Pure and Applied Mathematics Quarterly
Volume 2, Number 2
(*Special Issue: In honor of
John H. Coates, Part 2 of 2*)
539—555, 2006

The Growth of Selmer Ranks of an Abelian Variety with Complex Multiplication

V. Kumar Murty and Yi Ouyang

Abstract: Let K be a CM field and $\mathcal{O}$ be its ring of integers. Let p be an odd prime integer and $\mathfrak{p}$ be a prime in K lying above p. Let F be a Galois extension of K unramified over $\mathfrak{p}$. For an Abelian variety A defined over F with complex multiplication by $\mathcal{O}$, we study the variation of the $\mathfrak{p}$-ranks of the Selmer groups in pro-p algebraic extensions. We first study the $\mathbb{Z}_p$-extension case. When K is quadratic imaginary and E is an elliptic curve, we also study the $\mathfrak{p}$-ranks of the Selmer groups in an unramified p-class field tower.

1. Introduction

Let F be a number field and A an Abelian variety defined over F. The Mordell-Weil theorem states that the group of rational points $A(F)$ is finitely generated. In particular, this group has a well-defined rank:

$$r(A,F) \ = \ \mathrm{rank}_{\mathbb{Z}} A(F).$$

On the other hand, $A(\overline{F})$ is a divisible group. One can ask how the rank changes as F varies over a family of fields. In particular, if we consider a tower of fields

$$F \ = \ F_0 \ \subseteq \ F_1 \ \subseteq \ \cdots \ \subseteq F_n \ \cdots \ \subset \ \overline{F},$$

what can be said about the sequence

$$r(A,F_n)?$$

This problem was studied by Mazur [14] in the case that the tower of fields defines a $\mathbb{Z}_p$ extension. Mazur developed an analogue of Iwasawa theory for this

Received December 23, 2005.
*2000 Mathematics Subject Classification.*Primary 11G05 11G15.
Research partially supported by grants from NSERC (Discovery and Strategic Projects) and by Project 10341001 from NSFC and by SRF for ROCS, SEM.

context. Surprisingly, it turns out that under some conditions on A and the tower, the sequence of ranks can stay bounded.

Related to the group of rational points is the Selmer group. One can also ask about the rank of this group (or more precisely, a p-primary component of it) in the same tower. The work of Mazur and more recently of Coates and of Greenberg [10] throws considerable light on this question.In particular, Greenberg has managed to develop a theory that applies not just to $\mathbb{Z}_p$ extensions, but to Galois extensions whose group is p-adic analytic.

Using the techniques developed by them, we will study the growth of Selmer ranks for Abelian varieties with complex multiplication and in certain towers not covered by the general theory of Greenberg. In particular, consider an elliptic curve E with multiplication by an order in an imaginary quadratic field K. Suppose that E and its endomorphisms are defined over a number field F, and consider the p-class field tower of F for certain primes p. This is a tower of fields, each member of which is the p-Hilbert class field of the preceding member. Under some conditions on F, it is known from the work of Golod and Shafarevich that this class field tower is infinite. It is also known that this tower defines an infinite Galois extension of F whose Galois group is *not* a p-adic analytic group, and in particular, Greenberg's theory does not apply. Under some hypotheses on E, we show that the rank of the Selmer group in such a tower does not stay bounded.

2. Acknowledgement

This work was started when the second author was visiting the GANITA Lab at the University of Toronto at Mississauga. He would like to acknowledge the hospitality and friendly working conditions provided by the Lab.

3. Selmer groups of Abelian varieties

3.1. **Notations.** Let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$. Let p be a fixed prime number. Let F be a fixed number field. We assume F and all its algebraic extensions appearing in this paper are contained in $\overline{\mathbb{Q}}$. Thus $\overline{F} = \overline{\mathbb{Q}}$. For any subfield L of $\overline{\mathbb{Q}}$, G_L is defined to be $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$. For any Galois extension L/K, $G_{L/K}$ is the Galois group of L/K.

Let v be a place of F. For every place η of L above v, we define L_η to be the union of the completions of finite subextensions of L/F at η. Write $G_{L_\eta} = \mathrm{Gal}(\overline{F_v}/L_\eta)$.

Let $M \xrightarrow{\phi} N$ be a homomorphism of abelian groups(resp. modules etc), we denote by $M[\phi]$ the kernel of ϕ. If $M = N$, we denote by M_ϕ the union of all

$M[\phi^n]$ for $n \in \mathbb{N}$, i.e.,

$$M_\phi = \varinjlim_n M[\phi^n].$$

3.2. **A brief review of Selmer groups.** We assume that L/F is an algebraic extension of F. Let A, B be two Abelian varieties defined over F. Suppose an isogeny

$$\phi : A \to B$$

is given. Then the short exact sequence

$$0 \to \ker \phi \to A \to B \to 0$$

gives rise to the following fundamental short exact sequence

$$0 \to B(L)/\phi A(L) \xrightarrow{\kappa} H^1(L, \ker \phi) \to H^1(L, A(\overline{\mathbb{Q}}))[\phi] \to 0 \tag{1}$$

by Galois cohomology. The connecting homomorphism κ is defined as follows. For $b \in B(L)$, choose $a \in A(\overline{\mathbb{Q}})$ such that $\phi(a) = b$, then $\kappa(b)$ is the cohomological class associated to the cocycle

$$\kappa(b)(\sigma) = a^\sigma - a, \ \forall \sigma \in G_L.$$

Let v be a place of F. For every place η of L above v, we get a local exact sequence analogous to (1). If we regard G_{L_η} as a subgroup of G_L, then the restriction map from $H^1(L, -)$ to $H^1(L_\eta, -)$ yields the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \frac{B(L)}{\phi A(L)} & \xrightarrow{\kappa} & H^1(L, \ker\phi) & \longrightarrow & H^1(L, A(\bar{F}))[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \frac{B(L_\eta)}{\phi A(L_\eta)} & \xrightarrow{\kappa_\eta} & H^1(L_\eta, \ker\phi) & \longrightarrow & H^1(L_\eta, A(\bar{F}_v))[\phi] & \longrightarrow & 0
\end{array}$$

The *Selmer group* of A over L with respect to the isogeny ϕ, is the group

$$\mathrm{Sel}_A(L)[\phi] = \bigcap_\eta \ker(H^1(L, \ker\phi) \to H^1(L_\eta, A(\overline{F_v}))[\phi]).$$

The *Shafarevich-Tate group* of A over L is the group

$$Ш_A(L) = \bigcap_\eta \ker(H^1(L, A(\overline{F})) \to H^1(L_\eta, A(\overline{F_v})).$$

Easily by diagram chasing, these two groups and the Mordell-Weil group are related by the following important fundamental exact sequence

$$0 \to B(L)/\phi A(L) \to \mathrm{Sel}_A(L)[\phi] \to Ш_A(L)[\phi] \to 0. \tag{2}$$

Now assume $A = B$. We consider the isogenies ϕ^n for every $n \geq 1$. For every pair (n, m) such that $n \leq m$, we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{A(L)}{\phi^n A(L)} & \longrightarrow & H^1(L, \ker \phi^n) & \longrightarrow & H^1(L, A(\overline{F})[\phi^n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \frac{A(L)}{\phi^m A(L)} & \longrightarrow & H^1(L, \ker \phi^m) & \longrightarrow & H^1(L, A(\overline{F})[\phi^m] & \longrightarrow & 0 \end{array}$$

where the vertical maps are natural injections. Furthermore, the local analogue of the above diagram also holds and the restriction maps are compatible with the diagrams. Thus they induce the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{A(L)}{\phi^n A(L)} & \longrightarrow & \mathrm{Sel}_A(L)[\phi^n] & \longrightarrow & Ш_A(L)[\phi^n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \frac{A(L)}{\phi^m A(L)} & \longrightarrow & \mathrm{Sel}_A(L)[\phi^m] & \longrightarrow & Ш_A(L)[\phi^m] & \longrightarrow & 0 \end{array}$$

Taking the direct limit, one has the exact sequence

$$0 \to \varinjlim_n A(L)/\phi^n A(L) \to \varinjlim_n \mathrm{Sel}_A(L)[\phi^n] \to \varinjlim_n Ш_A(L)[\phi^n] \to 0. \tag{3}$$

The ϕ-primary part of the Selmer group $\mathrm{Sel}_A(L)$ is then defined to be

$$\mathrm{Sel}_A(L)_\phi = \mathrm{Sel}_A(L)[\phi^\infty] = \varinjlim_n \mathrm{Sel}_A(L)[\phi^n].$$

3.3. **A five term exact sequence.** This subsection follows Greenberg's exposition ([9]). We identify $H^1(L_\eta, A(\overline{F}_v))[\phi^\infty]$ with

$$\mathcal{H}_A(L_\eta) = \frac{H^1(L_\eta, \ker \phi^\infty)}{\mathrm{im}\, \kappa_\eta},$$

where the local Kummer mapping is the map

$$\kappa_\eta : \varinjlim_n A(L_\eta)/\phi^n A(L_\eta) \to H^1(L_\eta, \ker \phi^\infty).$$

Denote by $\mathcal{P}_A(L)$ the product of $\mathcal{H}_A(L_\eta)$ for all primes η of L. Then

$$\mathrm{Sel}_A(L)_\phi = \ker(H^1(L, \ker \phi^\infty) \to \mathcal{P}_A(L)).$$

Put

$$\mathcal{G}_A(L) = \mathrm{im}(H^1(L, \ker \phi^\infty) \to \mathcal{P}_A(L)),$$

then one has an exact sequence

$$0 \to \mathrm{Sel}_A(L)_\phi \to H^1(L, \ker \phi^\infty) \to \mathcal{G}_A(L) \to 0. \tag{4}$$

Suppose furthermore that the extension L/F is a Galois extension. Write $G = \mathrm{Gal}(L/F)$. For every intermediate field F' of L/F, write $G(L/F') = \mathrm{Gal}(L/F')$. One has the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Sel}_A(F')_\phi & \longrightarrow & H^1(F', \ker\phi^\infty) & \longrightarrow & \mathcal{G}_A(F') & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle s_{L/F'}} & & \downarrow{\scriptstyle h_{L/F'}} & & \downarrow{\scriptstyle g_{L/F'}} & & \\ 0 & \longrightarrow & \mathrm{Sel}_A(L)_\phi^{G(L/F')} & \longrightarrow & H^1(L, \ker\phi^\infty)^{G(L/F')} & \longrightarrow & \mathcal{G}_A(L)^{G(L/F')} & & \end{array}$$

where the vertical maps $s_{L/F'}$, $h_{L/F'}$ and $g_{L/F'}$ are natural restrictions. The snake lemma then gives the exact sequence:

$$0 \to \ker s_{L/F'} \to \ker h_{L/F'} \to \ker g_{L/F'} \to \mathrm{coker}\, s_{L/F'} \to \mathrm{coker}\, h_{L/F'}. \tag{5}$$

This five term exact sequence is of extreme importance in our paper.

3.4. **Two types of isogenies.** Let us consider two types of isogenies.

(i) Let the isogeny ϕ be the multiplication-by-p map. Then

$$\varinjlim_n A(L)/p^n A(L) = A(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

and $\ker\phi^\infty = A[p^\infty]$. The study of the natural restriction

$$s_{L/F'} : \mathrm{Sel}_A(F')_p \longrightarrow \mathrm{Sel}_A(L)_p^{G(L/F')}$$

is the so called *control problem* in the study of arithmetic of Abelian varieties. Mazur's famous control theorem is the following result.

Theorem 1 (Mazur)**.** *If L/F is a $\mathbb{Z}_p$-extension, assuming that A has good ordinary reduction at all primes of F lying over p, then* $\ker s_{L/F'}$ *and* $\mathrm{coker}\, s_{L/F'}$ *are finite and bounded as F' varies over finite extensions of F inside L.*

Greenberg's exposition [9] formulated a general plan to attack this problem by using the above exact sequence (5). Namely, through the study of the behavior of $\ker h_{L/F'}$, $\mathrm{coker}\, h_{L/F'}$ and $\ker g_{L/F'}$ as F' varies, one can get information about $\ker s_{L/F'}$ and $\mathrm{coker}\, s_{L/F'}$. The kernel and cokernel of $h_{L/F'}$ are not hard to describe, and are given by the inflation-restriction sequence. However, $\ker g_{L/F'}$ is much more difficult to study.

In the definition of $g_{L/F'}$, the local restriction map was extensively involved. For every prime v' of F' and a prime η of L over v, let $r_{v'} = r_{v',\eta}$ be the local restriction map $\mathcal{H}_A(F'_{v'}) \to \mathcal{H}_A(L_\eta)$. Let $r_{L/F'}$ be the restriction map $\mathcal{P}_A(F') \to \mathcal{P}_A(L)$. By carefully studying $r_{v'}$ and hence $r_{L/F'}$, Greenberg obtained information about $\ker g_{L/F'}$, and thus obtained generalized control theorems for the case that G is a p-adic analytic group, in particular, the cases $G = \mathbb{Z}_p$ and $L = F(A[p^\infty])$.

(ii) In this paper, we are interested in another type of isogeny. Let K be a CM-field and F/K be a Galois extension. Assume that A is an Abelian variety defined over F and having complex multiplication by the ring of integers $\mathcal{O}_K$ of K. Let $\mathfrak{p}$ be a prime in K lying over p. Let $\mathfrak{p}^h = (\alpha)$ for some integer $h > 0$ and $\alpha \in \mathcal{O}_K$. Then the multiplication-by-α map is an isogeny of A. Moreover, one has

$$\varinjlim_n A(L)/\alpha^n A(L) = A(L) \otimes K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}$$

and $\ker \alpha^\infty = A[\mathfrak{p}^\infty]$. For L/F a Galois extension with profinite Galois group G, the $\mathfrak{p}$-primary control problem then is

Question 1. *What can one say about the behaviors of the kernel and cokernel of the restriction map*

$$s_{L/F'} : \mathrm{Sel}_A(F')_{\mathfrak{p}} \longrightarrow \mathrm{Sel}_A(L)_{\mathfrak{p}}^{G(L/F')}$$

as F' varies over finite extensions of F inside L?

We shall study two cases in this paper. The first is the case that A is a general Abelian variety with complex multiplication and L/F is a $\mathbb{Z}_p$-extension. In this case, we will give a theorem(Theorem 2) in § 4, which is an analogue of Mazur's control Theorem. It is very likely known to the experts but we could not find an appropriate reference. The second is the case that the Abelian variety is actually an elliptic curve E and the extension L/F is an infinite class field extension. Note that L/F is a non-Abelian extension in this case. Our main result is stated in Theorem 4 in §4.

4. The $\mathbb{Z}_p$-extension case

In this section, we let K be a CM field and F/K be a Galois extension. Let $\mathcal{O}$ be the ring of integers of K. Let A be an Abelian variety defined over F and with complex multiplication by $\mathcal{O}$. Let $\mathfrak{p}$ be a prime of K lying over p. Let L/F be a $\mathbb{Z}_p$-extension with Galois group Γ. We shall prove the following theorem in this section.

Theorem 2. *Assume that A has good ordinary reduction at all primes of F lying over $\mathfrak{p}$. Then the natural maps*

$$s_{L/F_n} : \mathrm{Sel}_A(F_n)_{\mathfrak{p}} \to \mathrm{Sel}_A(L)_{\mathfrak{p}}^{\mathrm{Gal}(L/F_n)}$$

has finite kernel and cokernel of bounded order as n varies, where F_n is the unique subextension of order p^n in L/F.

To prove the above theorem, we are going to use the exact sequence (5). Write $\Gamma_n = \mathrm{Gal}(L/F_n)$, $s_{L/F_n} = s_n$, $h_{L/F_n} = h_n$ and $g_{L/F_n} = g_n$. Let us first consider $\ker h_n$ and $\mathrm{coker}\, h_n$. We have

Lemma 1. *The order of* $\ker h_n$ *is bounded as* n *varies; the cokernel* $\operatorname{coker} h_n$ *vanishes for every* $n \geq 0$.

Proof. By the inflation-restriction exact sequence, one has

$$\ker h_n = H^1(\Gamma_n, A(L)_{\mathfrak{p}}), \qquad \operatorname{coker} h_n \subseteq H^2(\Gamma_n, A(L)_{\mathfrak{p}}).$$

Since $\mathbb{Z}_p$ has cohomological dimension 1, we have $H^2(\Gamma_n, A(L)_{\mathfrak{p}}) = 0$ and thus $\operatorname{coker} h_n$ vanishes. Let γ be a topological generator of Γ, then γ^{p^n} is a topological generator of Γ_n. We have

$$H^1(\Gamma_n, A(L)_{\mathfrak{p}}) = A(L)_{\mathfrak{p}}/(\gamma^{p^n} - 1)A(L)_{\mathfrak{p}}.$$

Treating $\gamma^{p^n} - 1$ as an endomorphism of $A(L)_{\mathfrak{p}}$, one see easily that the kernel of it is just $A(F_n)_{\mathfrak{p}}$, a finite group. Thus

$$(\gamma^{p^n} - 1)(A(L)_{\mathfrak{p}})_{div} = (A(L)_{\mathfrak{p}})_{div},$$

and so

$$|A(L)_{\mathfrak{p}}/(\gamma^{p^n} - 1)A(L)_{\mathfrak{p}}| \leq [A(L)_{\mathfrak{p}} : (A(L)_{\mathfrak{p}})_{div}],$$

which is finite and independent of n. □

Let v be a place in F. Let v_n be a place of F_n lying over v and let η be a place in L lying above v_n. We consider the kernel of the restriction map

$$r_{v_n} : \mathcal{H}_A((F_n)_{v_n}) \to \mathcal{H}_A(L_\eta).$$

(i) If v is archimedean, then v splits completely in L/F, i.e., $F_v = L_\eta$, hence $\ker r_{v_n} = 0$.

(ii) If v non-archimedean, and $v \nmid \mathfrak{p}$, then we claim that $\operatorname{im} \kappa_{v_n} = \operatorname{im} \kappa_\eta = 0$. Indeed, $A((F_n)_{v_n}) \otimes K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}$ is a divisible group for $v_n \nmid \mathfrak{p}$. On the other hand, $H^1((F_n)_{v_n}, A[\mathfrak{p}^\infty])$ is a finite group, so that $\operatorname{im} \kappa_{v_n} = 0$. Similarly one has $\operatorname{im} \kappa_\eta = 0$. (One can also prove this claim by using Mattuck's Theorem that for a local field K, $A(K) = \mathcal{O}_K^{\dim A} \times U$ where U is a finite group.)

By the inflation-restriction sequence, then

$$\ker r_{v_n} = H^1(L_\eta/(F_n)_{v_n}, A(L_\eta)_{\mathfrak{p}}).$$

(ii-a) If $v \nmid p$, then v is unramified in the extension L/F. If v splits completely in L/K, $\ker r_{v_n}$ is trivial.

If v does not split completely in L/K, there are finitely many primes v_n of F_n and η of L lying over v. Let I_v be the inertia subgroup of $G_{F_v} = \operatorname{Gal}(\overline{F_v}/F_v)$. Let

$F_v^{ur} = \overline{F_v}^{I_v}$ be the maximal unramified extension of F_v. Then $\ker r_{v_n}$ is bounded by the order of $\ker(H^1((F_n)_{v_n}, A[\mathfrak{p}^\infty]) \to H^1(F_v^{ur}, A[\mathfrak{p}^\infty])$, which is given by

$$H^1(F_v^{ur}/(F_n)_{v_n}, A(F_v^{ur})_\mathfrak{p}) \cong A(F_v^{ur})_\mathfrak{p}/(\sigma - 1)A(F_v^{ur})_\mathfrak{p},$$

where σ is a topological generator of $\mathrm{Gal}(F_v^{ur}/(F_n)_{v_n})$. Since the kernel of $\sigma - 1$ acting on $A(F_v^{ur})_\mathfrak{p}$ is finite(it is just $A((F_n)_{v_n})_\mathfrak{p})$, so the cokernel of $\sigma - 1$ is also finite. Thus

$$(A(F_v^{ur})_\mathfrak{p})_{div} \subseteq (\sigma - 1)A(F_v^{ur})_\mathfrak{p} \subseteq A(F_v^{ur})_\mathfrak{p}.$$

Hence

$$|\ker r_{v_n}| \leq [A(F_v^{ur})_\mathfrak{p} : (A(F_v^{ur})_\mathfrak{p})_{div}],$$

an absolute constant independent of n. In particular, if A has good reduction at v, then the action of I_v on $A[\mathfrak{p}^\infty]$ is also trivial, hence $A(F_v^{ur})_\mathfrak{p} = A[\mathfrak{p}^\infty]$, a divisible group, so $\ker v_n = 0$.

(ii-b) If $v \mid p$ but $v \nmid \mathfrak{p}$, we want to show that $\ker r_{v_n}$ has bounded order. The reason for the case that v is unramified in the extension L/F is the same as $v \nmid p$. We also have $\ker v_n = 0$ if A has good reduction at v. Now if v is ramified in L/F, then v_n is totally ramified in the extension L/F_n for $n \gg 0$, thus the finite residue field f_{v_n} of v_n stabilizes to the residue field l_η of η. The fact that $\ker r_{v_n}$ has bounded order follows from the same reason in the proof of Lemma 1. In this case, $\ker r_{v_n}$ may not vanish even when A has good reduction at v. But the number of v_n lying above v stabilizes as $n \to \infty$.

Combining the above analysis, we have

Lemma 2. *For every n, the product $\bigoplus_{v_n \nmid \mathfrak{p}} \ker r_{v_n}$ over all primes $v_n \nmid \mathfrak{p}$ in F_n is a finite set bounded by an absolute constant independent of n.*

(iii) Now we discuss the case $v \mid \mathfrak{p}$. By our assumption, A has good ordinary reduction at v. We let $\Gamma_{v_n} = \mathrm{Gal}(L_\eta/(F_n)_{v_n})$. If v is unramified at L/F, by the proof of Proposition 2.3 of Greenberg [9], we know that $\ker r_{v_n} = 0$ for all v_n.

Now suppose v is ramified at L/F, then v_n is totally ramified for $n \gg 0$. Let $\mathcal{F}$ be the formal group attached to the Néron model of A at the local field F_v. Fix an algebraic closure $\overline{F_v}$ of F_v. Let $\overline{\mathfrak{m}}$ be the maximal ideal of $\overline{F_v}$. We assume L_η is contained in $\overline{F_v}$. The choice of $\overline{F_v}$ is not essential. As A has good ordinary reduction at v, $\dim A = \text{height } \mathcal{F}$ and we denote it by g. We have an exact sequence

$$0 \to \mathcal{F}(\overline{\mathfrak{m}}) \to A \to \tilde{A} \to 0$$

where $\tilde{A}$ is the reduction of A modulo v. Set $C = C_\mathfrak{p} = \mathcal{F}(\overline{\mathfrak{m}})[\mathfrak{p}^\infty]$. Then

$$0 \to C \to A[\mathfrak{p}^\infty] \to \tilde{A}_\mathfrak{p} \to 0.$$

The inclusion of $C \hookrightarrow A[\mathfrak{p}^\infty]$ induces a map

$$\lambda_M : H^1(M, C) \to H^1(M, A[\mathfrak{p}^\infty])$$

for every algebraic extension M of F_v.

In the paper [4], Coates-Greenberg studied the corresponding p-case, i.e., $C_p = \mathcal{F}(\overline{\mathfrak{m}})[p^\infty]$, $D_p = A[p^\infty]/C_p$. The inclusion of $C_p \hookrightarrow A[p^\infty]$ induces a map

$$\lambda_{M,p} : H^1(M, C_p) \to H^1(M, A[p^\infty])$$

for every algebraic extension M of F_v. According to (4.9) of [4], $\operatorname{im}\kappa_{M,p} \subseteq \operatorname{im}\lambda_{M,p}$, and by Propositions 4.3 and 4.4 of [4],

$$\operatorname{im}(\lambda_{F_{v_n},p})_{div} = \operatorname{im}(\kappa_{F_{v_n},p}), \quad \operatorname{im}(\lambda_{L_\eta,p}) = \operatorname{im}(\kappa_{L_\eta,p}).$$

Returning to our case, let M be a finite extension of F_v. We know that κ_M is injective and $\operatorname{im}\kappa_M$ is divisible. By Mattuck's theorem, the $\mathbb{Z}_p$-corank of $\operatorname{im}\kappa_M$ is $g \cdot [M : \mathbb{Q}_p]$. As for $H^1(M, A[\mathfrak{p}^\infty])$, using Poitou-Tate local duality theorem, the $\mathbb{Z}_p$-corank is also $g \cdot [M : \mathbb{Q}_p]$ since the $\mathbb{Z}_p$-corank of $A[\mathfrak{p}^\infty]$ is g. We see that $\operatorname{coker}\kappa_M$ in fact is finite.

Following the same argument of Greenberg [8, Page 64], one shows that $\operatorname{im}\kappa_M \subset \operatorname{im}\lambda_M$. As $\ker\lambda_M$ is finite, $H^1(M, C)$ then is also of $\mathbb{Z}_p$-corank $g \cdot [M : \mathbb{Q}_p]$. By using Poitou-Tate local duality theorem again, the $\mathbb{Z}_p$-corank of C must also be g and thus $\operatorname{im}\kappa_M = (\operatorname{im}\lambda_M)_{div}$.

Note that $\operatorname{im}\lambda_M/(\operatorname{im}\lambda_M)_{div}$ has order bounded by $|\tilde{A}(m)_\mathfrak{p}|$ where m is the residue field of M. For the $\mathbb{Z}_p$-extension L_η/F_v, we write $\lambda_{F_{v_n}}$, $\kappa_{F_{v_n}}$, r_{v_n} as λ_n, κ_n and r_n for simplicity. Since the residue fields f_{v_n} stabilize for $n \gg 0$, hence $\operatorname{im}(\lambda_{L_\eta})/\operatorname{im}(\kappa_{L_\eta})$ is a finite group. On the other hand, G_{L_η} has p-cohomological dimension 1, then $H^1(L_\eta, C)$ is divisible and

$$\operatorname{im}(\lambda_{L_\eta}) = \operatorname{im}(\kappa_{L_\eta}).$$

Then from

$$\mathcal{H}_A(F_{v_n}) \xrightarrow{a_n} H^1(F_{v_n}, A[\mathfrak{p}^\infty])/\operatorname{im}\lambda_n \xrightarrow{b_n} \mathcal{H}_A(L_\eta),$$

we have

$$\ker a_n \cong \operatorname{im}(\lambda_n)/\operatorname{im}(\kappa_n), \qquad \ker r_n/\ker a_n = \ker b_n.$$

Now $\ker a_n$ is just $\operatorname{im}(\lambda_n)/\operatorname{im}(\lambda_n)_{div}$. The order of $\ker a_n$ is equal to the $\mathfrak{p}$-part of $\tilde{A}(f_n)$, which is bounded by a finite number independent of n. As for $\ker b_n$, by the exact sequence

$$0 \to C \to A[\mathfrak{p}^\infty] \to \tilde{A}_\mathfrak{p} \to 0$$

and a diagram chasing as in Greenberg [9, Page 19], one has

$$\ker b_n \subset \ker(H^1(F_{v_n}, \tilde{A}_\mathfrak{p}) \xrightarrow{d_n} H^1(L_\eta, \tilde{A}_\mathfrak{p}) = H^1(L_\eta/F_{v_n}, \tilde{A}(L_\eta)_\mathfrak{p}).$$

The last term again has an order of $\tilde{A}(f_n)_{\mathfrak{p}}$ for $n \gg 0$, bounded and independent of n. Thus we have

Lemma 3. *Let $v \mid \mathfrak{p}$. Suppose v is ramified in a $\mathbb{Z}_p$-extension L/F, then the kernel of*

$$r_{v_n} : \mathcal{H}_A((F_n)_{v_n}) \to \mathcal{H}_A(L_\eta)$$

is bounded by $|\tilde{A}(f_n)_{\mathfrak{p}}|^2$ for $n \gg 0$.

Lemma 4. *As n varies, the product $\bigoplus_{v_n|\mathfrak{p}} \ker r_{v_n}$ over all primes $v_n \mid \mathfrak{p}$ in F_n is a finite set bounded by an absolute constant independent of n.*

By Lemmas 2 and 4, $\ker g_n$ is of finite order and bounded, and by Lemma 1, $\ker h_n$ and $\operatorname{coker} h_n$ are finite and bounded, we thus finish the proof of Theorem 2,

5. Infinite class field tower

Let p be a fixed prime number. Let F be a number field. Let F_∞ be the maximal unramified p-extension of F and put $\Gamma = \Gamma_F = \mathrm{Gal}(F_\infty/F)$. Let $\{\Gamma_n\}_{n\geq 0}$ be the derived series of Γ. For every $n \geq 0$, the fixed field F_{n+1} corresponding to Γ_{n+1} is then the the p-Hilbert class field of F_n. Let $\rho(k)$ (resp. $\nu(k)$) denote the p-rank of the ideal class group of a number field k(resp. the rank of the unit group).

In 1964, Golod-Shafarevich [7] proved that if $\rho(F) \geq 2 + 2\sqrt{\nu(F)+1}$, then Γ is infinite, thus established for the first time the existence of infinite p-class field tower. Stark asked the following question:

> Does the p-class rank $\rho(F_n)$ of the layers in an infinite p-class field tower tend to ∞ as n tends to ∞?

One way to reformulate Stark's question is the following. For any finitely generated pro-p group G, let $\mathbb{Z}/p\mathbb{Z}$ be a G-module on which G acts trivially and set

$$h_i(G) = \dim_{\mathbb{Z}/p\mathbb{Z}} H^i(G, \mathbb{Z}/p\mathbb{Z}),\ i = 1, 2.$$

Then

$$h_1(G) = \dim_{\mathbb{Z}/p\mathbb{Z}} \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z})$$

is just the number of minimal generators of G. By Burnside's basis theorem, we know that $h_1(G) = h_1(G^{ab})$. In particular, in the p-adic class field tower case, $h_1(\Gamma_n) = \rho(F_n)$.

As H ranges over all normal open subgroups of G, the limsup and liminf of

$$\dim H^1(H, \mathbb{Z}/p\mathbb{Z})$$

are known to be equal. This common value is called the Prüfer rank of G. A theorem due to Lubotzky and Mann([13]) states that a finitely generated pro-p group G has finite Prüfer rank if and only if G is a p-adic analytic group. Now, we may ask the question

Is Γ a p-adic analytic group?

If it is not, then Stark's question has a positive answer. By a general conjecture of Fontaine-Mazur [6], we do not expect Γ to be an analytic group. The Fontaine-Mazur conjecture states the following:

Conjecture 1. *For any number field k, Γ_k has no infinite p-adic analytic quotient.*

Without assuming the Fontaine-Mazur Conjecture, recently Hajir [11] and Boston [2] proved the following theorem:

Theorem 3 (Boston-Hajir)**.** *Let F be a number field. If the Golod-Shafarevich inequality*

$$\rho(F) \geq 2 + 2\sqrt{\nu(F) + 1}$$

holds, then the group Γ is not p-adic analytic and the p-class rank $\rho(F_n)$ tends to infinity with $n \to \infty$.

6. The case of elliptic curves in an infinite class field tower

6.1. **Questions and main result.** In this section, let K be an imaginary quadratic field and $\mathcal{O} = \mathcal{O}_K$ be the ring of integers of K. Let p be an odd prime number. Assume that F is a finite Galois extension of K for which $\rho(F_n) \to \infty$ as $n \to \infty$. As we have observed in § 5, this holds if F satisfies the Golod-Shafarevich inequality or if F has an infinite p-class field tower under the Fontaine-Mazur Conjecture.

We assume $p = \mathfrak{p}\bar{\mathfrak{p}}$ splits in K and $\mathfrak{p}$ is unramified over F/K. Let E be an elliptic curve defined over F which has complex multiplication by $\mathcal{O}$. We assume that E has good ordinary reduction at all primes above $\mathfrak{p}$ in F. We write $M_{\mathfrak{p}}$ for the $\mathfrak{p}$-primary part of an $\mathcal{O}$-module M. Let r and r_n be the $\mathbb{Z}/p\mathbb{Z}$-ranks of $\mathrm{Sel}_E(F_\infty)_p[p]$ and $\mathrm{Sel}_E(F_n)_p[p]$ respectively. By analogy with Stark's question, we would like to ask the following two questions about r and r_n:

(1). Is r_n bounded? If not, is it true that $r_n \to \infty$ if $n \to \infty$?
(2). Is it true that $r = \infty$?

In the following, the $\mathfrak{p}$-rank of an $\mathcal{O}$-module M is defined to be the $\mathbb{Z}/p\mathbb{Z}$-rank of $M_{\mathfrak{p}}[\mathfrak{p}]$. We will prove the following result.

Theorem 4. *Let F be a number field containing the imaginary quadratic field K and satisfying*

$$\rho(F) \ \geq \ 2 + 2(\nu(F)+1)^{1/2}.$$

Let E be an elliptic curve defined over F with complex multiplication by K. Assume that $\mathfrak{p}$ is a prime in K splitting over p and unramified in F/K. Suppose for every prime v at F above $\mathfrak{p}$, E has good ordinary reduction at v and $\tilde{E}(f_v)_{\mathfrak{p}} = 0$ where f_v is the residue field of F_v.

Let F_∞ be the maximal unramified nonconstant pro-p extension of F and F_n be the n-th layer of the p-class field tower F_∞/F. Then

(1). The $\mathfrak{p}$-rank of the Selmer group of E over F_n is unbounded as $n \to \infty$.

(2). If furthermore, $E(F)_p = 0$, then the $\mathfrak{p}$-rank of the Selmer group of E over F_∞ is infinite. Thus either the Mordell-Weil rank or the $\mathfrak{p}$-rank of the Shafarevich-Tate group of E over F_∞ is infinite.

6.2. **Preliminaries.** Before we begin the proof of Theorem 4, we make some preliminary remarks. Since $\mathfrak{p}$ splits completely in $K/\mathbb{Q}$, we have

$$E[\mathfrak{p}] \cong \mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathbb{Z}/p\mathbb{Z}$$

and

$$E[\mathfrak{p}^\infty] \cong \mathbb{Z}_p$$

as abelian groups. Let $\tilde{L} = F(E[\mathfrak{p}^\infty])$ and $\tilde{L}_n = F_n(E[\mathfrak{p}^\infty])$. The action of $\mathrm{Gal}(\tilde{L}/F)$ on $E[\mathfrak{p}^\infty]$ defines a canonical injection

$$\chi_\infty : \mathrm{Gal}(\tilde{L}/F) \hookrightarrow \mathbb{Z}_p^\times$$

whose image is of finite index in $\mathbb{Z}_p^\times$. Via χ_∞, the decomposition of $\mathbb{Z}_p^\times = \mu_{p-1} \times (1+p\mathbb{Z}_p)$ rises to the corresponding decomposition of $\mathrm{Gal}(\tilde{L}/F)$ as $\Delta \times \Gamma'$, where Δ is a subgroup of μ_{p-1} and Γ' is a subgroup of $1+p\mathbb{Z}_p$. Let L be the unique $\mathbb{Z}_p$-extension of F inside $\tilde{L}$ which is fixed by Δ. The classical theory of complex multiplication shows that L is actually the composition of F and the unique $\mathbb{Z}_p$-extension of K unramified outside $\mathfrak{p}$. Let $L_n = F_n L$ for every $n \geq 0$. Then L_n/F_n is the unique $\mathbb{Z}_p$-extension inside $\tilde{L}_n$ which is unramified outside $\mathfrak{p}$. Write $\Gamma'_n = \mathrm{Gal}(L_n/F_n) \cong \mathbb{Z}_p$. Then for every $n \geq 0$

$$\mathrm{Gal}(\tilde{L}_n/L_n) \cong \mathrm{Gal}(\tilde{L}/L) = \Delta \text{ and } \mathrm{Gal}(\tilde{L}_n/F_n) = \Delta \times \Gamma'_n.$$

We have the following elementary but useful lemma:

Lemma 5. *Let G be a pro-p group and A be a discrete p-primary G-module. Then $A = 0$ if and only if $H^0(G, A) = A^G = 0$.*

Proof. First consider the case both G and A finite. By the action of G on A, A is the disjoint union of G-orbits $\mathcal{O}_x = \{gx : g \in G\}$. The cardinality of $\mathcal{O}_x$ is the index of the stabilizer $G_x = \{g \in G : gx = x\}$ in G. Since $G_x = G$ if and only if $x \in A^G$, if $x \notin A^G$, $[G : G_x] = 0 \bmod p$. Therefore $|A^G| = |A| \bmod p$. Hence

$$A \neq 0 \Longleftrightarrow |A| = |A^G| = 0 \bmod p \Longleftrightarrow A^G \neq 0.$$

Now if G is profinite, we only need to show that if $A^G = 0$, then $A^U = 0$ for every normal open subgroup U of G. In this case, G/U is a finite p-group and A^U is a discrete G/U-module of p-power order, by the above argument, thus $A^U = 0$ if and only if $(A^U)^{G/U} = 0$, but $(A^U)^{G/U} = A^G = 0$. □

There are only two possibilities for $E[\mathfrak{p}](F)$, either trivial or the whole group $E[\mathfrak{p}]$. Hence from Lemma 5, we have

Lemma 6. *There are only two possibilities for $E(L_n)_\mathfrak{p}$: if $E[\mathfrak{p}](F)$ is trivial, then $L \neq \tilde{L}$ and $E(L_n)_\mathfrak{p} = 0$ for every $n \geq 0$; if $E[\mathfrak{p}] \subset E(F)$, then $L_n = \tilde{L}_n$ and $E(L_n)_\mathfrak{p} = E[\mathfrak{p}^\infty]$ for every $n \geq 0$.*

Lemma 7. *The intersection of F_∞ and L is a finite extension of F. In particular, if $E[\mathfrak{p}] \subset E(F)$, then F_∞ and L are disjoint over F.*

Proof. The intersection $F_\infty \cap L$ must be an abelian extension of F since L/F is abelian. However, the maximal abelian quotient of F_∞/F is nothing but the p-Hilbert class field F_1/F, hence $F_\infty \cap L \subset F_1$. In the case $E[\mathfrak{p}] \subset E(F)$, then $\tilde{L} = L$ and L/F is totally ramified over $\mathfrak{p}$. Since F_∞ is unramified over F, it follows that F_∞ and L are disjoint. □

Note that

$$\Gamma'_n = \mathrm{Gal}(L_n/F_n) = \mathrm{Gal}(L/F_n \cap L) \supseteq \mathrm{Gal}(L/F_\infty \cap L).$$

By the above lemma, Γ'_n is a subgroup of Γ' and as n varies, there are only a finite number of choices of Γ'_n since each of them must contain the open subgroup $\mathrm{Gal}(L/F_\infty \cap L)$.

Let M_n be the maximal abelian pro-p extension of $\tilde{L}_n$ unramified outside $\mathfrak{p}$ and let $\mathcal{X}_n = \mathrm{Gal}(M_n/L_n)$. Under standard techniques, $\mathcal{X}_n$ is an Iwasawa $\Lambda[\Delta] = \mathbb{Z}_p[\Delta][[T]]$-module. Moreover, we have the following result of Coates.

Theorem 5 (Coates)**.** *Let χ be the restriction of χ_∞ to Δ. Then there is a canonical pairing*

$$\mathrm{Sel}_E(L_n)_\mathfrak{p} \times \mathcal{X}_n^{(\chi)} \longrightarrow E[\mathfrak{p}^\infty]$$

which induces an isomorphism of Galois modules

$$\mathrm{Sel}_E(L_n)_\mathfrak{p} \cong \mathrm{Hom}(\mathcal{X}_n^{(\chi)}, E[\mathfrak{p}^\infty])$$

Proof. See Coates [3], Theorem 12, Page 121, or de Shalit [5], Theorem 1.5, page 124. □

6.3. **Proof of Theorem 4.** By Coates' theorem, we immediately have

Lemma 8. *The $\mathbb{Z}_p$-corank of $\mathrm{Sel}_E(L_n)_{\mathfrak{p}}$ tends to ∞ as n varies.*

Proof. By Coates' theorem, it suffices to show that the $\mathbb{Z}_p[\Delta]$-rank of $\mathcal{X}_n$ tends to ∞. However, since F_{n+1} and $\tilde{L}_n$ are both abelian extensions over F which are unramified outside $\mathfrak{p}$, their composition $\tilde{L}_{n+1}$ must also be unramified outside $\mathfrak{p}$ over F_n, and hence unramified outside $\mathfrak{p}$ over $\tilde{L}_n$. Thus $\tilde{L}_{n+1}/\tilde{L}_n$ is a subextension of $M_n/\tilde{L}_n$. Moreover, note that

$$\mathrm{Gal}(\tilde{L}_{n+1}/\tilde{L}_n) = \mathrm{Gal}(L_{n+1}/L_n) = \mathrm{Gal}(F_{n+1}/(F_{n+1} \cap L_n)).$$

Now, by Theorem 3, the p-rank of $\mathrm{Gal}(F_{n+1}/F_n)$ tends to ∞ while the p-rank of $\mathrm{Gal}((F_{n+1} \cap L_n)/F_n)$ is less than or equal to the $\mathbb{Z}_p$-rank of $\Gamma'_n = \mathrm{Gal}(L_n/F_n)$, which is 1. Therefore, the p-rank of $\mathrm{Gal}(\tilde{L}_{n+1}/\tilde{L}_n)$ tends to ∞ and hence the $\mathbb{Z}_p[\Delta]$-rank of $\mathcal{X}_n$ tends to ∞. □

Remark. Note that we have actually proved more. As $(\mathcal{X}_n)_{\Gamma'_n}$ certainly contains $\mathrm{Gal}(\tilde{L}_{n+1}/\tilde{L}_n)$, an application of Coates' theorem implies that the $\mathfrak{p}$-rank of $\mathrm{Sel}_E(L_n)_{\mathfrak{p}}^{\Gamma'_n}$ tends to ∞ as n varies.

Let $s_n = s_{L_n/F_n}$, $h_n = h_{L_n/F_n}$ and $g_n = g_{L_n/F_n}$. From the above lemma, if we can show that $\ker s_n$ and $\mathrm{coker}\, s_n$ are finite and bounded as n varies, then the rank $\mathrm{rank}_p \mathrm{Sel}_E(F_n)_{\mathfrak{p}}$ differs from $\mathrm{rank}_p \mathrm{Sel}_E(L_n)_{\mathfrak{p}}^{\Gamma'_n}$ by a bounded amount.

Following the exact sequence (5), we shall study the behavior of $\ker h_n$, $\mathrm{coker}\, h_n$ and $\ker g_n$ as n varies.

Lemma 9. *The orders of $\ker h_n$ and $\mathrm{coker}\, h_n$ vanish for every $n \geq 0$.*

Proof. By the inflation-restriction exact sequence, one has

$$\ker h_n = H^1(\Gamma'_n, E(L_n)_{\mathfrak{p}}), \qquad \mathrm{coker}\, h_n \subseteq H^2(\Gamma'_n, E(L_n)_{\mathfrak{p}}).$$

Since $\mathbb{Z}_p$ has cohomology dimension 1, we have $H^2(\Gamma'_n, E(L_n)_{\mathfrak{p}}) = 0$ and thus $\mathrm{coker}\, h_n$ vanishes. Now by Lemma 6, $E(L_n)_{\mathfrak{p}}$ is either trivial or $E[\mathfrak{p}^\infty]$.In the first case, $\ker h_n = 0$. For the second case, putting $\Gamma'_{n,m} = \mathrm{Gal}(F_n(E[\mathfrak{p}^m])/F_n)$, we have

$$\ker h_n = H^1(\Gamma'_n, E[\mathfrak{p}^\infty]) = \varinjlim H^1(\Gamma'_{n,m}, E[\mathfrak{p}^m]).$$

Now $E[\mathfrak{p}^m]$ is cyclic of order p^m and $\Gamma'_{n,m}$ is also cyclic. It is easy to show that $H^1(\Gamma'_{n,m}, E[\mathfrak{p}^m]) = 0$ (see Coates [3]), and so in this case as well, $\ker h_n = 0$. □

To study the map g_n, we first study $\ker r_v$ of the local restriction map

$$r_v : \mathcal{H}_E(F_{n,v}) \longrightarrow \mathcal{H}_E(L_{n,\eta})$$

for v a place in F_n and η a place in L_n above v. There are three cases to consider.

If $v \mid \infty$, then v splits completely in L_n/F_n and hence $\ker r_v = 0$.

If $v < \infty$ and $v \nmid \mathfrak{p}$, then $H^1(F_{n,v}, E[\mathfrak{p}^\infty])$ is finite but $E(F_{n,v}) \otimes K_\mathfrak{p}/\mathcal{O}_\mathfrak{p}$ is divisible, hence $\operatorname{im} \kappa_v = 0$. Similarly, $\operatorname{im} \kappa_\eta = 0$. Let δ be a topological generator of $\mathrm{Gal}(L_{n,\eta}/F_{n,v}) \cong \mathbb{Z}_p$, and let $B_v = E[\mathfrak{p}^\infty](L_{n,\eta})$, then by inflation-restriction,

$$\ker r_v = H^1(\langle \bar{\delta} \rangle, B_v) = B_v/(\delta - 1)B_v.$$

Since $E(F_{n,v})$ has a finite p-primary subgroup, the kernel of $\delta - 1$ acting on B_v is finite, hence $(\delta - 1)B_v \supseteq (B_v)_{div}$ and

$$|\ker r_v| \leq |B_v/(B_v)_{div}|.$$

Now since $L_{n,\eta} \subseteq F_{n,v}(E[\mathfrak{p}^\infty])$, B_v is the set of invariant elements in $E[\mathfrak{p}^\infty]$ by the Galois group of $\mathrm{Gal}(F_{n,v}(E[\mathfrak{p}^\infty])/L_{n,\eta})$, which is a subgroup of $\Delta = \mathrm{Gal}(\tilde{L}_n/L_n)$. Since the latter one is a cyclic group of order dividing $p-1$, B_v must be divisible. Therefore $\ker r_v = 0$.

Finally if $v \mid \mathfrak{p}$, by our assumption, E has good ordinary reduction at v. Now, v is (totally) ramified in the extension L_n/F_n. We let $\Gamma_v = \mathrm{Gal}(L_{n,\eta}/F_{n,v})$. Let $f_{n,v}$ be the residue field of v and l_η be the residue field of η. By Lemma 3, $\ker r_v$ is bounded by $|\tilde{E}(f_v)_\mathfrak{p}|^2 = |\tilde{E}(f_\eta)_\mathfrak{p}|^2$. Under the assumption of Theorem 4, by Lemma 5, $\tilde{E}(f_v)_\mathfrak{p} = 0$, Therefore

$$\ker r_v = 0.$$

By the above analysis, we see that $\ker g_n = 0$ for every $n \geq 1$, hence

Lemma 10. *The orders of* $\ker s_n$ *and* $\operatorname{coker} s_n$ *are both* 0 *for every* $n \geq 0$.

Now we can finish the proof of Theorem 4.

Proof of Theorem 4. First we prove (1). By Lemma 8 and its remark, the $\mathfrak{p}$-rank of $\mathrm{Sel}_E(L_n)_\mathfrak{p}^{\Gamma'_n}$ is unbounded and tends to infinity as n tends to infinity. Now by Lemma 10, the map

$$s_n : \mathrm{Sel}_E(F_n)_\mathfrak{p} \to \mathrm{Sel}_E(L_n)_\mathfrak{p}^{\Gamma'_n}$$

is an isomorphism, hence the $\mathfrak{p}$-rank of $\mathrm{Sel}_E(F_n)_\mathfrak{p}$ is unbounded and tends to infinity as n tends to infinity.

For (2), since $E(F)_\mathfrak{p} = 0$ and F_∞/F is a pro-p extension, by Lemma 5, $E(F_\infty)_\mathfrak{p} = 0$, thus

$$\ker h_{F_\infty/F_n} = \operatorname{coker} h_{F_\infty/F_n} = 0.$$

Hence $\ker s_{F_\infty/F_n} = 0$. Therefore the $\mathfrak{p}$-rank of $\mathrm{Sel}_E(F_\infty)_{\mathfrak{p}}^{\Gamma_n}$ is unbounded as n goes to infinity, hence the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_E(F_\infty)_{\mathfrak{p}}$ is unbounded.

□

References

[1] A. Akbary and V. K. Murty, *Descending rational points on elliptic curves to smaller fields*, Canad. J. Math. Vol. **53**(3)(2001), 449-469.

[2] N. Boston, *Some cases of the Fontaine-Mazur conjecture*, J. Number Theory **42**(1992), 285-291.

[3] J. Coates. *Infinite descent on elliptic curves with complex multiplication*. Arithmetic and geometry, Vol. I, 107–137, Progr. Math. **35**, Birkhäuser, 1983.

[4] J. Coates and R. Greenberg, *Kummer theory for Abelian varieties over local fields*. Invent. Math.**124**(1996), 129-174.

[5] E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication. p-adic L functions*. Perspectives in Mathematics **3**. Academic Press, Boston, 1987.

[6] J.-M. Fontaine and B. Mazur, *Geometric Galois representations. Elliptic curves, modular forms, & Fermat's last theorem*(Hong Kong, 1993), 41-78, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995.

[7] E. S. Golod and I. R. Shafarevich, *On the class field tower*. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **28**(1964), 261–272.

[8] R. Greenberg, *Iwasawa theory for elliptic curves*. Arithmetic theory of elliptic curves (Cetraro, 1997), 51-144, Lecture Notes in Math.**1716**, Springer, Berlin, 1999.

[9] R. Greenberg, *Galois theory for the Selmer group of Abelian varieties*, Comp. Math., **136**(2003), 255-297.

[10] R. Greenberg, *Introduction to Iwasawa theory for elliptic curves*. Arithmetic algebraic geometry (Park City, UT, 1999), 407–464, IAS/Park City Math. Ser. **9**, Amer. Math. Soc., Providence, RI, 2001.

[11] F. Hajir, *On the growth of p-class groups in p-class field towers*, J. of Algebra **188** (1997), 256-271.

[12] K. Iwasawa, *On the μ-invariants of $\mathbb{Z}_\ell$-extensions*. Number Theory, Algebraic Geometry and Commutative Algebra(in honor of Y. Akizuki). Kinokuniya: Tokyo, 1973, 1-11.

[13] A. Lubotzky and A. Mann, *Powerful p-groups II: p-adic analytic groups*. J. Algebra **105**(1987), 506-515.

[14] B. Mazur, *Rational points on Abelian varieties in towers of number fields*, Invent. Math., **18**(1972), 183-266.

[15] K. Rubin, *Elliptic curves with complex multiplication and the Conjecture of Birch and Swinnerton-Dyer*. Arithmetic theory of elliptic curves (Cetraro, 1997), 167–234, Lecture Notes in Math., **1716**, Springer, Berlin, 1999.

[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, 1986.

[17] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, 1994.

V. Kumar Murty
Department of Mathematics
University of Toronto

Toronto, ON M5S 3G3, Canada
E-mail: murty@math.toronto.edu

Yi Ouyang
Department of Mathematical Sciences
Tsinghua University
Beijing, China 100084
E-mail: youyang@math.tsinghua.edu.cn