



# Asymptotic growth of Mordell–Weil ranks of elliptic curves in noncommutative towers

Anwesh Ray

*Abstract.* Let  $E$  be an elliptic curve defined over a number field  $F$  with good ordinary reduction at all primes above  $p$ , and let  $F_\infty$  be a finitely ramified uniform pro- $p$  extension of  $F$  containing the cyclotomic  $\mathbb{Z}_p$ -extension  $F_{\text{cyc}}$ . Set  $F^{(n)}$  be the  $n$ th layer of the tower, and  $F_{\text{cyc}}^{(n)}$  the cyclotomic  $\mathbb{Z}_p$ -extension of  $F^{(n)}$ . We study the growth of the rank of  $E(F^{(n)})$  by analyzing the growth of the  $\lambda$ -invariant of the Selmer group over  $F_{\text{cyc}}^{(n)}$  as  $n \rightarrow \infty$ . This method has its origins in work of A. Cuoco, who studied  $\mathbb{Z}_p^2$ -extensions. Refined estimates for growth are proved that are close to conjectured estimates. The results are illustrated in special cases.

## 1 Introduction

The *Mordell–Weil Theorem* states that given an elliptic curve  $E$  defined over a number field  $F$ , its  $F$ -rational points form a finitely generated abelian group, i.e.,

$$E(F) \simeq \mathbb{Z}^r \oplus E(F)_{\text{tors}},$$

where  $r$  is a non-negative integer called the Mordell–Weil *rank*. In [22], Mazur initiated the study of Selmer groups of elliptic curves in  $\mathbb{Z}_p$ -extensions. A major application of Iwasawa theory is the study of the growth of Mordell–Weil ranks of abelian varieties in towers of number fields. Given an abelian variety defined over a number field  $F$  with good ordinary reduction at the primes above  $p$ , Mazur showed that the rank of  $A$  is bounded in the cyclotomic  $\mathbb{Z}_p$ -extension of  $F$ . Kato and Rohrlich proved the analogous statement for all elliptic curves defined over abelian number fields, see [15, 24]. Alongside further developments in Iwasawa theory over larger  $p$ -adic Lie extensions, there has been significant interest in analyzing the asymptotic growth of Mordell–Weil ranks in towers. For ordinary primes, Mazur in [23] formulated a precise conjecture on the growth of ranks in any  $\mathbb{Z}_p$ -extension of an imaginary quadratic field  $F$ , called the *Growth number conjecture*. This question has been studied in anticyclotomic extensions by Cornut [4] and Vatsal [26]. A prototypical example of interest is the  $\mathbb{Z}_p^2$ -extension  $F_\infty$  of an imaginary quadratic

---

Received by the editors October 30, 2021; revised January 19, 2022; accepted January 21, 2022.

Published online on Cambridge Core January 31, 2022.

AMS subject classification: 11R23, 11G05.

Keywords: Elliptic curves, Iwasawa invariants, Kida’s formula, towers of number fields, asymptotic growth of ranks.

field  $F$ . For every integer  $n \geq 1$ , set  $F^{(n)}$  to denote the  $n$ th layer. In this setting, it is the extension contained in  $F_\infty$  such that  $\text{Gal}(F^{(n)}/F) = (\mathbb{Z}/p^n\mathbb{Z})^2$ . For elliptic curves  $E/F$ , asymptotic formulas for the growth of the rank of  $E(F^{(n)})$  as  $n \rightarrow \infty$  have been proven by Lei and Sprung in [19]. More recently, such growth questions are studied in admissible uniform pro- $p$  extensions of number fields by Delbourgo and Lei in [7], and by Hung and Lim in [14].

In this note, we employ a new strategy to study the growth of ranks in noncommutative towers. Let  $F_{\text{cyc}}^{(n)}$  be the cyclotomic  $\mathbb{Z}_p$ -extension of  $F^{(n)}$ . We study the growth of the rank of  $E(F^{(n)})$  by analyzing the growth of the  $\lambda$ -invariant of the Selmer group over  $F_{\text{cyc}}^{(n)}$  as  $n \rightarrow \infty$  using a generalizations of Kida’s formula due to Hachimori and Matsuno [11] and Lim [20]. The method has several advantages. First, it is a straightforward application of Kida’s formula which a priori allows one to circumvent technicalities of noncommutative Iwasawa theory. In other words, the proof is short and can be understood without familiarity with methods in noncommutative Iwasawa theory, though it does build on previous work of Lim [21] which uses nontrivial results in the subject. Given an elliptic curve  $E$  over a number field  $F$ , we do however require that the Selmer group of  $E$  over the cyclotomic  $\mathbb{Z}_p$ -extension of  $F$  be cotorsion over the Iwasawa algebra and impose the  $\mathfrak{M}_H(G)$  conjecture (see [2, 20]).

Secondly, (and perhaps more importantly) the method strengthens known results and these estimates are closer to conjectured asymptotics. The error term in the asymptotic formulas of Hung–Lim are removed in the process, and the main term is sharper (see Remark 2.8 for further details). The significance of this is illustrated for certain examples, namely,  $\mathbb{Z}_p^d$ -extensions, false Tate-curve extensions, and trivializing extensions generated by the  $p$ -primary torsion of a non-CM elliptic curve. It should be pointed out here that for  $\mathbb{Z}_p^2$ -extensions, a similar question was studied by Cuoco in [6], who studied the growth of Iwasawa invariants associated with class group towers in families of  $\mathbb{Z}_p$ -extensions contained in the composite of two  $\mathbb{Z}_p$ -extensions. The results can also be applied to prove statistical results.

- (1) In Corollary 3.3, it is shown that if  $E$  is an elliptic curve defined over an imaginary quadratic field  $F$  such that  $E$  does not have complex multiplication and  $\text{rank } E(F) = 0$ , then the rank remains 0 is 100% of  $\mathbb{Z}_p^2$ -extensions of  $F$ .
- (2) In Corollary 3.7, we consider the curve  $E = 11a2$ . It is shown that there is a positive density set of primes  $\ell$  such that

$$\text{rank } E\left(\mathbb{Q}(\mu_{7^{n+1}}, \ell^{\frac{1}{7^n}})\right) \leq \lambda_7(E/\mathbb{Q}(\mu_{7^\infty}))7^n$$

for all integers  $n > 0$ .

The method employed in this paper shows that in any context in which a satisfactory generalization of Kida’s formula is proved, it should be possible to analyze the growth of  $\lambda$ -invariants in noncommutative towers. We point out that analogs of Kida’s formula have been proven for fine Selmer groups by Kundu in [17]. In this particular context, the number fields are assumed to be totally real. Also, such results were proved by Hatley and Lei in the supersingular setting, see [13].

## 2 Growth of Iwasawa invariants in towers

In this section, we introduce some preliminary notions and prove the main result of this paper.

### 2.1 Uniform pro- $p$ extensions

Throughout,  $p$  will be a prime  $\geq 5$  and  $F$  a number field. Let  $F_\infty$  be an infinite Galois extension of  $F$  with pro- $p$  Galois group  $G := \text{Gal}(F_\infty/F)$ . The lower central  $p$ -series of  $G$  is recursively defined as follows:

$$G_0 := G \text{ and } G_{n+1} := G_n^p [G_n, G].$$

**Definition 2.1** The group  $G$  is said to be *uniform* if

- (1) it is finitely generated,
- (2) it is *powerful*, i.e.,  $[G, G] \subseteq G^p$ , and
- (3)  $[G_n : G_{n+1}] = [G : G_1]$  for all  $n \in \mathbb{Z}_{\geq 1}$ .

Setting  $d := [G : G_1]$ , we observe that  $[G : G_n] = p^{dn}$ . Assume that  $G$  has the structure of a  $p$ -adic Lie group. We say that  $F_\infty$  is a *strongly admissible*  $p$ -adic Lie extension if

- (1) only finitely many primes ramify in  $F_\infty$ ,
- (2)  $F_\infty$  contains the cyclotomic  $\mathbb{Z}_p$ -extension  $F_{\text{cyc}}$  of  $F$ , and
- (3) the  $p$ -torsion subgroup of  $G$  is trivial.

We assume that  $F_\infty$  is pro- $p$  a strongly admissible  $p$ -adic Lie extension and  $G$  is uniform. Note that  $G_n/G_{n+1} \simeq (\mathbb{Z}/p\mathbb{Z})^d$  for  $n \in \mathbb{Z}_{\geq 1}$ . It is well known that the dimension of  $G$  is equal to  $d$  and that  $G_n = G^{p^n}$ , see [8, Theorem 3.6]. The extension  $F_\infty$  is filtered by a tower of number fields. Setting  $F^{(n)} := F_\infty^{G_n}$ , consider the nonabelian tower

$$F = F^{(0)} \subset F^{(1)} \subset \dots \subset F^{(n)} \subset \dots,$$

and let  $F_{\text{cyc}}^{(n)}$  be the cyclotomic  $\mathbb{Z}_p$ -extension of  $F^{(n)}$ . We have thus filtered the extension  $F_\infty$  into a tower of cyclotomic  $\mathbb{Z}_p$ -extensions

$$F_{\text{cyc}} = F_{\text{cyc}}^{(0)} \subset F_{\text{cyc}}^{(1)} \subset \dots \subset F_{\text{cyc}}^{(n)} \subset \dots$$

Set  $H := \text{Gal}(F_\infty/F_{\text{cyc}})$  and  $\Gamma := G/H \simeq \mathbb{Z}_p$ . For  $n \in \mathbb{Z}_{\geq 1}$ , we write  $H_n$  (resp.  $\Gamma_n$ ) for the descending central series of  $H$  (resp.  $\Gamma$ ). We list a few useful facts.

**Lemma 2.2** *The following assertions hold:*

- (1) *The normal subgroup  $H$  is uniform with  $(d - 1)$  generators, and  $H_n$  is identified with  $H \cap G_n$ .*
- (2)  *$\Gamma_n$  is identified with  $G_n/H_n$ .*

**Proof** See [8, Theorem 3.6] and [14, Lemma 2.6] for further details. ■

As a result, we have that  $F_{\text{cyc}}^{(n)} = F_{\infty}^{H_n}$  and hence,

$$\text{Gal}(F_{\text{cyc}}^{(n+1)}/F_{\text{cyc}}^{(n)}) = H_n/H_{n+1} \simeq (\mathbb{Z}/p\mathbb{Z})^{d-1}.$$

Since  $\Gamma_n = G_n/H_n$ , we have that  $\Gamma_n = \text{Gal}(F_{\text{cyc}}^{(n)}/F^{(n)})$ . We now introduce the Iwasawa-algebra at the  $n$ th level, taken to be

$$\Lambda(\Gamma_n) := \varprojlim_L \mathbb{Z}_p[\text{Gal}(L/F^{(n)})],$$

where  $L$  ranges over all number fields contained in between  $F^{(n)}$  and  $F_{\text{cyc}}^{(n)}$ . Choose a topological generator  $\gamma_n$  of  $\Gamma_n$  and fix the isomorphism  $\Lambda(\Gamma_n) \simeq \mathbb{Z}_p[[x]]$  sending  $\gamma_n - 1$  to  $x$ .

More generally, if  $\mathcal{G}$  is any pro- $p$  group, set

$$\Lambda(\mathcal{G}) := \varprojlim_U \mathbb{Z}_p[\mathcal{G}/U],$$

where  $U$  ranges over all finite index normal subgroups of  $\mathcal{G}$ . Given a number field  $F$ , we set  $\Lambda_F := \Lambda(\text{Gal}(F_{\text{cyc}}/F))$ .

## 2.2 Iwasawa invariants

Let  $M$  be a cofinitely generated cotorsion  $\mathbb{Z}_p[[x]]$ -module, i.e., the Pontryagin-dual  $M^\vee := \text{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$  is a finitely generated and torsion  $\mathbb{Z}_p[[x]]$ -module. Recall that a polynomial  $f(x) \in \mathbb{Z}_p[[x]]$  is said to be *distinguished* if it is a monic polynomial whose nonleading coefficients are all divisible by  $p$ . Note that all height 1 prime ideals of  $\mathbb{Z}_p[[x]]$  are principal ideals  $(a)$ , where  $a = p$  or  $a = f(x)$ , where  $f(x)$  is an irreducible distinguished polynomial. According to the structure theorem for  $\mathbb{Z}_p[[x]]$ -modules (see [27, Theorem 13.12]),  $M^\vee$  is pseudo-isomorphic to a finite direct sum of cyclic  $\mathbb{Z}_p[[x]]$ -modules, i.e., there is a map

$$M^\vee \longrightarrow \left( \bigoplus_{i=1}^s \mathbb{Z}_p[[x]]/(p^{\mu_i}) \right) \oplus \left( \bigoplus_{j=1}^t \mathbb{Z}_p[[x]]/(g_j^{e_j}(x)) \right)$$

with finite kernel and cokernel. Here,  $\mu_i > 0$ ,  $e_j > 0$ , and  $g_j(x)$  is an irreducible distinguished polynomial. Furthermore, the numbers  $\mu_1, \dots, \mu_s$  and irreducible distinguished polynomials  $g_1(x), \dots, g_t(x)$  are uniquely determined. The characteristic ideal of  $M^\vee$  is (up to a unit) generated by

$$f_M^{(p)}(x) = f_M(x) := p^{\sum_i \mu_i} \prod_j g_j^{e_j}(x).$$

The  $\mu$ -invariant of  $M$  is defined as the power of  $p$  in  $f_M(x)$ . More precisely,

$$\mu_p(M) := \begin{cases} \sum_{i=1}^s \mu_i & \text{if } s > 0, \\ 0 & \text{if } s = 0. \end{cases}$$

The  $\lambda$ -invariant of  $M$  is the degree of the characteristic element, i.e.,

$$\lambda_p(M) := \begin{cases} \sum_{i=1}^t e_i \deg g_i & \text{if } s > 0, \\ 0 & \text{if } s = 0. \end{cases}$$

Since the numbers  $\mu_i$  and polynomials  $g_j(x)$  are uniquely determined by  $M$ , the  $\mu$  and  $\lambda$ -invariants determined above are well defined.

Let  $F$  be a number field and  $E$  an elliptic curve over  $F$  with good ordinary reduction at all primes of  $F$  above  $p$ . Denote by  $\text{Sel}_{p^\infty}(E/F_{\text{cyc}})$  the  $p$ -primary Selmer group of  $E$  over  $F_{\text{cyc}}$  (see [1] for further details). Suppose  $\text{Sel}_{p^\infty}(E/F_{\text{cyc}})$  is a cotorsion  $\Lambda_F$ -module, we set  $\mu_p(E/F)$  and  $\lambda_p(E/F)$  to denote the  $\mu$  and  $\lambda$ -invariant of  $\text{Sel}_{p^\infty}(E/F_{\text{cyc}})$  respectively, when viewed as a module over  $\Lambda_F$ . We fix a strongly admissible pro- $p$ , uniform,  $p$ -adic Lie extension  $F_\infty/F$  and let  $\text{Sel}_{p^\infty}(E/F_\infty)$  be the Selmer group of  $E$  over  $F_\infty$  (see [21] for the definition). Throughout, we make the following assumption.

**Assumption 2.3** *With notation as above, assume that  $\text{Sel}_{p^\infty}(E/F_\infty)$  satisfies the  $\mathfrak{M}_H(G)$ -conjecture. In greater detail, set  $X(E/F_\infty)$  to be the Pontryagin dual of  $\text{Sel}_{p^\infty}(E/F_\infty)$ . We assume that*

$$X_f(E/F_\infty) := \frac{X(E/F_\infty)}{X(E/F_\infty)[p^\infty]}$$

*is finitely generated as a  $\Lambda(H)$ -module.*

### 2.3 An analogue of Kida’s formula

Hachimori and Matsuno in [11] proved an analogue of Kida’s formula for Selmer groups of elliptic curves. We recall this result and a refinement due to Lim. Let  $F$  be a number field and  $E/F$  an elliptic curve. Let  $L/F$  be a finite Galois extension such that  $\text{Gal}(L/F)$  is a  $p$ -group. Let  $P_1(E, L_{\text{cyc}})$  (resp.  $P_2(E, L_{\text{cyc}})$ ) be the set of primes  $\eta \nmid p$  of  $L_{\text{cyc}}$  that are ramified in the extension  $L_{\text{cyc}}/K_{\text{cyc}}$ , at which  $E$  has split multiplicative reduction (resp.  $E$  has good reduction and  $E(L_{\text{cyc}, \eta})[p] \neq 0$ ). Given a prime  $\eta$  of  $L_{\text{cyc}}$ , set  $e_{L_{\text{cyc}}/K_{\text{cyc}}}(\eta)$  to denote the ramification index of  $\eta$  with respect to the extension  $L_{\text{cyc}}/K_{\text{cyc}}$ .

**Theorem 2.4** (Lim) *Let  $p \geq 5$  be a prime number,  $F$  a number field and  $E/F$  an elliptic curve with good ordinary reduction at all primes of  $F$  above  $p$ . Let  $L/F$  be a Galois extension for which  $\text{Gal}(L/F)$  is a  $p$ -group. Assume that there is a pro- $p$  strongly admissible  $p$ -adic Lie extension  $F_\infty/F$  such that*

- (1)  $F_\infty$  contains  $L$ .
- (2) Assumption 2.3 is satisfied.

*Then, the following assertions hold*

- (1)  $\text{Sel}_{p^\infty}(E/L_{\text{cyc}})$  is cotorsion over the Iwasawa algebra  $\Lambda_L$ ,
- (2)  $\mu_p(E/L) = [L : K] \mu_p(E/K)$ , and

(3)

$$\begin{aligned} \lambda_p(E/L) &= [L_{\text{cyc}} : K_{\text{cyc}}] \lambda_p(E/K) + \sum_{\eta \in P_1(E/L_{\text{cyc}})} (e_{L_{\text{cyc}}/K_{\text{cyc}}}(\eta) - 1) \\ &\quad + 2 \sum_{\eta \in P_2(E/L_{\text{cyc}})} (e_{L_{\text{cyc}}/K_{\text{cyc}}}(\eta) - 1). \end{aligned}$$

**Proof** The result as stated follows from the results in [21], as we now explain. Note that since it is assumed that the Selmer group of  $E$  over  $F_\infty$  satisfies the  $\mathfrak{M}_H(G)$ -conjecture, it follows from [2, Proposition 2.5] that  $\text{Sel}_{p^\infty}(E/L_{\text{cyc}})$  is cotorsion over  $\Lambda_L$ . First, we reduce to the case when  $K_{\text{cyc}} \cap L = K$ , i.e.,  $[L : K] = [L_{\text{cyc}} : K_{\text{cyc}}]$ . Letting  $K' = K_{\text{cyc}} \cap L$ , it is easy to see that if the result holds for the extensions  $L/K'$  and  $K'/K$ , then it holds for  $L/K$ .

First, we prove that the result holds for  $K'/K$ . It is a simple exercise to show that  $\mu_p(E/K') = [K' : K] \mu_p(E/K)$ . Furthermore  $\lambda_p(E/K')$  is the  $\mathbb{Z}_p$ -corank of  $\text{Sel}_{p^\infty}(E/K'_{\text{cyc}})$ . Since  $K'$  is contained in  $K_{\text{cyc}}$ , we have that  $K'_{\text{cyc}} = K_{\text{cyc}}$ . Therefore,  $\lambda_p(E/K')$  is equal to  $\lambda_p(E/K)$ . Thus, the result is shown to hold for  $K'/K$  and it suffices to prove the result for  $L/K'$ . Upon replacing  $K$  with  $K'$ , we thus reduce to the case when  $[L : K] = [L_{\text{cyc}} : K_{\text{cyc}}]$ . In this setting, the result follows from [21, Theorem 4.1 and Section 5]. Indeed the decomposition conditions in *loc. cit.* are equivalent to the conditions on  $P_1$  and  $P_2$ . ■

**Remark 2.5** It should be noted here that in Section 5 of [21] an additional assumption is made, namely that  $F$  contains the  $p$ th roots of unity. This assumption is in place to guarantee the existence of an admissible  $p$ -adic Lie extension of  $L$ , see Lemma 4.2 of *loc. cit.* Since we have assumed that such an admissible  $p$ -adic Lie extension  $F_\infty/L$  exists to begin with, there is no need for this additional assumption.

### 2.4 Main result

Let  $E$  be an elliptic curve over a number field  $F$  with good ordinary reduction at all primes above  $p$ . Throughout, we shall make the following assumption.

We introduce some further notation. Let  $Q_1 = Q_1(E, F_\infty)$  (resp.  $Q_2 = Q_2(E, F_\infty)$ ) be the set of primes  $w \nmid p$  of  $F_{\text{cyc}}$  that are ramified in  $F_\infty$ , at which  $E$  has split multiplicative reduction (resp.  $E$  has good reduction and  $E(F_{\text{cyc},w})[p] \neq 0$ ). We stress here that  $Q_1$  and  $Q_2$  consist of subsets of primes of  $F_{\text{cyc}}$  and not  $F_\infty$ . Recall that it is stipulated that only finitely many primes ramify in  $F_\infty$ , and since all primes are finitely decomposed in  $F_{\text{cyc}}$ , it follows that  $Q_1$  and  $Q_2$  are finite. For  $i = 1, 2$ , we set  $q_i := \#Q_i$ .

**Theorem 2.6** *Let  $n$  be a positive integer. Suppose that the conditions of Assumption 2.3 hold, then,  $\text{Sel}_{p^\infty}(E/F_{\text{cyc}}^{(n)})$  is a cotorsion  $\Lambda_{F^{(n)}}$ -module, with*

$$\mu_p(E/F^{(n)}) = p^{nd} \mu_p(E/F).$$

Furthermore, we have that

$$p^{n(d-1)} \lambda_p(E/F) \leq \lambda_p(E/F^{(n)}) \leq p^{n(d-1)} \lambda_p(E/F) + (p^{n(d-1)} - p^{n(d-2)}) (q_1 + 2q_2).$$

**Proof** According to Theorem 2.4,  $\text{Sel}_{p^\infty}(E/F_{\text{cyc}}^{(n)})$  is a cotorsion module over  $\Lambda_{F^{(n)}}$  and the  $\mu$ -invariant is given by

$$\mu_p(E/F^{(n)}) = [F^{(n)} : F]\mu_p(E/F) = p^{nd}\mu_p(E/F).$$

Furthermore, the  $\lambda$ -invariant is

$$\lambda_p(E/F^{(n)}) = [F_{\text{cyc}}^{(n)} : F_{\text{cyc}}]\lambda_p(E/F) + \sum_{w \in P_1} (e(w) - 1) + 2 \sum_{w \in P_2} (e(w) - 1),$$

where  $e(w)$  is the ramification index of  $w$  in  $F_{\text{cyc}}^{(n)}/F_{\text{cyc}}$ ,  $P_1$  and  $P_2$  are the set of primes of  $F_{\text{cyc}}^{(n)}$  defined as follows:

$$P_1 = \{w \mid w \nmid p, E \text{ has split multiplicative reduction at } w\},$$

$$P_2 = \{w \mid w \nmid p, E \text{ has good reduction at } w \text{ and } E(\mathcal{F}_{n,w}) \text{ has a point of order } p\}.$$

Since  $p$  is odd, the primes  $P_i$  lie above  $Q_i$ , therefore,

$$\sum_{w \in P_i} (e(w) - 1) = \sum_{v \in Q_i} \left( \sum_{w|v} (e(w) - 1) \right).$$

Choose a prime  $w_0 \in P_i$  above  $v$ . Since  $e(w)$  is the same for all primes  $w|v$ , we have that

$$\sum_{w|v} (e(w) - 1) = (1 - e(w_0)^{-1}) \sum_{w|v} e(w) \leq (1 - e(w_0)^{-1}) [F_{\text{cyc}}^{(n)} : F_{\text{cyc}}].$$

According to Lemma 2.2,  $H$  is uniform with  $d - 1$  generators. Note that  $[F_{\text{cyc}}^{(n)} : F_{\text{cyc}}] = [H : H_n] = p^{(d-1)n}$ . Since pro- $p$  tame inertia is generated by a single element, it follows that  $e(w_0) \leq p^n$ . Putting it all together, the result follows. ■

**Theorem 2.7** *Let  $E$  be an elliptic curve defined over a number field  $F$  and  $F_\infty$  a uniform pro- $p$  extension of  $F$  satisfying aforementioned conditions and suppose that the Selmer group over  $F_{\text{cyc}}$  is cotorsion as a  $\mathbb{Z}_p[[x]]$ -module. Then, we have the following bound*

$$\text{rank } E(F^{(n)}) \leq p^{n(d-1)}\lambda_p(E/F) + (p^{n(d-1)} - p^{n(d-2)})(q_1 + 2q_2).$$

**Proof** The result immediately follows from Theorem 2.6 and the inequality

$$\text{rank } E(F^{(n)}) \leq \lambda_p(E/F^{(n)}),$$

see [10, Theorem 1.9]. ■

**Remark 2.8** The estimate above is stronger than [14, Theorem 3.1]. The error term is  $O(p^{n(d-2)})$  and their method used relies on the work of Harris. In greater detail, [12, Theorem 1.10] is the key result used in the estimate in [14, Lemma 3.3]. Note however, that the error estimate of Hung–Lim is known to be 0 under certain additional constraints. Namely, if certain cohomology groups vanish and the  $p$ -torsion group  $E(F_\infty)(p)$  is finite, see [14, Theorem 3.2] and the remark following it. If  $F_\infty$  contains the extension  $F(E[p^\infty])$  generated by the  $p$ -primary torsion of  $E$ , then the error term

of Hung–Lim is nonzero, even under additional assumptions. Also, even when the error term of Hung–Lim is 0, the estimate above is strictly better when  $q_1$  or  $q_2$  is nonzero.

The improvement in the bound has some nontrivial consequences, which we shall explain in the next section. The following is a Corollary to Theorem 2.6 and is entirely unconditional.

**Corollary 2.9** *Let  $E$  and  $F_\infty$  be as in Theorem 2.7. Assume that  $q_1 = q_2 = 0$  and*

$$\text{Sel}_{p^\infty}(E/F_{\text{cyc}}) = 0.$$

*Then,  $\text{Sel}_{p^\infty}(E/F_{\text{cyc}}^{(n)}) = 0$  for all  $n$ .*

**Proof** Since the  $\mu$ -invariant  $\mu_p(E/F) = 0$ , it follows that  $\mathfrak{M}_H(G)$  is satisfied for  $F_\infty$ , see [2, Theorem 2.1]. By Theorem 2.6, it follows that the  $\mu$  and  $\lambda$ -invariants of  $\text{Sel}_{p^\infty}(E/F_{\text{cyc}}^{(n)})$  are 0, hence,  $\text{Sel}_{p^\infty}(E/F_{\text{cyc}}^{(n)})$  is finite. On the other hand, this Selmer does not contain any finite index submodules (see [9, Proposition 4.14]), hence, must be 0. ■

### 3 Special cases

In this section, we study special cases of Theorem 2.7. Assume throughout that the Assumption 2.3 is satisfied. Recall from the proof of Theorem 2.4 that this in particular implies that  $\text{Sel}_{p^\infty}(E/L)$  is cotorsion over  $\Lambda_L$  for every number field extension  $L/K$  contained in  $F_\infty$ .

#### 3.1 $\mathbb{Z}_p^d$ -extensions

Throughout this subsection,  $F$  will be an abelian number field and  $E/\mathbb{Q}$  an elliptic curve with good ordinary reduction at  $p$ . Let  $F_\infty$  be the composite of all  $\mathbb{Z}_p$ -extensions of  $F$ , note that  $G = \text{Gal}(F_\infty/F) \simeq \mathbb{Z}_p^d$ , where  $d = r_2(F) + 1$ . For instance, when  $F$  is an imaginary quadratic field, then, this gives a  $\mathbb{Z}_p^2$ -extension of  $F$ . To emphasize the dependence on the prime  $p$ , we denote the extension by  $F_\infty(p)$ . On the other hand, it follows from results of Kato and Rohrlich [11, Theorem 2.2] that the Selmer group  $\text{Sel}_{p^\infty}(E/F_\infty)$  is cotorsion as a  $\mathbb{Z}_p[[x]]$ -module. It is well known that any  $\mathbb{Z}_p$ -extension is unramified away from  $p$  (see [27]), hence, the composite of such extensions has the same property. Let us state a few Corollaries to Theorem 2.7, the first of which gives a simple criterion for the rank to be zero throughout the  $\mathbb{Z}_p^d$ -tower.

**Corollary 3.1** *Let  $E$  be as above and assume that  $\lambda_p(E/F_{\text{cyc}}) = 0$ . Then,*

$$\text{rank } E(F^{(n)}) = 0$$

*for all  $n \in \mathbb{Z}_{\geq 1}$  and*

$$\mu_p(E/F^{(n)}) = p^{nd} \mu_p(E/F).$$

**Proof** Note that since  $E$  has good ordinary reduction at the primes above  $p$  and

$$\text{rank } E(F) \leq \lambda_p(E/F),$$

the Mordell–Weil rank of  $E$  is 0. Since  $F_\infty$  is unramified at all primes  $w \nmid p$ , the quantities  $q_1$  and  $q_2$  in Theorem 2.7 are both equal to 0. ■

**Remark 3.2** When  $F$  is an imaginary quadratic field and  $E$  is a CM elliptic curve over  $F$ , the result of Hung–Lim in the above context shall imply that the rank in *bounded* in the tower, however, not identically 0. In the more general case, their result implies that the growth is  $O(p^{n(d-2)})$  unless certain homology groups are known to vanish, see the discussion after [14, Theorem 3.2].

*Example:* Picking an elliptic curve  $E/\mathbb{Q}$  at random, there are typically some primes at which  $E[p]$  is residually reducible as a Galois module. At these primes, it is possible that the  $\mu$ -invariant  $\mu_p(E/\mathbb{Q})$  does not vanish. For instance, let’s pick the elliptic curve of smallest conductor with cremona label 11a2. We find that  $E$  has good ordinary reduction at 5 with  $\mu_5(E/\mathbb{Q}) = 2$  and  $\lambda_5(E/\mathbb{Q}) = 0$ . Suppose that there is an imaginary quadratic field  $F/\mathbb{Q}$  in which  $\text{rank } E(F) = 0$  and  $\lambda_5(E/F) = 0$  as well. Let  $F_\infty$  be the  $\mathbb{Z}_p^2$ -extension of  $F$ . Then, indeed, since  $\mu_5(E/F) \geq 2$ , the above result implies that

$$\mu_5(E/F^{(n)}) \geq 2p^{2n}$$

for all  $n \geq 1$ , however, the rank of  $E(F_n)$  remains 0 throughout. Unfortunately, the author is not aware of any existing computer packages that can compute the  $\lambda$ -invariant over an imaginary quadratic field.

**Corollary 3.3** *Let  $E/\mathbb{Q}$  be an elliptic curve and  $F$  an abelian number field satisfying*

- (1)  $\text{rank } E(F) = 0$  and
- (2)  $E$  does not have complex multiplication.

*Then, for 100% of primes  $p$  at which  $E$  has good ordinary reduction,*

$$\text{rank } E(F_\infty(p)) = 0.$$

**Proof** In her thesis [16, Theorem 5.1.1], Kundu generalized a result of Greenberg to show that the proportion of primes  $p$  such that

- (1)  $E$  has good ordinary reduction at the primes of  $F$  above  $p$  and
- (2)  $\text{Sel}_{p^\infty}(E/F_{\text{cyc}}) = 0$ ,

is 100%. The result follows from this and Corollary 3.1. ■

The following is a special case of [14, Conjecture 1].

**Conjecture 3.4** [14, Conjecture 1’] *Let  $E$  be an elliptic curve over an imaginary quadratic field  $F$ ,  $p \geq 5$  a prime and  $F_\infty$  be the  $\mathbb{Z}_p^2$ -extension of  $F$ . Assume that the following conditions are satisfied:*

- (1)  $E$  has good ordinary reduction at all primes above  $p$  and
- (2) Assumption 2.3 is satisfied.

*Then, we have that  $\text{rank } E(F^{(n)}) \leq \text{rank } E(F_{\text{cyc}})p^n$  for all  $n \geq 1$ .*

**Corollary 3.5** Consider the setting of the above conjecture. Under Assumption 2.3, the Theorem 2.7 specializes to give that

$$\text{rank } E(F^{(n)}) \leq \lambda_p(E/F)p^n.$$

Thus, the Conjecture is true when

$$\lambda_p(E/F) = \text{rank } E(F_{\text{cyc}}).$$

**Remark 3.6** Note that  $\lambda_p(E/F) \geq \text{rank } E(F^{(n)})$  for all  $n$  and hence,  $\lambda_p(E/F) \geq \text{rank } E(F_{\text{cyc}})$ . Indeed, it can be expected that  $\lambda_p(E/F) = \text{rank } E(F)$  for 100% of primes above which  $E$  has good ordinary reduction. There is much evidence pointing towards this expectation for elliptic curves defined over the rationals, see [18]. We do expect that similar arguments do carry over to elliptic curves over imaginary quadratic fields.

### 3.2 False-Tate curve extensions

Let  $\ell$  be a finite set of prime numbers that are coprime to  $p$  and let  $F_\infty$  be the False-Tate curve extension of  $F = \mathbb{Q}(\mu_p)$ , given by

$$F_\infty := \mathbb{Q}(\mu_{p^\infty}, \ell^{\frac{1}{p^\infty}}).$$

In other words, it is the extension obtained by adjoining all  $p$ -power roots of 1 and  $\ell$ . It is easy to see that  $F_\infty/F$  is a uniform pro- $p$  extension of  $F$  of dimension  $d = 2$ . Thus Theorem 2.7 specializes to give us that

$$\text{rank } E(F^{(n)}) \leq \lambda_p(E/F)p^n + (p^n - 1)(q_1 + 2q_2).$$

Let us compute the values of  $q_1$  and  $q_2$  for a given example. We note that it is difficult to compute  $\lambda_p(E/F)$  due to the base change to  $F = \mathbb{Q}(\mu_p)$ .

*Example:* We pick an elliptic curve and prime at random. Let  $E = 11a2$  in Cremona label and  $p = 7$ . The elliptic curve is defined over  $\mathbb{Q}$  and we consider its base change to  $F = \mathbb{Q}(\mu_7)$ . It follows from Assumption 2.3 and from the proof of Theorem 2.4 that  $\text{Sel}_{7^\infty}(E/\mathbb{Q}(\mu_{7^\infty}))$  is cotorsion over  $\Lambda_F$ . Note that since  $F$  is an abelian extension of  $\mathbb{Q}$ , the cotorsion property of the Selmer group (over  $\Lambda_F$ ) also follows from results due to Kato, see [15]. The image of the residual representation at  $p = 7$  contains  $\text{SL}_2(\mathbb{F}_7)$ , as stated in the link provided. Hence, after base change to  $\mathbb{Q}(\mu_7)$  the image of the residual representation will still contain  $\text{SL}_2(\mathbb{F}_7)$ . It is thus reasonable to expect that the  $\mu$ -invariant  $\mu_7(E/F) = 0$ , however, this is difficult to prove and needs to be assumed. Consider the False Tate extension

$$F_\infty := \mathbb{Q}(\mu_{7^\infty}, 11^{\frac{1}{7^\infty}}).$$

Then,  $E$  has split multiplicative reduction at 11, hence  $q_2 = 0$ , however,  $q_1 > 0$ . Since  $11^3 \equiv 1 \pmod{7}$  and  $11^3 \not\equiv 1 \pmod{49}$ , there are precisely two primes above 11 in  $F_{\text{cyc}} = \mathbb{Q}(\mu_{7^\infty})$ . It follows that  $q_1 = 2$ . Putting it all together, we find that

$$\text{rank } E(F^{(n)}) \leq \lambda_7(E/F)7^n + 2(7^n - 1).$$

Next, we prove a statistical result.

**Corollary 3.7** Consider the elliptic curve  $E = 11a2$  from the example above and set  $p = 7$ . There is a positive density set of primes  $\ell$  such that

$$\text{rank } E \left( \mathbb{Q}(\mu_{7^{n+1}}, \ell^{\frac{1}{7^n}}) \right) \leq \lambda_7(E/F)7^n$$

for any integer  $n \geq 1$ .

**Proof** For each prime number  $\ell$  such that  $\ell \equiv 1 \pmod{7}$ , let  $F_\infty^{(\ell)}$  denote the extension  $\mathbb{Q}(\mu_{7^\infty}, \ell^{\frac{1}{7^\infty}})$ . Note that  $\ell$  splits in  $\mathbb{Q}(\mu_7)$  and the only prime other than 7 that ramifies in  $F_\infty^{(\ell)}$  is  $\ell$ . Since  $E$  has bad reduction at only finitely many primes, we deduce that  $q_1 = 0$  for all extensions  $F_\infty^{(\ell)}$  except for finitely many choices of  $\ell$ . Recall that  $Q_2$  consists of the primes  $w \nmid 7$  of  $F_{\text{cyc}}$  that are ramified in  $F_\infty$ , such that  $E$  has good reduction at  $w$  and  $E(F_{\text{cyc},w})[7] \neq 0$ . Since the formal group of  $E$  at  $w$  is pro- $\ell$ ,  $E(F_{\text{cyc},w})[7] \simeq E(k_w)[7]$ , where  $k_w$  is the residue field of  $F_{\text{cyc},w}$ . Since  $k_w$  is a 7-extension of  $\mathbb{F}_\ell$ , it follows that  $E(k_w)[7] \neq 0$  if and only if  $E(\mathbb{F}_\ell)[7] \neq 0$ . Thus, the prime  $w$  lies in  $Q_2$  if the following conditions are satisfied:

- (1)  $w|\ell$ ,
- (2)  $E$  has good reduction at  $\ell$ , and
- (3)  $E(\mathbb{F}_\ell)[7] \neq 0$ .

This latter condition is satisfied for  $\frac{1}{7}$  of all primes  $\ell$ , see [3, Section 2] for further details. We show that a similar application of the Chebotarev density theorem shows that for a positive proportion of the primes  $\ell$ , both  $q_1$  and  $q_2$  are 0. Note that if a prime  $\ell$  splits in  $\mathbb{Q}(\mu_7)$  precisely when  $\ell \equiv 1 \pmod{7}$ . Let  $\bar{\rho} : \text{Gal}(\mathbb{Q}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_7)$  be the Galois representation on the 7-torsion points  $E[7]$ . Denote by  $\mathbb{Q}(\bar{\rho})$  the number field fixed by the kernel of  $\bar{\rho}$ . Note that  $\det \bar{\rho}$  is the mod-7 cyclotomic character, which we denote by  $\bar{\chi}$ . Therefore, the field  $\mathbb{Q}(\bar{\rho})$  contains  $\mathbb{Q}(\mu_7)$ , which is the field fixed by the kernel of  $\bar{\chi}$ . Let  $\ell \neq 7$  be a prime at which  $E$  has good reduction, note that  $\bar{\rho}$  is unramified at  $\ell$ . Let  $\sigma_\ell \in \text{Gal}(\mathbb{Q}(\bar{\rho})/\mathbb{Q})$  denote the Frobenius element at  $\ell$ , it is well known that the characteristic polynomial of  $\bar{\rho}(\sigma_\ell)$  is given by

$$\det(\text{Id} \cdot x - \bar{\rho}(\sigma_\ell)) = x^2 - (\ell + 1 - \#E(\mathbb{F}_\ell))x + \ell.$$

Thus, if  $\ell$  is a prime such that

$$(3.1) \quad \det \bar{\rho}(\sigma_\ell) = 1 \text{ and } \text{tr} \bar{\rho}(\sigma_\ell) \neq 2,$$

then,  $\ell$  splits in  $\mathbb{Q}(\mu_7)$  and  $E(\mathbb{F}_\ell)[7] = 0$ . We show that there is a positive density set of primes  $\ell$  satisfying the above conditions (3.1). According to the LMFD Database [5], the image of  $\bar{\rho}$  contains  $\text{SL}_2(\mathbb{F}_7)$ . Thus there is  $\sigma \in \text{Gal}(\mathbb{Q}(\bar{\rho})/\mathbb{Q})$  such that  $\bar{\rho}(\sigma) = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ , and thus satisfies (3.1). According to the Chebotarev density theorem, there

is a positive proportion of primes such that  $\sigma_\ell = \sigma$ , and thus,  $\bar{\rho}(\sigma_\ell) = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ . As a result, there is a positive density set of primes  $\ell$  such that  $q_1$  and  $q_2$  are both zero, and this completes the proof. ■

### 3.3 The field generated by torsion points

We come to the example in which  $F_\infty$  is the field  $\mathbb{Q}(E[p^\infty])$ , i.e., the field generated by the  $p$ -primary torsion points of  $E$ . Assume that  $E$  does not have complex multiplication. Then, by Serre’s Open image theorem (see [25, Section 4 and Theorem 3]),  $G$  is a finite index subgroup of  $\mathrm{GL}_2(\mathbb{Z}_p)$  and it follows from this that the dimension of  $G$  is 4. In this setting,  $F = \mathbb{Q}(E[p])$ , and  $F^{(n)} = \mathbb{Q}(E[p^{n+1}])$ . We find that

$$\mathrm{rank} E(F_n) \leq \lambda_p(E/F)p^{3n} + q_1(p^{3n} - p^{2n}),$$

where  $q_1$  is simply the number of primes  $\ell \neq p$  at which  $E$  has split multiplicative reduction, and  $q_2 = 0$ . On the other hand, according to [14, Remark after Theorem 3.2] the result of Hung–Lim [14, Theorem 3.2] gives

$$\mathrm{rank} E(F_n) \leq (\lambda_p(E/F) + q_1)p^{3n} + 8,$$

when the whole dual Selmer group  $\mathcal{X}(E/F_\infty)$  is finitely generated over  $\Lambda(H)$ .

**Acknowledgment** The author is grateful to Debanjana Kundu for pointing out an inaccuracy in the previous draft. The author also thank the anonymous referee for a timely and thorough reading of the manuscript and for suggestion various pertinent corrections.

### References

- [1] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, TATA Inst. Fund. Res. Lecture Notes, Narosa Publishing House, New Delhi, 2000.
- [2] J. Coates and R. Sujatha, *On the  $mh$  ( $g$ )-conjecture*. In Non-abelian fundamental groups and Iwasawa theory. In: London Mathematical Society, Lecture Note Series, Cambridge University Press 393, Cambridge University Press, 2012, pp. 132–161.
- [3] A. C. Cojocaru. *Questions about the reductions modulo primes of an elliptic curve*. In Proc. 7th Meeting of the Canadian Number Theory Association (Montreal, 2002), Citeseer, Princeton, NJ, 2004, pp. 61–79.
- [4] C. Cornut, *Mazur’s conjecture on higher Heegner points*. Invent. Math. 148(2002), no. 3, 495–523.
- [5] J. E. Cremona, J. W. Jones, A. V. Sutherland, and J. Voight, *The  $l$ -functions and modular forms database*. Notices Amer. Math. Soc. 68(2021), no. 9, 1520–1522.
- [6] A. A. Cuoco, *The growth of Iwasawa invariants in a family*. Comp. Math. 41(1980), no. 3, 415–437.
- [7] D. Delbourgo and A. Lei, *Estimating the growth in Mordell–Weil ranks and Shafarevich–Tate groups over lie extensions*. Ramanujan J. 43(2017), no. 1, 29–68.
- [8] J. D. Dixon, M. P. Du Sautoy, A. Mann, and D. Segal, *Analytic pro- $p$  groups*, Cambridge University Press, Cambridge, 2003.
- [9] R. Greenberg, *Arithmetic theory of elliptic curves: Lectures given at the 3rd Session of the Centro Internazionale Matematico Estivo (CIME) held in Cetaro, Italy, July 12–19, 1997*, Springer, Berlin, 1999.
- [10] R. Greenberg, *Iwasawa theory for elliptic curves*. In Arithmetic theory of elliptic curves, Springer, Berlin, 1999, pp. 51–144.
- [11] Y. Hachimori and K. Matsuno, *An analogue of Kida’s formula for the Selmer groups of elliptic curves*. J. Algebr. Geom. 8(1999), no. 3, 581–601.
- [12] M. Harris, *Correction to  $p$ -adic representations arising from descent on abelian varieties*. Compos. Math. 121(2000), no. 1, 105–108.
- [13] J. Hatley and A. Lei, *Arithmetic properties of signed selmer groups at non-ordinary primes*. Ann. l’Inst. Fourier 69(2019), 1259–1294.
- [14] P.-C. Hung and M. F. Lim, *On the growth of Mordell–Weil ranks in  $p$ -adic lie extensions*. Asian J. Math. 24(2020), no. 4, 549–570.

- [15] K. Kato, *p-adic hodge theory and values of zeta functions of modular forms*. Astérisque 295(2004), 117–290.
- [16] D. Kundu. *Iwasawa theory of fine Selmer groups*, Ph.D. Thesis, University of Toronto (Canada), 2020.
- [17] D. Kundu, *An analogue of Kida’s formula for fine Selmer groups of elliptic curves*. J. Number Theory 222(2021), 249–261.
- [18] D. Kundu and A. Ray, *Statistics for Iwasawa invariants of elliptic curves*. Trans. Am. Math. Soc. 374(2021), no. 11, 7945–7965.
- [19] A. Lei and F. Sprung, *Ranks of elliptic curves over  $\mathbb{Z}_p^2$ -extensions*. Israel J. Math. 236(2020), no. 1, 183–206.
- [20] M. F. Lim, *A remark on the  $M_h(g)$ -conjecture and Akashi series*. Int. J. Number Theory 11(2015), no. 01, 269–297.
- [21] M. F. Lim, *Some remarks on Kida’s formula when  $\mu \neq 0$* . Ramanujan J. 55(2021), no. 2, 1127–1144.
- [22] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*. Invent. Math. 18(1972), no. 3–4, 183–266.
- [23] B. Mazur, *Modular curves and arithmetic*. In: Proceedings of the International Congress of Mathematicians, 1, Polish Scientific Publishers, Warszawa, 1983, p. 2.
- [24] D. E. Rohrlich, *Onl-functions of elliptic curves and cyclotomic towers*. Invent. Math. 75(1984), no. 3, 409–423.
- [25] J. Serre, *Galois properties of finite order points of elliptic curves*. Invent. Math. 15(1971), no. 4, 259–331.
- [26] V. Vatsal, *Special values of anticyclotomicl-functions*. Duke Math. J. 116(2003), no. 2, 219–261.
- [27] L. C. Washington. *Introduction to cyclotomic fields*, Vol. 83, Springer Science & Business Media, Berlin, 1997.

*Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada*

*e-mail:* [anweshray@math.ubc.ca](mailto:anweshray@math.ubc.ca)