubin [10,11], where they obtain lower bounds for the $\mathbb{Z}_p$-corank of the Selmer group of an elliptic curve over Galois number field extensions of degree twice a power of an odd prime under the assumption (and some other assumptions on the reduction of the elliptic curve) that the $\mathbb{Z}_p$-corank of the Selmer group is odd. Our result differs from theirs in two aspects. First, we consider p-rank rather than $\mathbb{Z}_p$-corank. Second, our Abelian varieties have complex multiplication. In the case of a CM-elliptic curve, the $\mathbb{Z}_p$-corank of the Selmer group may not be odd, and so the results of [10,11] do not apply. We also remark that since our result is an estimate on the p-rank, this contribution can go either to the Mordell–Weil group or the Tate–Shafarevich group, though we are not able to distinguish which one at present.

We will then apply our lower bound to study the growth of the p-rank in certain classes of infinite p-extensions of number fields, namely the $\mathbb{Z}_p^d$-extension and the infinite p-Hilbert class tower (see Proposition 5.1 and Theorem 6.2). Theorem 6.2 complements results proved in [8,11,14] (see Section 7). In the case of a $\mathbb{Z}_p$-extension,

Received by the editors October 8, 2013.
Published electronically March 31, 2015.
This work was done while the first author was a postdoctoral fellow at University of Toronto.
AMS subject classification: **11G15**, 11G10, 11R23, 11R34.
Keywords: Selmer group, Abelian variety with complex multiplication, $\mathbb{Z}_p$-extension, p-Hilbert class tower.

we obtain a lower bound of certain Iwasawa invariants attached to the Selmer groups in terms of certain Iwasawa invariants attached to the $\mathbb{Z}_p$-extension (see Theorem 5.6).

We now give a brief description of the layout of the paper. In Section 2 we review the definitions and properties of Selmer groups. In Section 3 we record some lemmas on cohomology groups that will be used in the remainder of the paper. In Section 4 we will prove our lower bounds, which will be applied to the study of the growth of the p-rank of Selmer groups in $\mathbb{Z}_p^d$-extension in Section 5 and infinite p-Hilbert class tower in Section 6.

2 Preliminaries

In this section, we will review the arithmetic objects that will be studied in this paper. Let A and B be two abelian varieties defined over a number field F. Suppose we are given an isogeny

$$A \xrightarrow{\phi} B.$$

We write $A[\phi] = \ker \phi$. For any algebraic extension L of F, we will write $A(L)[\phi] = A[\phi] \cap A(L)$. The Selmer group of A over L with respect to ϕ is denoted and defined by

$$\mathrm{Sel}_\phi(A/L) = \ker\left(H^1\left(L, A[\phi]\right) \longrightarrow \prod_w H^1(L_w, A)\right),$$

where w runs through all the primes (including archimedean primes) of L.

If $A = B$, we can consider the isogeny ϕ^n for every $n \geq 1$, and we denote by $A[\phi^\infty]$ the union of all the $A[\phi^n]$ for $n \geq 1$. As before, we will write $A(L)[\phi^\infty] = A[\phi^\infty] \cap A(L)$. One can check easily that we have the following commutative diagram with exact rows for $m \geq n$:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_{\phi^n}(A/L) & \longrightarrow & H^1(L, A[\phi^n]) & \longrightarrow & \prod_w H^1(L_w, A) \\
 & & \downarrow & & \downarrow & & \| \\
0 & \longrightarrow & \mathrm{Sel}_{\phi^m}(A/L) & \longrightarrow & H^1(L, A[\phi^m]) & \longrightarrow & \prod_w H^1(L_w, A).
\end{array}$$

Taking the direct limit, we obtain the following exact sequence

$$0 \longrightarrow \varinjlim_n \mathrm{Sel}_{\phi^n}(A/L) \longrightarrow H^1\left(L, A[\phi^\infty]\right) \longrightarrow \prod_w H^1(L_w, A).$$

We shall write

$$\mathrm{Sel}_{\phi^\infty}(A/L) = \varinjlim_n \mathrm{Sel}_{\phi^n}(A/L).$$

We end this section by giving two examples of isogenies that will be considered in this paper. The first is the multiplication-by-p map, where p is a prime. In this case, we have $A[\phi^\infty] = A[p^\infty]$.

We now describe the second example. Let K be a finite Galois extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$, and let F be a finite Galois extension of K. Suppose that A is an Abelian variety defined over F with complex multiplication by $\mathcal{O}_K$. Let $\mathfrak{p}$ be a prime in K lying above p. There exists some integer $h > 0$ (for example, one may take h to

be the class number) such that $\mathfrak{p}^h = \alpha\mathcal{O}_K$. Then the multiplication-by-α map is an isogeny of A with degree a power of p.

3 Some Cohomology Lemmas

In this section, we record some basic results on Galois cohomology that will be used later. We begin by stating the following standard result (*cf.* [15, Corollary 1.6.13]).

Lemma 3.1 *Let G be a pro-p group. Then every discrete, simple, p-primary G-module A is isomorphic to $\mathbb{Z}/p$ (with trivial G-action). In particular, if A is a p-primary G-module, then $A = 0$ if and only if $A^G = 0$.*

For an Abelian group N, we define its p-rank to be the $\mathbb{F}_p$-dimension of $N[p]$ which we denote by $r_p(N)$. If G is a pro-p group, we write $h_1(G) = r_p(H^1(G, \mathbb{Z}/p))$. We now state and prove the following lemma, which gives an estimate of the p-rank of the first cohomology group.

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 $h_1(G)$ is finite, then $r_p(H^1(G, M))$ is finite, and we have the following estimates for $r_p(H^1(G, M))$:*

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

Moreover, if M is a trivial G-module, we have the equality

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

Proof We shall first establish the upper bound. If M is finite, it then follows from a standard dévissage argument and the first assertion of Lemma 3.1 that

$$r_p\big(H^1(G, M)\big) \le h_1(G)\log_p(|M|).$$

For a general M, we denote by M_{div} the maximal p-divisible subgroup of M. Note that M_{div} is a G-submodule of M. Then the short exact sequence

$$0 \longrightarrow M_{\mathrm{div}} \longrightarrow M \longrightarrow M/M_{\mathrm{div}} \longrightarrow 0$$

induces the exact sequence

$$H^1(G, M_{\mathrm{div}}) \longrightarrow H^1(G, M) \longrightarrow H^1(G, M/M_{\mathrm{div}}).$$

Therefore, we are reduced to showing that $r_p(H^1(G, M_{\mathrm{div}}))$ and $r_p(H^1(G, M/M_{\mathrm{div}}))$ are finite, and that the inequalities

$$r_p\big(H^1(G, M_{\mathrm{div}})\big) \le h_1(G)\ \operatorname{corank}_{\mathbb{Z}_p}(M),$$
$$r_p\big(H^1(G, M/M_{\mathrm{div}})\big) \le h_1(G)\log_p(|M/M_{\mathrm{div}}|)$$

hold. Since M is cofinitely generated over $\mathbb{Z}_p$, we have that M/M_{div} is finite. The finiteness of $r_p(H^1(G, M/M_{\mathrm{div}}))$ and the validity of the second inequality then follow

from the above discussion. To show that the first inequality holds, we first note that the short exact sequence

$$0 \longrightarrow M_{\mathrm{div}}[p] \longrightarrow M_{\mathrm{div}} \xrightarrow{p} M_{\mathrm{div}} \longrightarrow 0$$

of discrete G-modules induces a surjection $H^1(G, M_{\mathrm{div}}[p]) \twoheadrightarrow H^1(G, M_{\mathrm{div}})[p]$ and, consequently, the inequality

$$r_p\big(H^1(G, M_{\mathrm{div}})\big) \leq r_p\big(H^1(G, M_{\mathrm{div}}[p])\big).$$

By the above discussion, the latter is less than or equal to $h_1(G)\log_p(|M_{\mathrm{div}}[p]|)$, and the required inequality follows from the observation that

$$\log_p(|M_{\mathrm{div}}[p]|) = \mathrm{corank}_{\mathbb{Z}_p}(M).$$

We now prove the second assertion of the lemma. Let M be a trivial G-module. Since cohomology commutes with finite direct sums, it suffices to prove the equalities

$$h_1(G) = r_p\big(H^1(G, \mathbb{Z}/p^r)\big) = r_p\big(H^1(G, \mathbb{Q}_p/\mathbb{Z}_p)\big).$$

The natural injections

$$H^1(G, \mathbb{Z}/p) \hookrightarrow H^1(G, \mathbb{Z}/p^r) \hookrightarrow H^1(G, \mathbb{Q}_p/\mathbb{Z}_p)$$

yield the inequalities

$$h_1(G) \leq r_p\big(H^1(G, \mathbb{Z}/p^r)\big) \leq r_p\big(H^1(G, \mathbb{Q}_p/\mathbb{Z}_p)\big),$$

and the last term is less than or equal to $h_1(G)$ by our estimate for the upper bound.

Finally, it remains to show the lower bound. The short exact sequence

$$0 \longrightarrow M^G \longrightarrow M \longrightarrow M/M^G \longrightarrow 0$$

induces the exact sequence

$$(M/M^G)^G \longrightarrow H^1(G, M^G) \longrightarrow H^1(G, M).$$

(In fact, the map on the left is injective, although we will not need this.) This gives the inequality

$$\begin{aligned} r_p\big(H^1(G, M)\big) &\geq r_p\big(H^1(G, M^G)\big) - r_p\big((M/M^G)^G\big) \\ &= h_1(G) r_p\big(M^G\big) - r_p\big((M/M^G)^G\big), \end{aligned}$$

where the second equality follows from the second assertion of the lemma. ∎

Corollary 3.3 *Retain the notation and assumptions of the preceding lemma. If G is a compact p-adic Lie group, then the quantity*

$$\sup\{r_p\big(H^1(U, M)\big) : U \text{ an open subgroup of } G\}$$

is finite. If G is not a p-adic Lie group and $M^G \neq 0$, then the above quantity is infinite.

Proof By a theorem of Lubotzky and Mann [7], we have that G is a compact p-adic Lie group if and only if $\sup\{h_1(U) : U \text{ an open subgroup of } G\}$ is finite. The first assertion then follows from the estimate for the upper bound in the preceding

lemma. To show the second assertion, note that for any open normal subgroup U of G, we have the inequality

$$r_p\big(H^1(U,M)\big) \geq h_1(U) r_p\big(M^U\big) - r_p\big((M/M^U)^U\big) \geq h_1(U) r_p\big(M^U\big) - r_p\big(M\big).$$

Since $M^G \neq 0$, it follows from the equality $(M^U)^{G/U} = M^G$ and Lemma 3.1 that $M^U \neq 0$. Therefore, the lower estimate goes to infinity by the theorem of Lubotzky and Mann, giving us the required conclusion. ∎

4 A Lower Bound for the p-rank of Selmer Group

In this section, we will prove a lower bound for the p-rank of the Selmer group. For a given number field L, we will let $\mu(L)$ be the group of all roots of unity in L.

Proposition 4.1 *Let A and B be two Abelian varieties defined over F. Let p be an odd prime and suppose that there is an isogeny $\phi\colon A \to B$ such that $A[\phi]$ has p-power order. Suppose that A satisfies at least one of the following conditions.*

(i) *The Abelian variety A has good reduction everywhere over F.*
(ii) *The Abelian variety A has complex multiplication by K, and p does not divide $|\mu(K)|$.*

Let L be an unramified Galois p-extension of F. Then we have the inequality

$$r_p\big(\operatorname{Sel}_\phi(A/F)\big) \geq r_p\big(H^1(\operatorname{Gal}(L/F), A(L)[\phi])\big).$$

Proof Denote by Σ the Galois group $\operatorname{Gal}(L/F)$. We first prove the inequality when A satisfies (i). Consider the following commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Sel}_\phi(A/F) & \longrightarrow & H^1(F, A[\phi]) & \longrightarrow & \prod_v H^1(F_v, A) \\ & & \downarrow{\scriptstyle s_{L/F}} & & \downarrow{\scriptstyle h_{L/F}} & & \downarrow{\scriptstyle g_{L/F}} \\ 0 & \longrightarrow & \operatorname{Sel}_\phi(A/L)^\Sigma & \longrightarrow & H^1(L, A[\phi])^\Sigma & \longrightarrow & \big(\prod_w H^1(L_w, A)\big)^\Sigma, \end{array}$$

where the vertical maps $s_{L/F}$, $h_{L/F}$, and $g_{L/F}$ are the natural restrictions. Since L is an unramified extension of F, and A has good reduction everywhere over F, it follows from [4, Propositions 4.1, 4.3] (see also [9, Corollary 4.4]) that $\ker g_{L/F} = 0$. A diagram chasing argument will then show that $\ker h_{L/F}$ injects into $\operatorname{Sel}_\phi(A/F)$. On the other hand, the inflation-restriction sequence gives the equality $\ker h_{L/F} = H^1(\Sigma, A(L)[\phi])$. Therefore, we have an injection

$$H^1(\Sigma, A(L)[\phi]) \hookrightarrow \operatorname{Sel}_\phi(A/F)\ ,$$

which gives us the required inequality.

Now suppose that A satisfies (ii). Then by [16, Theorem 7], there exists a finite extension F' of F such that A has good reduction everywhere over F', and $[F'\colon F]$ divides $2|\mu(K)|$. Set $L' = F'L$ and $\Sigma' = \operatorname{Gal}(L'/F')$. By the above argument, we have an injection

$$H^1(\Sigma', A(L')[\phi]) \hookrightarrow \operatorname{Sel}_\phi(A/F'),$$

which is also a $\mathrm{Gal}(F'/F)$-map. Taking $\mathrm{Gal}(F'/F)$-invariants, we have

$$H^1(\Sigma', A(L')[\phi])^{\mathrm{Gal}(F'/F)} \hookrightarrow \mathrm{Sel}_\phi(A/F')^{\mathrm{Gal}(F'/F)}.$$

Now consider the following commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_\phi(A/F) & \longrightarrow & H^1(F, A[\phi]) & \longrightarrow & \prod_v H^1(F_v, A) \\
 & & \downarrow{\scriptstyle s_{F'/F}} & & \downarrow{\scriptstyle h_{F'/F}} & & \downarrow{\scriptstyle g_{F'/F}} \\
0 & \longrightarrow & \mathrm{Sel}_\phi(A/F')^{\mathrm{Gal}(F'/F)} & \longrightarrow & H^1(F', A[\phi])^{\mathrm{Gal}(F'/F)} & \longrightarrow & \Big(\prod_v H^1(F'_v, A)\Big)^{\mathrm{Gal}(F'/F)},
\end{array}$$

where the vertical maps are the natural restrictions. Since $\mathrm{Gal}(F'/F)$ has order coprime to p, we have $\ker h_{F'/F} = \mathrm{coker}\, h_{F'/F} = \ker g_{F'/F} = 0$, and consequently it follows from a diagram chasing argument that the map $s_{F'/F}$ is an isomorphism. It remains to show that $H^1(\Sigma', A(L')[\phi])^{\mathrm{Gal}(F'/F)} \cong H^1(\Sigma, A(L)[\phi])$. This follows from the observation that the two spectral sequences

$$H^i\big(\mathrm{Gal}(F'/F), H^j(\Sigma', A(L')[\phi])\big) \Longrightarrow H^{i+j}\big(\mathrm{Gal}(L'/F), A(L')[\phi]\big),$$
$$H^i\big(\Sigma, H^j(\mathrm{Gal}(L'/L), A(L')[\phi])\big) \Longrightarrow H^{i+j}\big(\mathrm{Gal}(L'/F), A(L')[\phi]\big)$$

collapse (since $\mathrm{Gal}(L'/L) \cong \mathrm{Gal}(F'/F)$ has order coprime to p) and yield the isomorphisms

$$H^1(\Sigma', A(L')[\phi])^{\mathrm{Gal}(F'/F)} \cong H^1\big(\mathrm{Gal}(L'/F), A(L')[\phi]\big) \cong H^1(\Sigma, A(L)[\phi]).$$

This finishes the proof. ∎

In the case where $A = B$, we have the following proposition, which is proved similarly.

Proposition 4.2 *Retaining the notation and assumptions of Proposition 4.1, we have the inequality*

$$r_p\big(\mathrm{Sel}_{\phi^n}(A/F)\big) \geq r_p\big(H^1(\mathrm{Gal}(L/F), A(L)[\phi^n])\big)$$

for $1 \leq n \leq \infty$.

Set L to be the p-Hilbert class field of F and set ϕ to be multiplication-by-p. Then, combining the above results with Lemma 3.2, we obtain the following corollary.

Corollary 4.3 *Suppose that A is an Abelian variety over F satisfying either of the two conditions in Proposition 4.1. Then we have the inequality*

$$r_p(\mathrm{Sel}_{p^n}(A/F)) \geq r_p(\mathrm{Cl}(F))r_p(A(F)[p^n]) - r_p\big((A(L)[p^n]/A(F)[p^n])^{\mathrm{Gal}(L/F)}\big)$$

for $1 \leq n \leq \infty$.

Proof It remains to show that $h_1(\mathrm{Gal}(L/F)) = r_p(\mathrm{Cl}(F))$. Since $\mathrm{Cl}(F)$ is a finite Abelian group, the p-rank of $\mathrm{Cl}(F)$ is also given by the $\mathbb{F}_p$-dimension of $\mathrm{Cl}(F)/p$, but the latter is isomorphic to $H^1(\mathrm{Gal}(L/F), \mathbb{Z}/p)$ by class field theory. ∎

One can also deduce the following variant of Corollary 4.3.

Corollary 4.4 *Let A be an Abelian variety defined over a number field F, with complex multiplication by the ring of integers $\mathcal{O}_K$ of K. We also assume that $K \subseteq F$. Let p be an odd prime, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ lying above p. Suppose that at least one of the following statements hold.*

(i) *The Abelian variety A has good reduction everywhere over F.*
(ii) *p does not divide $|\mu(K)|$.*

Let L be the p-Hilbert class field of F. Then we have

$$r_p\big(\mathrm{Sel}_{\mathfrak{p}^n}(A/F)\big) \geq r_p\big(\mathrm{Cl}(F)\big)\, r_p\big(A(F)[\mathfrak{p}^n]\big) - r_p\Big(\big(A(L)[\mathfrak{p}^n]/A(F)[\mathfrak{p}^n]\big)^{\mathrm{Gal}(L/F)}\Big)$$

for $1 \leq n \leq \infty$.

Proof For $1 \leq n < \infty$, we can find an Abelian variety B_n and an isogeny $\phi_n : A \to B_n$ such that $\ker \phi_n = A(F)[\mathfrak{p}^n]$ (*cf.* [13, p. 72, Theorem 4]). The required conclusion then follows from Proposition 4.1. For $n = \infty$, let h be a positive integer such that $\mathfrak{p}^h = \alpha\mathcal{O}_K$. Since A has complex multiplication by the ring of integers $\mathcal{O}_K$, the multiplication-by-α map is an isogeny of A with p-power degree. The required inequality now follows from Proposition 4.2. ∎

Remark 4.5 Suppose that $A = E$ is an elliptic curve with complex multiplication by an imaginary quadratic field K. Since $\mu(K)$ has order a power of 2 when K is not $\mathbb{Q}(\sqrt{-3})$, and order 6 when $K = \mathbb{Q}(\sqrt{-3})$, Proposition 4.1(ii) and Corollary 4.4 hold if $p \geq 5$. In the case that $p = 3$, statement (ii) also holds if one assumes further that K is not $\mathbb{Q}(\sqrt{-3})$.

5 Growth of Selmer Groups in $\mathbb{Z}_p^d$-extension

Let A and B be two Abelian varieties defined over F. Let p be an odd prime and suppose that there is an isogeny $\phi : A \to B$ such that $A[\phi]$ has p-power order. We assume throughout the section that A satisfies either of the two conditions in Proposition 4.1. We will be interested in the growth of the p-rank of the Selmer group $\mathrm{Sel}_\phi(A/F)$ (and $\mathrm{Sel}_{\phi^\infty}(A/F)$ in the case $A = B$). We let $S(A/F)$ be either $\mathrm{Sel}_\phi(A/F)$ or $\mathrm{Sel}_{\phi^\infty}(A/F)$ for this section.

Let F_∞ be a Galois extension of F with Galois group $\Sigma \cong \mathbb{Z}_p^d$. Denote M_∞ to be the maximal Abelian unramified pro-p extension of F_∞ and write $X_\infty = \mathrm{Gal}(M_\infty/F_\infty)$. We also write $\Sigma_n = \Sigma^{p^n}$ and $F_n = F_\infty^{\Sigma_n}$. Combining the estimates obtained in Section 3 with a theorem of Monsky [12], we prove the following proposition.

Proposition 5.1 *Suppose that A is an Abelian variety over F satisfying either of the two conditions in Proposition 4.1, and suppose that $A(F)[\phi] \neq 0$. Let F_∞ be a $\mathbb{Z}_p^d$-extension of F with the property that X_∞/pX_∞ is infinite. Then the following statements hold.*

(i) *The p-rank of $S(A/F_n)$ goes to infinity as n goes to infinity.*
(ii) *The group $S(A/F_\infty)$ has infinite p-rank.*

Proof (i) By a theorem of Monsky [12], the assumption of X_∞/pX_∞ being infinite implies that $r_p(\mathrm{Cl}(F_n))$ goes to infinity as n goes to infinity. If A satisfies either of the

two conditions in Proposition 4.1, then A also satisfies the same condition over F_n. The conclusion then follows from an application of Corollary 4.3.

(ii) As in the argument of Proposition 4.1, the kernel of the map

$$S(A/F_n) \longrightarrow S(A/F_\infty)^{\Sigma_n}$$

is contained in either $H^1(\Sigma_n, A(F_\infty)[\phi])$ or $H^1(\Sigma_n, A(F_\infty)[\phi^\infty])$. By Corollary 3.3, the latter groups have bounded p-rank as n goes to infinity. The assertion then follows from this and assertion (i). ∎

For the remainder of the section, we shall focus our attention on the case $d = 1$, and we write $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$, where $\Gamma \cong \mathbb{Z}_p$. Fix a topological generator γ for Γ. Then this ring is topologically isomorphic to $\mathbb{Z}_p[\![T]\!]$, where the isomorphism is induced by $\gamma \mapsto 1 + T$ (*cf.* [15, Chap. V, Proposition 5.3.5]). By abuse of notation, we shall also denote the ring $\mathbb{Z}_p[\![T]\!]$ by Λ. We now recall the following structure theorem for finitely generated Λ-modules (*cf.* [15, Chap. V, 5.3.8]).

Theorem 5.2 *Let M be a finitely generated Λ-module. Then there is a Λ-homomorphism*

$$M \longrightarrow \Lambda^r \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/p^{m_i} \Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/f_j^{n_j} \Big)$$

with finite kernel and cokernel, where each f_j is an irreducible distinguished polynomial. The numbers r, m_i, n_j and f_j are uniquely determined by M.

The Iwasawa μ-invariant (resp., the Iwasawa λ-invariant) of M is given by $\sum_{i=1}^{s} m_i$ (resp., $\sum_{j=1}^{t} n_i \deg f_j$). We are also interested in $s(M)$ which is the number of summands in $(\bigoplus_{i=1}^{s} \Lambda/p^{m_i})$. Clearly, we have $s(M) = 0$ if and only if $\mu(M) = 0$. Also, we see that if M is a finitely generated Λ-module with the above decomposition, then M/pM is a finitely generated Λ-module with $\mu(M/pM) = r(M) + s(M)$. The following lemma is a straightforward calculation.

Lemma 5.3 *Let M be a finitely generated Λ-module. Let $w_n = (1+T)^{p^n} - 1$. Then for big enough n, we have*

$$r_p\big(M/(p, w_n)M\big) = \big(r(M) + s(M)\big)\, p^n + O(1) = \mu(M/p)p^n + O(1).$$

Proof It suffices to compute the terms in the summands in Theorem 5.2:

$$\begin{aligned} r_p\big(\Lambda/(p, w_n)\Lambda\big) &= r_p\big(\mathbb{Z}/p[T]/T^{p^n}\big) = p^n, \\ r_p\big((\Lambda/p^{m_i})/(p, w_n)\big) &= r_p\big(\mathbb{Z}/p[T]/T^{p^n}\big) = p^n, \\ r_p\big((\Lambda/f_j^{n_j})/(p, w_n)\big) &= r_p\big(\mathbb{Z}/p[T]/(T^{p^n}, f_j^{n_j})\big) = n_j \deg f_j \end{aligned}$$

for big enough n. ∎

The following lemma is well known, but for the convenience of the reader we include a proof.

Lemma 5.4 *Let A be an Abelian variety over F, and let F_∞ be a $\mathbb{Z}_p$-extension of F. Then $\mathrm{Hom}_{\mathbb{Z}_p}(S(A/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$ is a finitely generated Λ-module.*

Proof Write $W = \mathrm{Hom}_{\mathbb{Z}_p}(S(A/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$. By the topological Nakayama lemma (*cf.* [15, Chap. V, Proposition 5.3.10]), it suffices to show that W_Γ is a finitely generated $\mathbb{Z}_p$-module. This is equivalent to showing that $S(A/F_\infty)^\Gamma$ is a cofinitely generated $\mathbb{Z}_p$-module. Let S be a finite set of primes of F consisting of primes above p, primes at which A has bad reduction primes and the archimedean primes. Let F_S be the maximal extension of F unramified outside S. Then for any algebraic extension L of F that is contained in F_S, we write $G_S(L) = \mathrm{Gal}(F_S/L)$. By the standard theory of Selmer groups, $S(A/F_\infty)$ is contained in either $H^1(G_S(F_\infty), A[\phi])$ or $H^1(G_S(F_\infty), A[\phi^\infty])$. Therefore, we are reduced to showing that

$$H^1(G_S(F_\infty), A[\phi])^\Gamma \quad \text{and} \quad H^1(G_S(F_\infty), A[\phi^\infty])^\Gamma$$

are cofinitely generated $\mathbb{Z}_p$-modules. Since Γ has cohomological dimension 1, we have surjections

$$H^1(G_S(F), A[\phi]) \twoheadrightarrow H^1\big(G_S(F_\infty), A[\phi]\big)^\Gamma,$$
$$H^1(G_S(F), A[\phi^\infty]) \twoheadrightarrow H^1\big(G_S(F_\infty), A[\phi^\infty]\big)^\Gamma.$$

Therefore, we are reduced to showing that $H^1(G_S(F), A[\phi])$ and $H^1(G_S(F), A[\phi^\infty])$ are cofinitely generated $\mathbb{Z}_p$-modules, which is a consequence of the next lemma. ∎

Lemma 5.5 *Let M be a discrete $G_S(F)$-module that is a cofinitely generated $\mathbb{Z}_p$-module. Then $H^i(G_S(F), M)$ is cofinitely generated over $\mathbb{Z}_p$ for each i.*

Proof By considering the cohomology sequence of the short exact sequence

$$0 \longrightarrow M_{\mathrm{div}} \longrightarrow M \longrightarrow M/M_{\mathrm{div}} \longrightarrow 0,$$

we are reduced to showing the lemma for the case when M is finite and M is p-divisible. If M is finite, then $H^i(G_S(F), M)$ is finite by [15, Chap. VIII, Theorem 8.3.20], thus proving the lemma in this case. Now suppose that M is p-divisible. The short exact sequence

$$0 \longrightarrow M[p] \longrightarrow M \xrightarrow{p} M \longrightarrow 0$$

of discrete $G_S(F)$-modules induces a surjection

$$H^i(G_S(F), M[p]) \twoheadrightarrow H^i(G_S(F), M)[p].$$

Since $M[p]$ is finite, it follows from the above discussion and the surjection that $H^i(G_S(F), M)[p]$ is finite. By the dual version of Nakayama Lemma, this implies that $H^i(G_S(F), M)$ is cofinitely generated over $\mathbb{Z}_p$. ∎

Retaining the notation in the above proof, we then have that $S(A/F_\infty)[p]$ is isomorphic to the Pontryagin dual of W/pW. Assuming the hypothesis of Proposition 5.1, it will then follow from Lemmas 5.3 and 5.4 and Proposition 5.1(ii) (for the $d = 1$ case) that $r(W) + s(W) > 0$. In fact, we will show the following sharper result. Recall that X_∞ is the Galois group of the maximal unramified pro-p extension of F_∞ over F_∞.

Theorem 5.6 *Suppose that A is an Abelian variety over F satisfying either of the two conditions in Proposition 4.1. Let F_∞ be a $\mathbb{Z}_p$-extension of F. Then we have the inequality*

$$r(W) + s(W) \geq r_p\big(A(F_\infty)[\phi]\big)\, s(X_\infty)$$

of Iwasawa invariants. In particular, if $A(F)[\phi] \neq 0$ and $\mu(X_\infty) > 0$, then $r(W) + s(W) > 0$.

Proof As seen in the proof of Proposition 5.1, the kernel of the map

$$S(A/F_n) \longrightarrow S(A/F_\infty)^{\Gamma_n}$$

has bounded p-rank. Combining with Lemma 5.3, we obtain the estimate

$$\big(r(W) + s(W)\big)\, p^n \geq r_p\big(\operatorname{Sel}_{p^\infty}(A/F_n)\big) + O(1).$$

By Corollary 4.3, the term on the right is greater or equal to

$$r_p\big(A(F_n)[\phi]\big)\, r_p\big(\operatorname{Cl}(F_n)\big) + O(1).$$

By [15, Chap. XI, Lemma 11.1.5], there exists n_0 (depending on F_∞) such that for $n \geq n_0$, there is a surjection

$$\operatorname{Cl}(F)/p \twoheadrightarrow X_\infty/\Big(p, \frac{w_n}{w_{n_0}}\Big)$$

with kernel bounded independent of n. Calculations similar to those in Lemma 5.3 yield

$$r_p\big(\operatorname{Cl}(F_n)\big) = s(X_\infty)p^n + O(1)$$

for big enough n, noting that $r(X_\infty) = 0$ (*cf.* [15, Chap. XI, Proposition 11.1.4]). Therefore, we obtain the following estimate

$$\big(r(W) + s(W)\big)\, p^n \geq r_p\big(A(F_n)[\phi]\big)\, s(X_\infty)p^n + O(1)$$

for big enough n. This implies the inequality as asserted in the theorem. ∎

Remark 5.7 If F_∞ is the cyclotomic $\mathbb{Z}_p$-extension of F, then $\mu(X_\infty)$ (and hence $s(X_\infty)$) is conjectured to be zero. Therefore, Theorem 5.6 is conjecturally vacuous in this case.

We end the section discussing how one can obtain examples of Theorem 5.6, if one allows a change of the base field F. Again, let p be an odd prime. If F_∞ is a $\mathbb{Z}_p$-extension of F, we will write $\mu(F_\infty/F)$ (resp. $s(F_\infty/F)$) for the μ-invariant (resp. s-invariant) of the group X_∞ attached to the $\mathbb{Z}_p$-extension F_∞/F as defined in this section. Now choose a number field L such that it has a $\mathbb{Z}_p$-extension L_∞ with $\mu(L_\infty/L) > 0$ (such a choice exists by [6, Theorem 1]). Now suppose that A is an Abelian variety defined over a number field F and satisfies either of the two conditions in Proposition 4.1. We then choose a number field M big enough such that it contains the fields F and L, and that $A[\phi]$ is rational over M. Set $M_\infty = ML_\infty$. This is clearly a $\mathbb{Z}_p$-extension of M, and it is an easy exercise to check that $\mu(M_\infty/M) \geq \mu(L_\infty/L)$. By our choice of L_∞/L, we then have $\mu(M_\infty/M) > 0$, and hence $s(M_\infty/M) > 0$. Note that if A satisfies either of the two conditions in Proposition 4.1, then A also satisfies the same condition over M. Therefore, we can now apply Theorem 5.6 to obtain

$r(W)+s(W)>0$, where W here is the Pontryagin dual of $S(A/M_\infty)$. We record our discussion formally.

Proposition 5.8 *Suppose that A is an Abelian variety over F satisfying either of the two conditions in Proposition 4.1. Then there exists a finite extension M of F and a $\mathbb{Z}_p$-extension M_∞ of M such that $r(W)+s(W)>0$, where W is the Pontryagin dual of $S(A/M_\infty)$.*

6 Growth of Selmer Groups in Hilbert Class Field Tower

Retain the assumptions and notation introduced in the first paragraph of Section 5. We introduce an interesting class of (infinite) unramified extensions of F. Let S be a (possibly empty) finite set of primes in F. We denote the S-ideal class group of F by $\mathrm{Cl}_S(F)$. For the remainder of the section, F_∞ will denote the maximal unramified p-extension of F in which all primes in S split completely. Write $\Sigma=\Sigma_F=\mathrm{Gal}(F_\infty/F)$, and let $\{\Sigma_n\}$ be the derived series of Σ. For each n, the fixed field F_{n+1} corresponding to Σ_{n+1} is the p-Hilbert S-class field of F_n.

Let S_∞ be the collection of infinite primes of F, and define δ to be 0 if $\mu_p\subseteq F$ and 1 otherwise. Let $r_1(F)$ and $r_2(F)$ denote the number of real and complex places of F respectively. It is known that if the following inequality

$$r_p(\mathrm{Cl}_S(F))\geq 2+2\sqrt{r_1(F)+r_2(F)+\delta+|S\smallsetminus S_\infty|}$$

holds, then Σ is infinite (see [3] and [15, Chap. X, Theorem 10.10.5]). Stark posed the question on whether $r_p(\mathrm{Cl}_S(F_n))$ tends to infinity in an infinite p-class field tower as n tends to infinity. By class field theory, we have $r_p(\mathrm{Cl}_S(F_n))=h_1(\Sigma_n)$. It then follows from the theorem of Lubotzsky and Mann [7] that Stark's question is equivalent to whether the group Σ is p-adic analytic. By the following conjecture of Fontaine–Mazur [2], one does not expect Σ to be an analytic group if it is infinite.

Conjecture (Fontaine–Mazur) *For any number field F, the group Σ_F has no infinite p-adic analytic quotient.*

Without assuming the Fontaine–Mazur Conjecture, we have the following unconditional (weaker) result, proved by various authors.

Theorem 6.1 *Let F be a number field. If the inequality*

$$r_p(\mathrm{Cl}_S(F))\geq 2+2\sqrt{r_1(F)+r_2(F)+\delta+|S\smallsetminus S_\infty|}$$

holds, then the group Σ_F is not p-adic analytic.

Proof When S is the empty set, this theorem has been proved independently by Boston [1] and Hajir [5]. For a general nonempty S, this was proved in [8, Lemma 2.3]. ∎

Collecting all the information we have, we obtain the following result, which answers an analogue of Stark's question, namely the growth of the p-rank of the Selmer groups.

Theorem 6.2 *Let p be a prime such that the inequality*

$$r_p(\mathrm{Cl}_S(F)) \geq 2 + 2\sqrt{r_1(F) + r_2(F) + \delta + |S \smallsetminus S_\infty|}$$

holds. Suppose that A is an Abelian variety over F satisfying either of the two conditions in Proposition 4.1. Let F_∞ be the maximal unramified p-extension of F in which all primes of a given set S split completely, and let F_n be defined as above. Then for big enough n, we have the inequality

$$r_p\big(S(A/F_n)\big) \geq r_p\big(\mathrm{Cl}_S(F_n)\big)\, r_p\big(A(F_\infty)[\phi]\big).$$

In particular, if $A(F)[\phi] \neq 0$, then the p-rank of $S(A/F_n)$ is unbounded as n tends to infinity.

Proof It follows from [8, Theorem 2.5] that $A(F_\infty)[p^\infty]$ is finite. Since ϕ is assumed to have degree a power of p, we have that $A[\phi^\infty]$ is also contained in $A[p^\infty]$. Therefore, for big enough n, the group Σ_n acts trivially on $A(F_\infty)[\phi^\infty]$. Therefore, the required inequality follows from Lemma 3.2 and Propositions 4.1 and 4.2. The second assertion then follows from Lemma 3.3 and Theorem 6.1. ∎

We end the section discussing how one can obtain examples of Theorem 6.2, if one allows a change of the base field F. Now let A be an abelian variety that satisfies either of the two conditions in Proposition 4.1. Replacing F if necessary, we may assume that $A(F)[\phi] \neq 0$. Now choose a finite p-extension M of F such that

$$r_p(\mathrm{Cl}_S(M)) \geq 2 + 2\sqrt{r_1(M) + r_2(M) + \delta + |S \smallsetminus S_\infty|},$$

where we abuse notation denoting the set of primes of M above S (which is originally a finite set of primes of F) by S. Such a choice of M satisfying the inequality is possible by [15, Chap. X, Proposition 10.10.3] (see also the proof of [15, Chap. X, Corollary 10.10.6]). Combining our discussion with Theorem 6.2, we have the following result.

Proposition 6.3 *Suppose that A is an Abelian variety over F satisfying either of the two conditions in Proposition 4.1. Then there exists a finite extension M of F such that the conditions (and hence the conclusions) of Theorem 6.2 hold.*

7 Concluding Remarks

We make some remarks about Theorem 6.2 and its relation to works of [8, 11, 14].

- If the Abelian variety A satisfies Proposition 4.1(i), then this theorem is a special case of [8, Theorem A].
- This result, in some sense, is a generalization of a variant of [14, Theorem 4]. Note that in their paper, Murty and Ouyang proved the theorem for $\mathfrak{p}$-rank of the Selmer group of an elliptic curve with complex multiplication in an infinite p-class field tower, which is a finer version than our result in the case of an elliptic curve.
- In their paper, Mazur and Rubin [11, Theorem 2.19] have an analogue of Theorem 6.2. Namely, if A is an elliptic curve over $\mathbb{Q}$ with Selmer group of an odd $\mathbb{Z}_p$-corank, and F is an imaginary quadratic field F of discriminant prime to p with an infinite p-Hilbert class field, then the $\mathbb{Z}_p$-corank of its p-power Selmer group

grows to infinity over the infinite p-Hilbert class field. Note that in their result, they are considering $\mathbb{Z}_p$-corank, and they do not require the assumption that the infinite p-Hilbert class field is not p-adic analytic.

Acknowledgment The authors would like to thank the anonymous referee for comments that improved the clarity of the paper.

References

[1] N. Boston, *Some cases of the Fontaine-Mazur conjecture.* J. Number Theory **42**(1992), no. 3, 285–291. http://dx.doi.org/10.1016/0022-314X(92)90093-5
[2] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*. In: Elliptic curves, modular forms and Fermat's last theorem (Hong Kong 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 41–78.
[3] E. S. Golod and I. R. Šafarevič, *On the class field tower.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **28**(1964), 261–272.
[4] R. Greenberg, *Galois theory for the Selmer group of an Abelian variety.* Compositio Math. **136**(2003), no. 3, 255–297. http://dx.doi.org/10.1023/A:1023251032273
[5] F. Hajir, *On the growth of p-class groups in p-class towers.* J. Algebra **188**(1997), no. 1, 256–271. http://dx.doi.org/10.1006/jabr.1996.6849
[6] K. Iwasawa, *On the μ-invariants of $\mathbb{Z}_l$-extensions.* In: Number theory, algebraic geometry and commutative algebra, in honour of Yasuo Akizuki, Kinokuniya, Tokyo, 1973, pp. 1–11.
[7] A. Lubotzky and A. Mann, *Powerful p-groups. II. p-adic analytic groups.* J. Algebra **105**(1987), no. 2, 506–515. http://dx.doi.org/10.1016/0021-8693(87)90212-2
[8] A. Matar, *Selmer groups and generalized class field towers.* Int. J. Number Theory **8**(2012), no. 4, 881–909. http://dx.doi.org/10.1142/S1793042112500522
[9] B. Mazur, *Rational points of Abelian varieties with values in towers of number fields.* Invent. Math. **18**(1972), 183–266. http://dx.doi.org/10.1007/BF01389815
[10] B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants.* Ann. of Math. **166**(2007), no. 2, 579–612. http://dx.doi.org/10.4007/annals.2007.166.579
[11] B. Mazur and K. Rubin, *Growth of Selmer rank in nonabelian extensions of number fields.* Duke Math. J. **143**(2008), no. 3, 437–461. http://dx.doi.org/10.1215/00127094-2008-025
[12] P. Monsky, *p-ranks of class groups in $\mathbb{Z}_p^d$-extensions.* Math. Ann. **263**(1983), no. 4, 509–514. http://dx.doi.org/10.1007/BF01457057
[13] D. Mumford, *Abelian varieties*. Second ed., Tata Institute of Fundamental Research Studies in Mathematics, 5, Oxford University Press, London, 1974.
[14] V. K. Murty and Y. Ouyang, *The growth of Selmer ranks of an Abelian variety with complex multiplication.* Pure Appl. Math. Q. **2**(2006), no. 2, 539–555. http://dx.doi.org/10.4310/PAMQ.2006.v2.n2.a7
[15] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*. Second ed., Grundlehren der Mathematischen Wissenschaften, 323, Springer-Verlag, Berlin, 2008.
[16] J.-P. Serre and J. Tate, *Good reduction of abelian varieties.* Ann. of Math. **88**(1968), 492–517. http://dx.doi.org/10.2307/1970722

School of Mathematics and Statistics, Central China Normal University, NO.152, Luoyu RoadWuhan Hubei430079, China
e-mail: limmf@mail.ccnu.edu.cn

Department of Mathematics, University of Toronto, 40 St. George St., Toronto ON, M5S 2E4 Canada
e-mail: murty@math.toronto.edu