ASIAN J. MATH.
Vol. 24, No. 4, pp. 549–570, August 2020

002

# ON THE GROWTH OF MORDELL-WEIL RANKS IN $P$-ADIC LIE EXTENSIONS*

PIN-CHI HUNG† AND MENG FAI LIM‡

**Abstract.** Let $p$ be an odd prime and $F_\infty$ a $p$-adic Lie extension of a number field $F$. Let $A$ be an abelian variety over $F$ which has ordinary reduction at every primes above $p$. Under various assumptions, we establish asymptotic upper bounds for the growth of Mordell-Weil rank of the abelian variety of $A$ in the said $p$-adic Lie extension. Our upper bound can be expressed in terms of invariants coming from the cyclotomic level. Motivated by this formula, we make a conjecture on an asymptotic upper bound of the growth of Mordell-Weil ranks over a $p$-adic Lie extension which is in terms of the Mordell-Weil rank of the abelian variety over the cyclotomic $\mathbb{Z}_p$-extension. Finally, it is then natural to ask whether there is such a conjectural upper bound when the abelian variety has non-ordinary reduction. For this, we can at least modestly formulate an analogous conjectural upper bound for the growth of Mordell-Weil ranks of an elliptic curve with good supersingular reduction at the prime $p$ over a $\mathbb{Z}_p^2$-extension of an imaginary quadratic field.

**Key words.** Mordell-Weil ranks, $p$-adic Lie extensions, $\mathfrak{M}_H(G)$-conjecture.

**Mathematics Subject Classification.** 11G10, 11R23.

## 1. Introduction.

Let $A$ be an Abelian variety defined over a number field $F$. The well-known Mordell-Weil theorem asserts that the group $A(F)$ of $F$-rational points is a finitely generated abelian group. In particular, this group has a well-defined $\mathbb{Z}$-rank which is called the Mordell-Weil rank of $A$. In this paper, we are interested in the variation of the Mordell-Weil ranks of an abelian variety in a $p$-adic Lie extension, where $p$ is an odd prime at which the abelian variety has ordinary reduction at every prime of $F$ above $p$. In studying the Mordell-Weil rank, the Selmer group plays an important role. In his fundamental work [42], Mazur developed the (ordinary) Iwasawa theory of Selmer groups, and applied it to obtain an upper bound for the growth of Mordell-Weil ranks in a cyclotomic $\mathbb{Z}_p$-extension which we now describe.

Let $F^{\mathrm{cyc}}$ be the cyclotomic $\mathbb{Z}_p$-extension of $F$. Denote by $F_n$ the intermediate subfield of $F^{\mathrm{cyc}}/F$ with index $|F_n : F| = p^n$. Write $X(A/F^{\mathrm{cyc}})$ for the Pontryagin dual of the Selmer group of $A$ over $F^{\mathrm{cyc}}$. This Selmer group carries a natural $\mathbb{Z}_p[\![\Gamma]\!]$-module structure, where $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$. Mazur conjectured that $X(A/F^{\mathrm{cyc}})$ is a torsion $\mathbb{Z}_p[\![\Gamma]\!]$-module. Granted the validity of the conjecture, one can attach Iwasawa $\lambda$-invariant to this module which is usually denoted by $\lambda_{\mathbb{Z}_p[\![\Gamma]\!]}(X(A/F^{\mathrm{cyc}}))$. The following is a theorem of Mazur [42, p. 185] (or see [19, Theorem 1.9]) which gives a uniform bound on the Mordell-Weil ranks in a cyclotomic $\mathbb{Z}_p$-extension in term of this Iwasawa $\lambda$-invariant.

THEOREM (Mazur). Let $A$ be an abelian variety defined over a number field which has good ordinary reduction at every primes above $p$. Let $F^{cyc}$ be the cyclotomic $\mathbb{Z}_p$-extension of $F$ with intermediate subfield $F_n$ of index $|F_n : F| = p^n$. Suppose that $X(A/F^{\mathrm{cyc}})$ is a torsion $\mathbb{Z}_p[\![\Gamma]\!]$-module. Then we have

$$\mathrm{rank}_{\mathbb{Z}}(A(F_n)) \leq \lambda_{\mathbb{Z}_p[\![\Gamma]\!]}(X(A/F^{\mathrm{cyc}})).$$

*Received April 22, 2019; accepted for publication October 25, 2019.

†Room R0718, First Academic Building, Soochow University, Taipei, R.O.C. (pinchihung1111@gmail.com).

‡School of Mathematics and Statistics & Hubei Key Laboratory of Mathematical Sciences, Central China Normal University, Wuhan, 430079, P.R. China (limmf@mail.ccnu.edu.cn).

The goal of this paper is to search for such an analogous upper bound over a $p$-adic Lie extension of higher dimension. Indeed, if $F_\infty$ is now a uniform $p$-adic Lie extension (see Section 3 for definition) of $F$ of dimension $d$ with Galois group $G$, there is a natural extension of the notion of a torsion $\mathbb{Z}_p[\![G]\!]$-module (see [53]). Under the assumption that $X(A/F_\infty)$ is torsion over $\mathbb{Z}_p[\![G]\!]$, one can show that $\mathrm{rank}_{\mathbb{Z}}(A(F_n)) = O(p^{(d-1)n})$ by appealing to the work of Harris [24] (also see [2, Corollary 19], [23, Corollary 2.9] or [40, Theorem 3.2]). However, Harris's result does not give a concrete upper bound as in the cyclotomic $\mathbb{Z}_p$-extension. The main reason behind this is that we do not have a nice enough structure theory for modules over noncommutative Iwasawa algebras unlike the cyclotomic situation (see [4, 8]).

After much intensive study by Coates, Fukaya, Kato, Sujatha and Venjakob [4, 55], they were led to conjecture that the dual Selmer group $X(A/F_\infty)$ satisfies a stronger torsion property which enables one to define a higher analogue of the Iwasawa $\lambda$-invariant. We now describe this aspect of their work. Denote by $X(A/F_\infty)(p)$ the $\mathbb{Z}_p[\![G]\!]$-submodule of $X(A/F_\infty)$ consisting of elements annihilated by some power of $p$ and write $X_f(A/F_\infty) = X(A/F_\infty)/X(A/F_\infty)(p)$. Coates et al [4] conjectured that $X_f(A/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$, where $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. Granted this conjecture, it then makes sense to speak of $\mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\big(X_f(A/F_\infty)\big)$. It has been long observed in literature that this quantity serves as a higher analog of the classical $\lambda$-invariant (for instances, see [6, 26]). In view of this, it would seem natural to expect an upper bound of the Mordell-Weil ranks which has a description in term of this quantity, and this is precisely the main theorem of our paper.

Theorem (Theorem 3.1). Assume that $(i)$ $A$ is an abelian variety over a number field $F$ which has ordinary reduction at every primes above $p$, $(ii)$ $F_\infty$ is a uniform admissible $p$-adic extension of $F$ of dimension $d \geq 2$ and $(iii)$ $X_f(A/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$. Denoting by $F_n$ the fixed field of $\mathrm{Gal}(F_\infty/F)^{p^n}$, we have

$$\mathrm{rank}_Z(A(F_n)) \leq \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\big(X_f(A/F_\infty)\big)p^{(d-1)n} + O(p^{(d-2)n}).$$

We mention in passing that the error term $O(p^{(d-2)n})$ arises due to the usage of an asymptotic formula of Harris [24]. By imposing an extra assumption, we can elucidate the error terms further, and this is the content of the next theorem.

Theorem (Theorem 3.2). Retain all the assumptions of Theorem 3.1. Assume further that $H_i(H_n, X(A/F_\infty))$ is finite for every $i \geq 1$ and $n \geq 0$. Then one has

$$\mathrm{rank}_Z(A(F_n)) \leq \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\big(X_f(A/F_\infty)\big)p^{(d-1)n} + d\,\mathrm{corank}_{\mathbb{Z}_p}(A(F_\infty)(p)).$$

The point of the extra finiteness assumption in the preceding theorem is to allow us to *avoid* the usage of Harris's formula which is the key in obtaining such a precise upper bound. The finiteness assumption are known to be valid in many situations (see Remark after Theorem 3.2).

We should mention that a proof of Theorem 3.2 was established in [12, Corollary 1.4] by an algebraic $K$-theoretical argument. (Although their result is stated for (solvable) admissible $p$-adic Lie extension of dimension $\leq 3$, one can check that their algebraic $K$-theoretical argument carries over to the general situation.) Our proof here is different from there in that we do not use any algebraic $K$-theory, instead giving a direct proof via control theorems and some rank calculations of Howson and Harris. Our reason of having this approach is twofold.

Firstly, the above approach can be adapted to yield a description of $\mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\left(X_f(A/F_\infty)\right)$ in terms of invariants coming from the cyclotomic level $F^{\mathrm{cyc}}$. Combining this description with the above theorems, one obtains an upper bound in terms of these cyclotomic invariants (see Corollary 4.5). The latter inspires us to make a conjecture on an asymptotic upper bound of the Mordell-Weil ranks in terms of the cyclotomic Mordell-Weil rank (see Conjecture 1). We like to mention that although Theorems 3.1 and 3.2, and Corollary 4.5 are derived under the validity of $\mathfrak{M}_H(G)$-conjecture, our Conjecture 1 *does not* require the $\mathfrak{M}_H(G)$-conjecture in its formulation (although we need an appropriate conjecture of Mazur for our Conjecture 1). We provide some (mild) theoretical evidence to our Conjecture 1 (see Section 5). We also mention that in proving Conjecture 1 in these situations, we do not assume the $\mathfrak{M}_H(G)$-conjecture.

The second reason of adopting a non algebraic $K$-theoretical proof stems from a recent work of Lei and Sprung [35], where they obtained an upper bound for an elliptic curve with good supersingular reduction at the prime $p$ over a $\mathbb{Z}_p^2$-extension of an imaginary quadratic field which is in the spirit of Harris. As the supersingular situation is slightly more delicate, the approach we adopted is more suitable than the algebraic K-theoretical approach. Indeed, we are able to establish analogue of Theorem 3.2 for this non-ordinary situation under an appropriate supersingular variant of the $\mathfrak{M}_H(G)$-conjecture. We also mention that as in the case of Theorem 3.2, we do not use Harris's asymptotic formula which allows us to establish a precise upper bound (see Theorem 6.3 for details). Following the ordinary situation, we also formulate a conjecture on an upper bound of the Mordell-Weil ranks in this non-ordinary setting (see Conjecture 2).

We now give a brief description of the layout of the paper. In Section 2, we recall certain algebraic notion which will be used subsequently in the paper. We also prove several lemmas in preparation for the proof of the main results. Section 3 is where we introduce the Selmer groups and prove our main results. In Section 4, we calculate the quantity $\mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\left(X_f(A/F_\infty)\right)$ in terms of various cyclotomic invariants. It is also here that we state our Conjecture 1 and present some evidence for it. This is further continued in Section 5, where we describe how the combination of the works of Cornut-Vatsal, Howard, Nekovář can be applied to establish the validity of our Conjecture 1 for a $\mathbb{Z}_p^2$-extension of an imaginary quadratic field. Finally, in Section 6, we establish results analogue to those in Sections 3 and 4 for an elliptic curve with good supersingular reduction over the $\mathbb{Z}_p^2$-extension of an imaginary field. Building on this, we formulate our conjecture (Conjecture 2) on the upper bound of the Mordell-Weil ranks in this modest non-ordinary setting.

**Acknowledgments.** The authors are very grateful of Antonio Lei for his comments and interest on the paper. We would especially like to thank him for the discussion pertaining to Section 6 and for making us aware of the paper [41]. The authors also like to thank John Coates for his interest and helpful comments on the paper. We also thank Ming-Lun Hsieh for his encouragement on the authors' collaboration. We are grateful to the anonymous referee for providing various helpful comments and feedback. Some part of the research of this article was conducted when M. F. Lim was visiting the National Center for Theoretical Sciences and Academia Sinica of Taiwan, and he would like to acknowledge the hospitality and conducive working conditions provided by these institutes. Finally, P. -C. Hung's research is supported by the MOST grant 107-2115-M-031-001-MY2, and M. F. Lim's research is supported by the National Natural Science Foundation of China under Grant No.

11550110172 and Grant No. 11771164.

**2. Algebraic Preliminaries.** In this section, we recall some algebraic preliminaries that will be required in the later part of the paper. Let $G$ be a compact pro-$p$ $p$-adic Lie group without $p$-torsion. It is well known that $\mathbb{Z}_p[\![G]\!]$ is an Auslander regular ring (cf. [53, Theorems 3.26]). Furthermore, the ring $\mathbb{Z}_p[\![G]\!]$ has no zero divisors (cf. [46]), and therefore, admits a skew field $Q(G)$ which is flat over $\mathbb{Z}_p[\![G]\!]$ (see [17, Chapters 6 and 10] or [32, Chapter 4, §9 and §10]). Thanks to this, we can define the notion of $\mathbb{Z}_p[\![G]\!]$-rank of a finitely generated $\mathbb{Z}_p[\![G]\!]$-module $M$, which is given by

$$\operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M) = \dim_{Q(G)}(Q(G) \otimes_{\mathbb{Z}_p[\![G]\!]} M).$$

The module $M$ is then said to be a *torsion* $\mathbb{Z}_p[\![G]\!]$-module if $\operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M) = 0$.

Now if $M$ is a finitely generated $\mathbb{Z}_p[\![G]\!]$-module, then its homology groups $H_i(G, M)$ are finitely generated over $\mathbb{Z}_p$ (see [26, Proof of Theorem 1.1] or [40, Lemma 3.2.3]). Hence the quantity $\operatorname{rank}_{\mathbb{Z}_p}\big(H_i(G, M)\big)$ is well-defined. In view of this observation, we can now state the following result of Howson (see [26, Theorem 1.1] or [38, Lemma 4.3]).

PROPOSITION 2.1 (Howson). *Let $M$ be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module. Then we have*

$$\operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M) = \sum_{i=0}^{d} (-1)^i \operatorname{rank}_{\mathbb{Z}_p}\big(H_i(G, M)\big),$$

*where here $d$ denotes the dimension of the $p$-adic group $G$.*

From now on, our group $G$ is always assumed to be a uniform pro-$p$ group in the sense of [14, Section 4]. We write $G_n$ for the lower $p$-series $P_{n+1}(G)$ which is defined recursively by $P_1(G) = G$ and

$$P_{n+1}(G) = \overline{P_n(G)^p [P_n(G), G]}, \text{ for } n \geq 1.$$

It follows from [14, Thm. 3.6] that $G^{p^n} = P_{n+1}(G)$ and that we have an equality $|G : P_2(G)| = |P_n(G) : P_{n+1}(G)|$ for every $i \geq 1$ (cf. [14, Definition 4.1]). It follows from these that $|G : G_n| = p^{dn}$, where $d = \dim G$. We now record the following lemma whose proof is left to the readers as an exercise (or see [26, Corollary 1.5]).

LEMMA 2.2. *Let $M$ be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module. Then $M$ is finitely generated over $\mathbb{Z}_p[\![G_n]\!]$ with*

$$\operatorname{rank}_{\mathbb{Z}_p[\![G_n]\!]}(M) = |G : G_n| \operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M) = p^{dn} \operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M).$$

The next lemma will be useful in the subsequent of the paper.

LEMMA 2.3. *Let $G$ be a uniform pro-$p$ group of dimension $d$ and $M$ a finitely generated $\mathbb{Z}_p[\![G]\!]$-module. Suppose that $H_i(G_n, M)$ is finite for every $i \geq 1$ and $n \geq 0$. (Here $G_0$ is to be understood as $G$.) Then for every $n \geq 0$, we have*

$$\operatorname{rank}_{\mathbb{Z}_p}(M_{G_n}) = \operatorname{rank}_{\mathbb{Z}_p[\![G_n]\!]}(M) = p^{dn} \operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M).$$

*Proof.* This follows from combining Proposition 2.1 and Lemma 2.2. □

To prepare for the next lemma, we need to introduce some more notation. For a $\mathbb{Z}_p[\![G]\!]$-module $M$, denote by $M(p)$ the $\mathbb{Z}_p[\![G]\!]$-submodule of $M$ consisting of all the elements of $M$ which are annihilated by some power of $p$.

LEMMA 2.4. *Let $G$ be a uniform pro-$p$ group of dimension $d$ and $M$ a finitely generated $\mathbb{Z}_p[\![G]\!]$-module. Then for every $i \geq 0$, we have*

$$\operatorname{rank}_{\mathbb{Z}_p}\big(H_i(G,M)\big) = \operatorname{rank}_{\mathbb{Z}_p}\big(H_i(G,M_f)\big),$$

*where $M_f = M/M(p)$.*

*Proof.* From the short exact sequence

$$0 \longrightarrow M(p) \longrightarrow M \longrightarrow M_f \longrightarrow 0,$$

we have an exact sequence

$$H_i\big(G,M(p)\big) \longrightarrow H_i(G,M) \longrightarrow H_i(G,M_f) \longrightarrow H_{i-1}\big(G,M(p)\big),$$

where $H_{-1}\big(G,M(p)\big)$ is to be understood to be zero. Since the ring $\mathbb{Z}_p[\![G]\!]$ is Noetherian and $M$ is finitely generated over $\mathbb{Z}_p[\![G]\!]$, so is $M(p)$. Therefore, there exists a sufficiently large $t$ such that $p^t$ annihilates $M(p)$, and hence all its $G$-homology groups. As the $G$-homology groups are finitely generated over $\mathbb{Z}_p$ (see discussion before Proposition 2.1), they must therefore be finite. The equality of the lemma is now a consequence of this observation and the above four terms exact sequence. □

LEMMA 2.5. *Let $G$ be a uniform pro-$p$ group of dimension $d$. Suppose that $M$ is a $\mathbb{Z}_p[\![G]\!]$-module which is finitely generated over $\mathbb{Z}_p$. Then we have*

$$\operatorname{rank}_{\mathbb{Z}_p}\big(H_1(G,M)\big) \leq d \operatorname{rank}_{\mathbb{Z}_p}(M).$$

*Proof.* By virtue of Lemma 2.4, we may assume that $M$ is free as a $\mathbb{Z}_p$-module. Under this said assumption, we have a short exact sequence

$$0 \longrightarrow M \xrightarrow{\cdot p} M \longrightarrow M/p \longrightarrow 0$$

which in turn induces an injection $H_1(G,M)/p \hookrightarrow H_1(G,M/p)$. It then follows that

$$\operatorname{rank}_{\mathbb{Z}_p}\big(H_1(G,M)\big) \leq \dim_{\mathbb{F}_p}\big(H_1(G,M)/p\big) \leq \dim_{\mathbb{F}_p}\big(H_1(G,M/p)\big).$$

Now since $G$ is pro-$p$, the only simple discrete $G$-module is isomorphic to $\mathbb{Z}/p$ with a trival $G$-action (cf. [45, Corollary 1.6.13]). Hence we may apply a dévissage argument to obtain the inequality

$$\dim_{\mathbb{F}_p}\big(H_1(G,M/p)\big) \leq \dim_{\mathbb{F}_p}\big(H_1(G,\mathbb{Z}/p)\big)\dim_{\mathbb{F}_p}(M/p).$$

As $G$ is a uniform group of dimension $d$, we have $\dim_{\mathbb{F}_p}\big(H_1(G,\mathbb{Z}/p)\big) = d$ by [14, Theorem 4.35]. Finally, as $M$ is assumed to be torsionfree, we have $\operatorname{rank}_{\mathbb{Z}_p}(M) = \dim_{\mathbb{F}_p}(M/p)$. The required estimate is now a consequence of these observations. □

Suppose that the uniform group $G$ contains a closed normal subgroup $H$ with the property that $\Gamma := G/H \cong \mathbb{Z}_p$. Since $\Gamma$ is clearly a uniform group, it follows from [14, Proposition 4.31] that $H$ is also a uniform group. Write $H_n$ (resp., $\Gamma_n$) for the lower $p$-series $P_{n+1}(H)$ of $H$ (resp., for $P_{n+1}(\Gamma)$ of $\Gamma$). The next lemma records the relations between the lower $p$-series of the groups $H$, $G$ and $\Gamma$.

LEMMA 2.6. *For every $n \geq 1$, we have $H_n = H \cap G_n$ and $G_n/H_n \cong \Gamma_n$.*

*Proof.* Since $H$ and $G$ are uniform, we have $H_n = H^{p^n}$ and $G_n = G^{p^n}$ (cf. [14, Theorem 3.6]). Clearly, one has the inclusion $H^{p^n} \subseteq H \cap G^{p^n}$. Conversely, let $h \in H \cap G^{p^n}$. Then there exists $g \in G$ such that $h = g^{p^n}$ which in turn implies that the coset $gH$ is a torsion element in $G/H$. But since $G/H \cong \mathbb{Z}_p$ has no $p$-torsion, this forces $g \in H$. Hence we have $h \in H^{p^n}$ and this proves the first equality. For the second equality, one simply observes that

$$G_n/H_n = G^{p^n}/H^{p^n} \cong G^{p^n}H/H = (G/H)^{p^n} \cong \Gamma^{p^n} = \Gamma_n.$$

□

We end the section with one final lemma.

LEMMA 2.7. *Let $G$ be a uniform pro-$p$ group which contains a closed normal subgroup $H$ with the property that $\Gamma := G/H \cong \mathbb{Z}_p$. Let $M$ be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module which has the properties that $M_f := M/M(p)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$ and that $H_i(H, M)$ is finitely generated over $\mathbb{Z}_p$ for all $i \geq 1$. Then for every $i \geq 1$, we have*

$$\operatorname{rank}_{\mathbb{Z}_p}\big(H_i(H, M)\big) = \operatorname{rank}_{\mathbb{Z}_p}\big(H_i(H, M_f)\big).$$

*Proof.* Taking $H$-homology of the following short exact sequence

$$0 \longrightarrow M(p) \longrightarrow M \longrightarrow M_f \longrightarrow 0,$$

we obtain a long exact sequence

$$H_i\big(H, M(p)\big) \longrightarrow H_i(H, M) \xrightarrow{f_i} H_i(H, M_f) \longrightarrow H_{i-1}\big(H, M(p)\big)$$

for $i \geq 1$. As seen in the proof of Lemma 2.4 there exists a sufficiently large $t$ such that $p^t$ annihilates $M(p)$. It then follows from this that $p^t$ annihilates $H_i\big(H, M(p)\big)$. This in turn implies that $p^t$ annihilates $\ker f_i$ and $\operatorname{coker} f_i$. But since $H_i(H, M)$, and therefore, $\ker f_i$ is finitely generated over $\mathbb{Z}_p$, it follows that $\ker f_i$ is finite. Also, as $M_f$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$, the group $H_i(H, M_f)$ is therefore finitely generated over $\mathbb{Z}_p$ which in turn implies the same holds for $\operatorname{coker} f_i$. But we have already seen that $\operatorname{coker} f_i$ is annihilated by $p^t$, and so $\operatorname{coker} f_i$ is finite. In conclusion, the map $f_i$ has finite kernel and cokernel, and the equality of the lemma is now an immediate consequence of this. □

**3. Selmer groups.** In this section, we recall the definition of the Selmer group of an abelian variety. As before, $p$ will denote an odd prime. Let $F$ be a number field and $A$ an abelian variety over $F$. Let $v$ be a prime of $F$. For every finite extension $L$ of $F$, we define

$$J_v(A/L) = \bigoplus_{w|v} H^1(L_w, A)(p),$$

where $w$ runs over the (finite) set of primes of $L$ above $v$. If $\mathcal{L}$ is an infinite extension of $F$, we define

$$J_v(A/\mathcal{L}) = \varinjlim_{L} J_v(A/L),$$

where the direct limit is taken over all finite extensions $L$ of $F$ contained in $\mathcal{L}$. For any algebraic (possibly infinite) extension $\mathcal{L}$ of $F$, the Selmer group of $A$ over $\mathcal{L}$ is defined to be

$$\mathrm{Sel}(A/\mathcal{L}) = \ker\Big(H^1(\mathcal{L}, A(p)) \longrightarrow \bigoplus_v J_v(A/\mathcal{L})\Big),$$

where $v$ runs through all the primes of $F$.

If $L$ is a finite extension of $F$, then the Selmer group and the Mordell-Weil group are related by the following short exact sequence

$$0 \longrightarrow A(L) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}(A/L) \longrightarrow Ш(A/L)(p) \longrightarrow 0,$$

where $Ш(A/L)$ is the Tate-Shafarevich group. It follows from this that

$$\mathrm{rank}_{\mathbb{Z}}(A(L)) \leq \mathrm{corank}_{\mathbb{Z}_p}\big(\mathrm{Sel}(A/L)\big).$$

Hence the problem of obtaining an upper bound for the Mordell-Weil ranks is reduced to obtaining an upper bound for the coranks of the Selmer groups. (Of course, it has been conjectured that $Ш(A/L)$ is finite and hence the above inequality should be an equality under this conjecture. However, for our purposes, we do not need to assume this.)

A Galois extension $F_\infty$ of $F$ is said to be a uniform admissible $p$-adic Lie extension of $F$ if (i) $\mathrm{Gal}(F_\infty/F)$ is a uniform pro-$p$ group, (ii) $F_\infty$ contains the cyclotomic $\mathbb{Z}_p$-extension $F^{\mathrm{cyc}}$ of $F$ and (iii) $F_\infty$ is unramified outside a finite set of primes of $F$. We shall always write $G = \mathrm{Gal}(F_\infty/F)$, $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$ and $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$. Denote by $X(A/F_\infty)$ the Pontryagin dual of $\mathrm{Sel}(A/F_\infty)$.

To continue, we need to recall certain facts from [5]. For now, let $K$ be a finite extension of $\mathbb{Q}_p$. Write $I_K$ for the inertia subgroup. Suppose for now that $A$ is an abelian variety of dimension $g$ defined over $K$. Write $V = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, where $T_p(A)$ denotes the Tate module of $A$. Following [5], we let $W$ be the $\mathrm{Gal}(\bar{K}/K)$-invariant $\mathbb{Q}_p$-subspace of $V$ of minimal dimension such that some subgroup of $I_K$ of finite index acts trivially on $V/W$. Set $C$ to be the image of $W$ under the natural map $V \longrightarrow V/T_p(A) = A(p)$. As seen in the discussion in [5, pp 150], in the event that the abelian variety $A$ has semistable reduction over $K$, $C$ is precisely $\mathcal{F}(\bar{\mathfrak{m}})(p)$, where $\mathcal{F}$ is the formal group over $\mathcal{O}_K$ attached to the Neron model for $A$ over $\mathcal{O}_K$. Then as abelian groups, we have $C \cong (\mathbb{Q}_p/\mathbb{Z}_p)^h$, where $g \leq h \leq 2g$. In general, an abelian variety $A$ will have semistable reduction over some finite extension $K'$ of $K$. If $\mathcal{F}'$ is the associated formal group over $K'$, then the above discussion yields $C = \mathcal{F}'(\bar{\mathfrak{m}})(p)$. Hence we still have $C \cong (\mathbb{Q}_p/\mathbb{Z}_p)^h$ with $g \leq h \leq 2g$.

Returning to the global situation, we let $A$ be an abelian variety defined over a number field $F$. For each prime $v$ of $F$ above $p$, denote by $C_v$ the $\mathrm{Gal}(\bar{F}_v/F_v)$-submodule of $A(p)$ with $h_v = \mathrm{corank}_{\mathbb{Z}_p}(C_v)$ defined as in the preceding paragraph. We can now state the following conjecture.

Conjecture (Mazur, Schneider). $\mathrm{rank}_{\mathbb{Z}_p[\![G]\!]}\big(X(A/F_\infty)\big) = \sum_{v|p}(h_v - g)$.

The conjecture was first stated by Mazur in [42] for an abelian variety with good ordinary reduction over a cyclotomic $\mathbb{Z}_p$-extension. This conjecture was extended to general abelian varieties by Schneider in [50]. For a general $p$-adic Lie extension, the conjecture was raised in [47] (also see [7, 21, 23]).

We shall say that our abelian variety has *ordinary reduction* at all primes above $p$ if $h_v = g$ for every $v|p$. For instance, an elliptic curve which has either good ordinary reduction (in the usual sense) or multiplicative reduction at every prime above $p$ is ordinary in the above sense. Throughout this paper (with the exception of Section 6), we always assume that our abelian variety has *ordinary reduction* at all primes above $p$. Under this assumption, the conjecture of Mazur and Schneider is then equivalent to saying that $X(A/F_\infty)$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module.

Coates et al [4, 9] have predicted that $X(A/F_\infty)$ satisfies a stronger torsion property. In fact, they formulated their conjecture on the structure of the dual Selmer group of an elliptic curve with good ordinary reduction at all primes above $p$. When the elliptic curve has multiplicative reduction at primes above $p$, this was formulated in [33]. Here we merely mimic these prior works in stating the following conjecture for abelian variety with ordinary reduction (in the above sense) at all primes of $F$ above $p$.

$\mathfrak{M}_H(G)$-Conjecture. *For every admissible $p$-adic Lie extension $F_\infty$ of $F$, $X(A/F_\infty)/X(A/F_\infty)(p)$ is a finitely generated $\mathbb{Z}_p[\![H]\!]$-module.*

From now on, we write $X_f(A/F_\infty) = X(A/F_\infty)/X(A/F_\infty)(p)$. Assuming the validity of the $\mathfrak{M}_H(G)$-Conjecture, it then makes sense to speak of $\mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\big(X_f(A/F_\infty)\big)$. We can now state the following theorems.

Theorem 3.1. *Assume that (i) $A$ is an abelian variety over a number field $F$ which has ordinary reduction at every prime above $p$, (ii) $F_\infty$ is a uniform admissible $p$-adic extension of $F$ of dimension $d \geq 2$ and (iii) $X_f(A/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$. Then we have*

$$\mathrm{rank}_{\mathbb{Z}}(A(F_n)) \leq \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\big(X_f(A/F_\infty)\big)p^{(d-1)n} + O(p^{(d-2)n}).$$

As mentioned in the introduction, we can obtain a more precise upper bound under an additional assumption on the $H_n$-homology of the dual Selmer groups.

Theorem 3.2. *Retain all the assumptions of Theorem 3.1. Assume further that $H_i(H_n, X(A/F_\infty))$ is finite for every $i \geq 1$ and $n \geq 0$. Then*

$$\mathrm{rank}_{\mathbb{Z}}(A(F_n)) \leq \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\big(X_f(A/F_\infty)\big)p^{(d-1)n} + d\,\mathrm{corank}_{\mathbb{Z}_p}\big(A(F_\infty)(p)\big).$$

Remark.

(1) We have presented our results for uniform $p$-adic Lie extension mainly for convenience. By virtue of Lazard's theorem (see [14, Corollary 8.34]), a compact $p$-adic Lie group contains a uniform subgroup of finite index. Therefore, by base-changing of the base field, we can obtain an upper bound of the Mordell-Weil ranks in an arbitrary admissible $p$-adic Lie extension.

(2) As already mentioned in the introduction, Theorem 3.2 can be proved by an algebraic $K$-theoretical argument similar to that in [12, Corollary 1.4]. Our proof here is different from there in that we do not use any algebraic $K$-theory. A version of Theorem 3.2 was also obtained in [6, Proposition 6.9] for an elliptic curve over an $GL_2$-extension under the stronger assumption that $X(A/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$.

(3) The extra assumption on the finiteness of the $H_n$-homology groups in the preceding theorem is known to be satisfied in many cases and we shall mention them here.

(*a*) When $\dim G = 2$ (i.e., $\dim H = 1$), it follows from [37, Proposition 5.1(c)] that $H_i(H_n, X(A/F_\infty)) = 0$ for every $i \geq 1$ and $n \geq 0$. Hence this assumption holds in this situation.

(*b*) In fact if $\dim G \leq 3$, this assumption is also verified in [12, Lemma 2.3] and is an intermediate argument required for the proof of [12, Corollary 1.4].

(*c*) If $A$ is an elliptic curve, the hypothesis has been verified for a large class of $p$-adic Lie extensions (see [2, Proposition 13], [8, Remark 2.6] and [57, Theorem 1.2 and Lemma 4.3]).

Before proving the theorems, we first establish the following lemma.

LEMMA 3.3. *Assume that* (*i*) *$A$ is an abelian variety over a number field $F$ which has ordinary reduction at every prime above $p$ and* (*ii*) *$F_\infty$ is a uniform admissible $p$-adic extension of $F$. Then we have*

$$\operatorname{rank}_{\mathbb{Z}}(A(F_n)) \leq \operatorname{rank}_{\mathbb{Z}_p}\left(X_f(A/F_\infty)_{G_n}\right) + \operatorname{corank}_{\mathbb{Z}_p}\left(H^1\big(G_n, A(F_\infty)(p)\big)\right).$$

*Proof.* It suffices to show that the quantity on the right is an upper bound for $\operatorname{corank}_{\mathbb{Z}_p}(\operatorname{Sel}(A/F_n))$. Consider the following commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Sel}(A/F_n) & \longrightarrow & H^1(G_S(F_n), A(p)) & \longrightarrow & \bigoplus_{v\in S} J_v(A/F_n) \\ & & \downarrow{\scriptstyle s_n} & & \downarrow{\scriptstyle h_n} & & \downarrow{\scriptstyle g_n} \\ 0 & \longrightarrow & \operatorname{Sel}(A/F_\infty)^{G_n} & \longrightarrow & H^1(G_S(F_\infty), A(p))^{G_n} & \longrightarrow & \Big(\bigoplus_{v\in S} J_v(A/F_\infty)\Big)^{G_n} \end{array}$$

with exact rows, and where the vertical maps are given by restriction maps. A diagram chasing argument immediately yields an exact sequence

$$0 \longrightarrow \ker s_n \longrightarrow S(A/F_n) \longrightarrow S(A/F_\infty)^{G_n}$$

with $\ker s_n$ contained in $H^1(G_n, A(F_\infty)[p^\infty])$. It follows from this that

$$\operatorname{corank}_{\mathbb{Z}_p}(S(A/F_n)) \leq \operatorname{rank}_{\mathbb{Z}_p}\left(X(A/F_\infty)_{G_n}\right) + \operatorname{corank}_{\mathbb{Z}_p}\left(H^1\big(G_n, A(F_\infty)(p)\big)\right).$$

Finally, taking into account that $\operatorname{rank}_{\mathbb{Z}_p}\left(X(A/F_\infty)_{G_n}\right) = \operatorname{rank}_{\mathbb{Z}_p}\left(X_f(A/F_\infty)_{G_n}\right)$ by Lemma 2.4, we have the lemma. □

We are now in position to prove our theorems.

*Proof of Theorem 3.1.* It follows from Lemma 3.3 that

$$\operatorname{rank}_{\mathbb{Z}}(A(F_n)) \leq \operatorname{rank}_{\mathbb{Z}_p}\left(X_f(A/F_\infty)_{G_n}\right) + \operatorname{corank}_{\mathbb{Z}_p}\left(H^1\big(G_n, A(F_\infty)(p)\big)\right).$$

By Lemma 2.5, the second quantity on the right is bounded by $d \operatorname{corank}_{\mathbb{Z}_p}\big(A(F_\infty)(p)\big)$. It therefore remains to estimate $\operatorname{rank}_{\mathbb{Z}_p}\left(X_f(A/F_\infty)_{G_n}\right)$. Since $X_f(A/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$, it is also finitely generated over $\mathbb{Z}_p[\![H_n]\!]$. Hence we have

$$\begin{aligned} \operatorname{rank}_{\mathbb{Z}_p}\left(X_f(A/F_\infty)_{G_n}\right) &= \operatorname{rank}_{\mathbb{Z}_p}\left(\left(X_f(A/F_\infty)_{H_n}\right)_{\Gamma_n}\right) \leq \operatorname{rank}_{\mathbb{Z}_p}\left(X_f(A/F_\infty)_{H_n}\right) \\ &= \operatorname{rank}_{\mathbb{Z}_p[\![H]\!]}\left(X_f(A/F_\infty)\right)p^{(d-1)n} + O(p^{(d-2)n}), \end{aligned}$$

where the first equality follows from Lemma 2.6, and the final equality follows from [24, Theorem 1.10] and noting that $H$ has dimension $d-1$. The required estimate is now immediate from combining the above estimates. □

*Proof of Theorem 3.2.* As seen in the proof of Theorem 3.1, we have

$$\mathrm{rank}_{\mathbb{Z}}(A(F_n)) \leq \mathrm{rank}_{\mathbb{Z}_p}\left(X_f(A/F_\infty)_{H_n}\right) + \mathrm{corank}_{\mathbb{Z}_p}\left(H^1\big(G_n, A(F_\infty)(p)\big)\right).$$

By Lemma 2.5, the second quantity is bounded by $d\,\mathrm{corank}_{\mathbb{Z}_p}(A(F_\infty)(p))$. On the other hand, it follows from Lemma 2.4 and the hypothesis of the theorem that $H_i(H_n, X_f(A/F_\infty))$ is finite for every $i \geq 1$ and $n \geq 0$. Hence we may apply Lemma 2.3 to conclude that

$$\mathrm{rank}_{\mathbb{Z}_p}\left(X_f(A/F_\infty)_{H_n}\right) = \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\left(X_f(A/F_\infty)\right)p^{(d-1)n}.$$

The conclusion of the theorem then follows from these. □

**4. Comparing ranks.** Retain the setting and notation from the previous section. We shall derive a formula which relates the $\mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}(X_f(A/F_\infty))$ in terms of certain invariants from the cyclotomic level. Recall that by [5, p. 150-151] (also see discussion in Section 3), for each prime $v$ of $F$ above $p$, we have a short exact sequence

$$0 \longrightarrow C_v \longrightarrow A(p) \longrightarrow D_v \longrightarrow 0$$

of discrete $\mathrm{Gal}(\bar{F}_v/F_v)$-modules which is characterized by the facts that $C_v$ is divisible and $D_v$ is the maximal quotient of $A(p)$ by a divisible subgroup such that the inertia group acts on $D_v$ via a finite quotient. Since our abelian variety $A$ has ordinary reduction at the prime $v$, both $C_v$ and $D_v$ are divisible abelian groups of corank $\dim(A)$. Furthermore, by [5, Propositions 4.1, 4.7 and 4.8], we have

$$J_v(A/F_\infty) \cong \begin{cases} \varinjlim_{\mathcal{L}} \bigoplus_{w|v} H^1(\mathcal{L}_w, D_v), & \text{if } v \text{ divides } p \\ \varinjlim_{\mathcal{L}} \bigoplus_{w|v} H^1(\mathcal{L}_w, A(p)), & \text{if } v \text{ does not divides } p \end{cases}$$

where the direct limit is taken over all finite extensions $\mathcal{L}$ of $F^{\mathrm{cyc}}$ contained in $F_\infty$.

We can now state the main result of this section.

Proposition 4.1. *Let $F_\infty$ be a strongly admissible pro-$p$ Lie extension of $F$. Let $A$ be an abelian variety over $F$ which has ordinary reduction at every primes above $p$. Assume that $X(A/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$-conjecture. Then*

$$\mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\left(X_f(A/F_\infty)\right) = \mathrm{rank}_{\mathbb{Z}_p}\left(X_f(A/F^{\mathrm{cyc}})\right) + \sum_{\substack{w \in S(F^{\mathrm{cyc}}), \\ \dim H_w \geq 1}} \mathrm{corank}_{\mathbb{Z}_p}\left(Z_v(F_w^{\mathrm{cyc}})(p)\right),$$

*where $S(F^{\mathrm{cyc}})$ is the set of primes of $F^{\mathrm{cyc}}$ above $S$. Here $Z_v$ denotes $D_v$ or $A(p)$ accordingly as $v$ divides $p$ or not.*

Remark. Proposition 4.1 has been proved for an elliptic curve $E$ under the stronger assumption that $X(E/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$ (see [2, Theorem 16], [6, Corollary 6.10], [22, Theorem 5.4], [23, Theorem 3.1] and [26, Theorem 2.8]).

The approach for the proof in this general case follows those in the above citations. For the convenience of the readers, we shall supply a proof here.

As a start, we have the following lemma.

LEMMA 4.2. *Retaining the assumptions of Proposition 4.1, we have short exact sequences*

$$0 \longrightarrow \mathrm{Sel}(A/F^{\mathrm{cyc}}) \longrightarrow H^1(G_S(F^{\mathrm{cyc}}), A(p)) \longrightarrow \bigoplus_{v\in S} J_v(A/F^{\mathrm{cyc}}) \longrightarrow 0$$

*and*

$$0 \longrightarrow \mathrm{Sel}(A/F_\infty) \longrightarrow H^1(G_S(F_\infty), A(p)) \longrightarrow \bigoplus_{v\in S} J_v(A/F_\infty) \longrightarrow 0.$$

*Proof.* Since $X(A/F_\infty)$ is assumed to satisfy the $\mathfrak{M}_H(G)$-conjecture, it follows from [9, Proposition 2.5] that for every finite extension $L$ of $F$ contained in $F_\infty$, $X(A/L^{\mathrm{cyc}})$ is torsion over $\mathbb{Z}_p[\![\Gamma_L]\!]$, where $\Gamma_L = \mathrm{Gal}(L^{\mathrm{cyc}}/L)$. Since $A(L^{\mathrm{cyc}})(p)$ is finite (cf. [48]), we may apply a similar argument to that in [37, Proposition 3.3] to obtain a short exact sequence

$$0 \longrightarrow \mathrm{Sel}(A/L^{\mathrm{cyc}}) \longrightarrow H^1(G_S(L^{\mathrm{cyc}}), A(p)) \longrightarrow \bigoplus_{v\in S} J_v(A/L^{\mathrm{cyc}}) \longrightarrow 0.$$

In particular, this yields the first short exact sequence by taking $L = F$. On the other hand, by taking direct limit over $L$, we obtain the second short exact sequence. □

The next two lemmas are concerned with the $H$-homology of global cohomology groups and local cohomology groups.

LEMMA 4.3. *Retain the assumptions of Proposition 4.1. We then have that $H^i(H, H^1(G_S(F_\infty), A(p)))$ is cofinitely generated over $\mathbb{Z}_p$ for every $i \geq 1$. Moreover, we have an exact sequence*

$$\begin{aligned} 0 \longrightarrow H^1(H, A(F_\infty)(p)) &\longrightarrow H^1(G_S(F^{\mathrm{cyc}}), A(p)) \\ &\longrightarrow H^1(G_S(F_\infty), A(p))^H \longrightarrow H^2(H, A(F_\infty)(p)) \longrightarrow 0 \end{aligned}$$

*and isomorphisms*

$$H^i\big(H, H^1(G_S(F_\infty), A(p))\big) \cong H^{i+2}\big(H, A(F_\infty)(p)\big) \text{ for } i \geq 1.$$

*Proof.* Since $X(A/F_\infty)$ is assumed to satisfy the $\mathfrak{M}_H(G)$-conjecture, it follows from [9, Proposition 2.5] that for every finite extension $L$ of $F$ contained in $F_\infty$, $X(A/L^{\mathrm{cyc}})$ is torsion over $\mathbb{Z}_p[\![\Gamma_L]\!]$, where $\Gamma_L = \mathrm{Gal}(L^{\mathrm{cyc}}/L)$. Via similar arguments to those in [37, Proposition 3.3 and Corollary 3.4], we have that $H^2(G_S(F^{\mathrm{cyc}}), A(p)) = 0$ and $H^2(G_S(F_\infty), A(p)) = 0$. Hence the spectral sequence

$$H^i\big(H, H^j(G_S(F_\infty), A(p))\big) \Longrightarrow H^{i+j}(G_S(F^{\mathrm{cyc}}), A(p))$$

degenerates to yield an exact sequence

$$\begin{aligned} 0 \longrightarrow H^1(H, A(F_\infty)(p)) &\longrightarrow H^1(G_S(F^{\mathrm{cyc}}), A(p)) \\ &\longrightarrow H^1(G_S(F_\infty), A(p))^H \longrightarrow H^2(H, A(F_\infty)(p)) \longrightarrow 0 \end{aligned}$$

and isomorphisms

$$H^i\big(H, H^1(G_S(F_\infty), A(p))\big) \cong H^{i+2}\big(H, A(F_\infty)(p)\big) \text{ for } i \geq 1$$

where the $\mathbb{Z}_p$-cofinitely generation of latter groups follow on noting that for any $p$-adic Lie group $H$ and any $\mathbb{Z}_p$-cofinitely generated $H$-module $W$, all of the cohomology groups $H^i(H, W)$ are cofinitely generated $\mathbb{Z}_p$-modules. □

LEMMA 4.4. *Retain the assumption of Proposition 4.1. Then* $H^i\left(H, \bigoplus_{v\in S} J_v(A/F_\infty)\right)$ *is cofinitely generated over* $\mathbb{Z}_p$ *for every* $i \geq 1$. *Moreover, we have an exact sequence*

$$0 \longrightarrow \bigoplus_{w\in S(F^{\mathrm{cyc}})} H^1(H_w, Z_v(F_{\infty,w})) \longrightarrow \bigoplus_{v\in S} J_v(A/F^{\mathrm{cyc}}) \longrightarrow \left(\bigoplus_{v\in S} J_v(A/F_\infty)\right)^H$$

$$\longrightarrow \bigoplus_{w\in S(F^{\mathrm{cyc}})} H^2(H_w, Z_v(F_{\infty,w})) \longrightarrow 0$$

*and isomorphisms*

$$H^i\left(H, \bigoplus_{v\in S} J_v(A/F_\infty)\right) \cong \bigoplus_{w\in S(F^{\mathrm{cyc}})} H^{i+2}\big(H_w, Z_v(F_{\infty,w})\big) \text{ for } i \geq 1.$$

*Here* $Z_v$ *denotes* $D_v$ *or* $A(p)$ *accordingly as* $v$ *divides* $p$ *or not.*

*Proof.* This is a local version of Lemma 4.3 with a similar proof noting that $H^2(F_w^{\mathrm{cyc}}, A(p)) = 0$ and $H^2(F_{\infty,w}, A(p)) = 0$ by [45, Theorem 7.1.8(i)]. □

We can now give the proof of Proposition 4.1.

*Proof of Proposition 4.1.* Consider the following commutative diagram

$$\begin{array}{ccccccc}
0 \longrightarrow \mathrm{Sel}(A/F^{\mathrm{cyc}}) & \longrightarrow & H^1(G_S(F^{\mathrm{cyc}}), A(p)) & \longrightarrow & \bigoplus_{v\in S} J_v(A/F^{\mathrm{cyc}}) & \longrightarrow & 0 \\
\downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\
0 \longrightarrow \mathrm{Sel}(A/F_\infty)^H & \longrightarrow & H^1(G_S(F_\infty), A(p))^H & \longrightarrow & \bigoplus_{v\in S} J_v(A/F_\infty)^H & \longrightarrow & H^1\big(H, S(A/F_\infty)\big) \longrightarrow \cdots
\end{array}$$

with exact rows. To simplify notation, we write $W_\infty = H^1(G_S(F_\infty), A(p))$ and $J_\infty = \bigoplus_{v\in S} J_v(A/F_\infty)$. From the commutative diagram, we have a long exact sequence

$$\begin{gathered}
0 \longrightarrow \ker\alpha \longrightarrow \ker\beta \longrightarrow \ker\gamma \longrightarrow \operatorname{coker}\alpha \longrightarrow \operatorname{coker}\beta \\
\longrightarrow \operatorname{coker}\gamma \longrightarrow H^1\big(H, \mathrm{Sel}(A/F_\infty)\big) \longrightarrow H^1(H, W_\infty) \longrightarrow H^1(H, J_\infty) \longrightarrow \cdots \\
\cdots \longrightarrow H^{i-1}(H, J_\infty) \longrightarrow H^i\big(H, \mathrm{Sel}(A/F_\infty)\big) \longrightarrow H^i(H, W_\infty) \longrightarrow H^i(H, J_\infty) \longrightarrow \cdots .
\end{gathered}$$

By Lemmas 4.3 and 4.4, the groups $\ker\beta$, $\ker\gamma$, $\operatorname{coker}\beta$, $\operatorname{coker}\gamma$, $H^i(H, W_\infty)$ (for $i \geq 1$) and $H^i(H, J_\infty)$ (for $i \geq 1$) are cofinitely generated over $\mathbb{Z}_p$. Thus, combining this observation with the above exact sequence, we have that $\ker\alpha$, $\operatorname{coker}\alpha$ and

$H^1\big(H, S(A/F_\infty)\big)$ (for $i \geq 1$) are cofinitely generated over $\mathbb{Z}_p$. Moreover, we have

$$\begin{aligned}
&\operatorname{corank}_{\mathbb{Z}_p}(\ker\alpha) - \operatorname{corank}_{\mathbb{Z}_p}(\operatorname{coker}\alpha)\\
&= -\sum_{i\geq 1}(-1)^i \operatorname{corank}_{\mathbb{Z}_p} H^i(H, \operatorname{Sel}(A/F_\infty)) + \sum_{i\geq 1}(-1)^i \operatorname{corank}_{\mathbb{Z}_p} H^i(H, A(F_\infty)(p))\\
&\quad - \sum_{\substack{w\in S(F^{\mathrm{cyc}}),\\ \dim H_w \geq 1}} \left(\sum_{i\geq 1}(-1)^i \operatorname{corank}_{\mathbb{Z}_p} H^i(H_w, Z_v(F_{\infty,w}))\right),
\end{aligned}$$

where here $Z_v$ denotes $D_v$ or $A(p)$ accordingly as $v$ divides $p$ or not. Applying Proposition 2.1 and Lemma 2.7, the right hand side is just

$$\begin{aligned}
&-\sum_{i\geq 1}(-1)^i \operatorname{rank}_{\mathbb{Z}_p} H_i(H, X_f(A/F_\infty)) - \operatorname{corank}_{\mathbb{Z}_p} H^0(H, A(F_\infty)(p))\\
&+ \sum_{\substack{w\in S(F^{\mathrm{cyc}}),\\ \dim H_w \geq 1}} \operatorname{corank}_{\mathbb{Z}_p} H^0(H_w, Z_v(F_{\infty,w})).
\end{aligned}$$

Now consider the following commutative diagram

$$\begin{array}{ccccccccc}
 & & & & X(A/F_\infty)(p)_H & \longrightarrow & X(A/F_\infty)_H & \longrightarrow & X_f(A/F_\infty)_H \longrightarrow 0\\
 & & & & \downarrow{\scriptstyle h'} & & \downarrow{\scriptstyle \alpha^\vee} & & \downarrow{\scriptstyle h''}\\
0 & \longrightarrow & X(A/F^{\mathrm{cyc}})(p) & \longrightarrow & X(A/F^{\mathrm{cyc}}) & \longrightarrow & X(A/F^{\mathrm{cyc}}) & \longrightarrow & X_f(A/F^{\mathrm{cyc}}) \longrightarrow 0
\end{array}$$

with exact rows. This in turns yields a long exact sequence

$$\ker h' \longrightarrow \ker(\alpha^\vee) \xrightarrow{f} \ker h'' \longrightarrow \operatorname{coker} h' \longrightarrow \operatorname{coker}(\alpha^\vee) \longrightarrow \ker h'' \longrightarrow 0.$$

Since $X(A/F_\infty)$ satisfies $\mathfrak{M}_H(G)$-conjecture, we have that $X_f(A/F_\infty)_H$ is finitely generated over $\mathbb{Z}_p$. By [9, Proposition 2.5], $X(A/F^{\mathrm{cyc}})$ is torsion over $\mathbb{Z}_p[\![\Gamma]\!]$ and so $X_f(A/F^{\mathrm{cyc}})$ is finitely generated over $\mathbb{Z}_p$. Hence $\ker h''$ and $\operatorname{coker} h''$ are finitely generated over $\mathbb{Z}_p$, and we have

$$\operatorname{rank}_{\mathbb{Z}_p}(\ker h'') - \operatorname{rank}_{\mathbb{Z}_p}(\operatorname{coker} h'') = \operatorname{rank}_{\mathbb{Z}_p}\big(X_f(A/F_\infty)_H\big) - \operatorname{rank}_{\mathbb{Z}_p}(X_f(A/F^{\mathrm{cyc}})).$$

On the other hand, as already seen above, $\ker(\alpha^\vee)$ and $\operatorname{coker}(\alpha^\vee)$ are finitely generated over $\mathbb{Z}_p$. Hence so are $\ker f$ and $\operatorname{coker} h'$. But since these latter groups are $p$-primary, they must be finite. Thus, we have

$$\operatorname{rank}_{\mathbb{Z}_p}(\ker(\alpha^\vee)) - \operatorname{rank}_{\mathbb{Z}_p}(\operatorname{coker}(\alpha^\vee)) = \operatorname{rank}_{\mathbb{Z}_p}\big(X_f(A/F_\infty)_H\big) - \operatorname{rank}_{\mathbb{Z}_p}(X_f(A/F^{\mathrm{cyc}})).$$

Combining this with the above calculations and applying Proposition 2.1 for $X_f(A/F_\infty)$, we obtain the required formula. □

A combination of Theorem 3.1/3.2 and Proposition 4.1 yields the following.

COROLLARY 4.5. *Retain the setting of Theorem 3.1. Then we have*

$$\begin{aligned}
&\operatorname{rank}_{\mathbb{Z}}(A(F_n))\\
&\leq \left(\operatorname{rank}_{\mathbb{Z}_p}(X_f(A/F^{\mathrm{cyc}})) + \sum_{\substack{w\in S(F^{\mathrm{cyc}}),\\ \dim H_w \geq 1}} \operatorname{corank}_{\mathbb{Z}_p}\big(Z_v(F_w^{\mathrm{cyc}})(p)\big)\right) p^{(d-1)n} + O(p^{(d-2)n}),
\end{aligned}$$

*where $S(F^{\mathrm{cyc}})$ is the set of primes of $F^{\mathrm{cyc}}$ above $S$.*

*Furthermore, in the event that the extra assumption of Theorem 3.2 is also valid, we can replace $O(p^{(d-2)n})$ in the above inequality by $d\,\mathrm{corank}_{\mathbb{Z}_p}\left(A(F_\infty)(p)\right)$.*

Notice that the bound on the right hand side makes sense as long as we know that $X(A/F^{\mathrm{cyc}})$ is torsion over $\mathbb{Z}_p[\![\Gamma]\!]$. Hence we are naturally led to raise the following question.

Question. Can one prove the inequality in 4.5 under the weaker assumption that $X(A/F^{\mathrm{cyc}})$ is torsion over $\mathbb{Z}_p[\![\Gamma]\!]$?

Note that it is still unknown if one can deduce the validity of $\mathfrak{M}_H(G)$-conjecture from Mazur's conjecture. A case where such an implication holds is when $X(A/F^{\mathrm{cyc}})$ is finitely generated over $\mathbb{Z}_p$ (see [9, Theorem 2.1]). However, there are examples where $X(A/F^{\mathrm{cyc}})$ is not finitely generated over $\mathbb{Z}_p$ (see [16] and [42, §1, Example 2]). Despite this, it seems reasonable to conjecture that the upper bound is valid whenever $X(A/F^{\mathrm{cyc}})$ is torsion over $\mathbb{Z}_p[\![\Gamma]\!]$. In fact, we shall go one step further in formulating a more refined conjectural upper bound (see Conjecture 1 below). Before doing so, we recall the following observation of Mazur [42].

Lemma 4.6. *Let $A$ be an abelian variety over a number field $F$ which has ordinary reduction at every primes above $p$. Suppose that $X(A/F^{\mathrm{cyc}})$ is finitely generated torsion over $\mathbb{Z}_p[\![\Gamma]\!]$. Then $A(F^{\mathrm{cyc}})$ is finitely generated as an abelian group.*

*Proof.* Since Mazur's conjecture holds, we may apply his theorem (as mentioned in the introduction) to see that $\mathrm{rank}_{\mathbb{Z}}(A(F_n)) \leq \lambda_{\mathbb{Z}_p[\![\Gamma]\!]}(X(A/F^{\mathrm{cyc}}))$ for every $n$. Choose $n_0$ such that $\mathrm{rank}_{\mathbb{Z}}(A(F_{n_0}))$ is as large as possible. Then $A(F^{\mathrm{cyc}})/A(F_{n_0})$ must be a torsion group. Let $P \in A(F^{\mathrm{cyc}})$. Then there exists an integer $m \geq 1$ such that $mP \in A(F_{n_0})$. This in turn implies that $m\,(\sigma(P) - P) = \sigma(mP) - mP = 0$ for all $\sigma \in \mathrm{Gal}(F^{\mathrm{cyc}}/F_{n_0})$. In other words, $\sigma(P) - P \in A(F^{\mathrm{cyc}})_{tor}$. By a result of Ribet [48], the torsion subgroup $A(F^{\mathrm{cyc}})_{tor}$ of $A(F^{\mathrm{cyc}})$ is finite. Set $t = |A(F^{\mathrm{cyc}})_{tor}|$. Then $t\,(\sigma(P) - P) = 0$ or $\sigma(tP) = tP$ for all $\sigma \in \mathrm{Gal}(F^{\mathrm{cyc}}/F_{n_0})$. Hence $tP \in A(F_{n_0})$.

Therefore, we can define a homomorphism $\varphi : A(F^{\mathrm{cyc}}) \longrightarrow A(F_{n_0})$ by $P \mapsto tP$. The image of $\varphi$ is finitely generated since it is a subgroup of $A(F_{n_0})$. On the other hand, the kernel of $\varphi$ is $A(F^{\mathrm{cyc}})_{tor}$ and so is finite. Consequently, $A(F^{\mathrm{cyc}})$ is finitely generated. □

By the preceding lemma, it makes sense to speak of $\mathrm{rank}_{\mathbb{Z}}(A(F^{\mathrm{cyc}}))$ under the validity of conjecture of Mazur and Schneider. In view of Corollary 4.5 and the question raised after, it seems plausible to make the following conjecture.

Conjecture 1. Assume that $(i)$ $A$ is an abelian variety over a number field $F$ which has ordinary reduction at every primes above $p$, $(ii)$ $F_\infty$ is a uniform admissible $p$-adic extension of $F$ of dimension $d \geq 2$ and $(iii)$ $X(A/F^{\mathrm{cyc}})$ is finitely generated torsion over $\mathbb{Z}_p[\![\Gamma]\!]$. Then we have

$$\mathrm{rank}_{\mathbb{Z}}(A(F_n)) \leq \left( \mathrm{rank}_{\mathbb{Z}}(A(F^{\mathrm{cyc}})) + \sum_{\substack{w \in S(F^{\mathrm{cyc}}), \\ \dim H_w \geq 1}} \mathrm{corank}_{\mathbb{Z}_p}\left(Z_v(F_w^{\mathrm{cyc}})(p)\right) \right) p^{(d-1)n} + O(p^{(d-2)n}),$$

where $S(F^{\mathrm{cyc}})$ is the set of primes of $F^{\mathrm{cyc}}$ above $S$ which are not divisible by $p$. In the event that the extra assumption of Theorem 3.2 is also valid, we replace $O(p^{(d-2)n})$ in the above inequality by $d\,\mathrm{corank}_{\mathbb{Z}_p}(A(F_\infty)(p))$.

The point of Conjecture 1 is that here we have replaced $\mathrm{rank}_{\mathbb{Z}_p}(X(A/F^{\mathrm{cyc}}))$ by the smaller quantity $\mathrm{rank}_{\mathbb{Z}}(A(F^{\mathrm{cyc}}))$. Note that there are examples where $\mathrm{rank}_{\mathbb{Z}_p}(X(A/F^{\mathrm{cyc}})) \neq \mathrm{rank}_{\mathbb{Z}}(A(F^{\mathrm{cyc}}))$ (see [19, pp. 140-142]). Nevertheless, we at least can record the following simple observation.

PROPOSITION 4.7. *Assume that* (*i*) *$A$ is an abelian variety over a number field $F$ which has ordinary reduction at every primes above $p$,* (*ii*) *$F_\infty$ is a uniform admissible $p$-adic extension of $F$ of dimension $d \geq 2$ and* (*iii*) *$X(A/F^{\mathrm{cyc}})$ is finitely generated over $\mathbb{Z}_p$ with $\mathrm{rank}_{\mathbb{Z}_p}(X(A/F^{\mathrm{cyc}})) = \mathrm{rank}_{\mathbb{Z}}(A(F^{\mathrm{cyc}}))$. Then we have*

$$\mathrm{rank}_{\mathbb{Z}}(A(F_n)) \leq \left( \mathrm{rank}_{\mathbb{Z}}(A(F^{\mathrm{cyc}})) + \sum_{\substack{w \in S(F^{\mathrm{cyc}}), \\ \dim H_w \geq 1}} \mathrm{corank}_{\mathbb{Z}_p}\left(Z_v(F_w^{\mathrm{cyc}})(p)\right) \right) p^{(d-1)n} + O(p^{(d-2)n}),$$

*where $S(F^{\mathrm{cyc}})$ is the set of primes of $F^{\mathrm{cyc}}$ above $S$ which are not divisible by $p$.*

*Proof.* Since $X(A/F^{\mathrm{cyc}})$ is finitely generated over $\mathbb{Z}_p$, it follows from a similar argument to that in [9, Theorem 2.1] that $X(A/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$ and hence satisfies the $\mathfrak{M}_H(G)$-conjecture. The conclusion is now a consequence of Corollary 4.5 and hypothesis (iii). □

We also refer readers to [11, Theorem 1.8], [13, Section 2.5] and [15, Theorems A.38 and A.41] for discussion in support for Conjecture 1.

Finally, one may be tempted to ask the following naive question.

QUESTION. Retain the assumptions of Conjecture 1. Does one always have

$$\mathrm{rank}_{\mathbb{Z}}(A(F_n)) = \left( \mathrm{rank}_{\mathbb{Z}}(A(F^{\mathrm{cyc}})) + \sum_{\substack{w \in S(F^{\mathrm{cyc}}), \\ \dim H_w \geq 1}} \mathrm{corank}_{\mathbb{Z}_p}\left(Z_v(F_w^{\mathrm{cyc}})(p)\right) \right) p^{(d-1)n} + O(p^{(d-2)n})$$

for $n \gg 0$?

However, as we shall see in the next section, this question has a *negative* answer.

**5. Additional evidence for Conjecture 1.** In this section, we describe how the deep works of Cornut-Vatsal [10], Howard [25] and Nekovář [44] can be applied to give further evidence to Conjecture 1. For the remainder of this section, $E$ will denote an elliptic curve defined over $\mathbb{Q}$ with good ordinary reduction at the prime $p$. Let $F$ be an imaginary quadratic field of $\mathbb{Q}$, and $F_\infty$ the $\mathbb{Z}_p^2$-extension of $F$. As before, write $G = \mathrm{Gal}(F_\infty)$ and $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. We also write $F_n$ for the intermediate subfield of $F_\infty/F$ with $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n \times \mathbb{Z}/p^n$. We shall further assume that our elliptic curve $E$ has no complex multiplication and has conductor coprime to the discriminant of $F$. For ease of comparison, we first work out how the conjectured upper bound of Conjecture 1 looks like in this situation. As a start, we record the following lemma which we prove in slight generality.

LEMMA 5.1. *Let $A$ be an abelian variety over $F$ with good ordinary reduction at the prime $v$ above $p$. Then for every prime $w$ of $F^{\mathrm{cyc}}$ above $v$, we have that $D_v(F_w^{\mathrm{cyc}})$ is finite.*

*Proof.* The long cohomology exact sequence of

$$0 \longrightarrow C_v \longrightarrow A(p) \longrightarrow D_v \longrightarrow 0$$

gives rise to an exact sequence

$$\begin{aligned} A(F_w^{\mathrm{cyc}})(p) \longrightarrow D_v(F_w^{\mathrm{cyc}}) &\longrightarrow H^1(F_w^{\mathrm{cyc}}, C_v) \\ &\longrightarrow H^1(F_w^{\mathrm{cyc}}, A(p)) \longrightarrow H^1(F_w^{\mathrm{cyc}}, D_v) \longrightarrow 0, \end{aligned}$$

where the final zero follows from that fact that $H^2(F_w^{\mathrm{cyc}}, C_v) = 0$ (cf. [45, Theorem 7.1.8(i)]). Since our abelian variety has good ordinary reduction at every prime of $v$, Imai's theorem [27] asserts that $A(F_w^{\mathrm{cyc}})(p)$ is finite. On the other hand, a local Euler characteristics argument (cf. [18, §3]) shows that $\mathrm{corank}_{\mathbb{Z}_p}(H^1(F_w^{\mathrm{cyc}}, A(p))) = \mathrm{corank}_{\mathbb{Z}_p}(H^1(F_w^{\mathrm{cyc}}, C_v)) + \mathrm{corank}_{\mathbb{Z}_p}(H^1(F_w^{\mathrm{cyc}}, D_v)$. Putting these information into the exact sequence, we see that the $D_v(F_w^{\mathrm{cyc}})$ has trivial $\mathbb{Z}_p$-corank. □

By a theorem of Kato [28], $X(E/F^{\mathrm{cyc}})$ is torsion over $\mathbb{Z}_p[\![\mathrm{Gal}(F^{\mathrm{cyc}}/F)]\!]$. Hence $\mathrm{rank}_{\mathbb{Z}}(E(F^{\mathrm{cyc}}))$ is well-defined (also see Theorem 6.4). Since $E$ is assumed to have no complex multiplication, $E(p)$ is not realizable over $F_\infty$ which, by [39, Lemma 6.2] or [57, Lemma 5.3], in turn implies that $E(F_\infty)(p)$ is finite. Finally, since no primes outside $p$ ramified in a $\mathbb{Z}_p^2$-extension, there are no extra contributions from local terms outside $p$. Hence Conjecture 1 in this setting reads as follow.

Conjecture 1′. Retain the notation and settings of this section. Then

$$\mathrm{rank}_{\mathbb{Z}}(E(F_n)) \leq \mathrm{rank}_{\mathbb{Z}}\left(E(F^{\mathrm{cyc}})\right)p^n.$$

Denote by $\epsilon(E/F, 1)$ the root number of Hasse-Weil $L$-function $L(E/F, s)$.

Theorem 5.2 (Cornut-Vatsal, Howard, Nekovář). *Retain the above settings. In the event $\epsilon(E/F, 1) = -1$, suppose further that $F$ only contains one prime above $p$ and that $p$ does not divide the class number of $F$. Then*

$$\mathrm{rank}_{\mathbb{Z}}(E(F_n)) = \begin{cases} O(1), & \text{if } \epsilon(E/F, 1) = +1 \\ p^n + O(1), & \text{if } \epsilon(E/F, 1) = -1. \end{cases}$$

*Proof.* As explained in the proof of [52, Proposition 3.14] (also see [41]), it follows from a combination of the deep results of Cornut-Vatsal [10], Howard [25] and Nekovář [44] that

$$\mathrm{corank}_{\mathbb{Z}_p[\![H]\!]}(E(F_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = \begin{cases} 0, & \text{if } \epsilon(E/F, 1) = +1, \\ 1, & \text{if } \epsilon(E/F, 1) = -1. \end{cases}$$

Therefore, by an application of [24, Theorem 1.10], we have

$$\mathrm{corank}_{\mathbb{Z}_p}\left(\left(E(F_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{H_n}\right) = \begin{cases} O(1), & \text{if } \epsilon(E/F, 1) = +1, \\ p^n + O(1), & \text{if } \epsilon(E/F, 1) = -1. \end{cases}$$

On the other hand, we have

$$\begin{aligned} \mathrm{corank}_{\mathbb{Z}_p}(E(F_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p) &\leq \mathrm{corank}_{\mathbb{Z}_p}\left(\left(E(F_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{G_n}\right) \\ &\leq \mathrm{corank}_{\mathbb{Z}_p}\left(\left(E(F_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{H_n}\right), \end{aligned}$$

where the second inequality is obvious (noting Lemma 2.6). For the first equality, we simply note that the kernel of the natural map

$$E(F_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \big(E(F_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\big)^{G_n}$$

is contained in the kernel of the map

$$\mathrm{Sel}(E/F_n) \longrightarrow S(E/F_\infty)^{G_n}$$

which in turn is contained in $H^1(G_n, E(F_\infty)(p))$ as seen in the proof of Lemma 3.3. But this latter group is finite as $E(F_\infty)(p)$ is finite by the discussion before Conjecture $1'$.

Now the conclusion of the proposition clearly follows in the case of $\epsilon(E/F, 1) = +1$. For the situation when $\epsilon(E/F, 1) = -1$, Bertolini [1, Proposition 7.6] has shown that

$$\mathrm{rank}_{\mathbb{Z}}(E(F_n^{\mathrm{ac}})) = p^n + O(1),$$

where here $F^{\mathrm{ac}}$ denotes the anticyclotomic $\mathbb{Z}_p$-extension of $F$ and $F_n^{\mathrm{ac}}$ is the intermediate subfield of $F^{\mathrm{ac}}$ with $|F_n^{\mathrm{ac}} : F| = p^n$. Since $E(F_n^{\mathrm{ac}}) \subseteq E(F_n)$, the required equality follows. □

Remark. Proposition 5.1, in particular, gives a negative answer to the question raised at the end of the preceding section when $\epsilon(E/F, 1) = +1$.

Corollary 5.3. *Retain the settings of Theorem 5.2. In the event that* $\epsilon(E/F, 1) = -1$*, suppose further that* $Ш(E/F)(p)$ *is finite. Then Conjecture* $1'$ *is valid.*

*Proof.* This is clear when $\epsilon(E/F, 1) = +1$. For the $\epsilon(E/F, 1) = -1$ case, it therefore remains to prove that $\mathrm{rank}_{\mathbb{Z}}(E(F^{\mathrm{cyc}})) \geq 1$ which amounts to showing that $\mathrm{rank}_{\mathbb{Z}}(E(F)) \geq 1$. But by the parity result of [43, Theorem 1], and noting that $Ш(E/F)(p)$ is finite by our hypothesis, we have that $\mathrm{rank}_{\mathbb{Z}}(E(F))$ is odd. In particularly, $\mathrm{rank}_{\mathbb{Z}}(E(F)) \geq 1$. □

Remark. We emphasis that we *do not* require the assumption that $X(E/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$-conjecture throughout the discussion in this section.

**6. A variant of Conjecture 1 for elliptic curve with supersingular reduction.** Throughout this section, let $E$ denote an elliptic curve over $\mathbb{Q}$ which has good supersingular reduction at the prime $p$. In particular, $E$ is no longer ordinary in the sense of Section 3. Despite this, we like to formulate a variant of Conjecture 1 for this class of elliptic curves in a modest setting, namely the case of a $\mathbb{Z}_p^2$-extension.

Denote by $\widetilde{E}$ the reduced curve of $E$ modulo $p$. We shall assume that $a_p = p + 1 - |\widetilde{E}(\mathbb{F}_p)| = 0$ (note that this automatically holds if $p \geq 5$). Let $F$ be an imaginary quadratic field of $\mathbb{Q}$ at which the prime $p$ splits completely, say $p = \mathfrak{p}\overline{\mathfrak{p}}$. Denote by $F(\mathfrak{p}^\infty)$ the unique $\mathbb{Z}_p$-extension of $F$ unramified outside $\mathfrak{p}$ and by $F(\mathfrak{p}^n)$ the intermediate subfield of $F(\mathfrak{p}^\infty)$ with $|F(\mathfrak{p}^n) : F| = p^n$. We have analogous definitions for $F(\overline{\mathfrak{p}}^\infty)$ and $F(\overline{\mathfrak{p}}^n)$. For each pair of nonnegative integers $m$ and $n$, write $F(\mathfrak{p}^m\overline{\mathfrak{p}}^n)$ for the compositum of the fields $F(\mathfrak{p}^m)$ and $F(\overline{\mathfrak{p}}^n)$.

We now denote by $\hat{E}$ the formal group associated to $E/\mathbb{Q}_p$. Let $w$ be a prime of $F_\infty$ above $\mathfrak{p}$. By abuse of notation, we write $w$ for the prime of $F(\mathfrak{p}^m\overline{\mathfrak{p}}^n)$ below this prime of $F_\infty$. Following [30, 35], we define the following groups

$$E^+(F(\mathfrak{p}^m\overline{\mathfrak{p}}^n)_w) = \{P \in \hat{E}(F(\mathfrak{p}^m\overline{\mathfrak{p}}^n)_w) \ : \ \mathrm{tr}_{m/l+1,n}(P) \in \hat{E}(F(\mathfrak{p}^l\overline{\mathfrak{p}}^n)_w), 2 \mid l, l < m\},$$

$$E^-(F(\mathfrak{p}^m\overline{\mathfrak{p}}^n)_w) = \{P \in \hat{E}(F(\mathfrak{p}^m\overline{\mathfrak{p}}^n)_w) \ : \ \mathrm{tr}_{m/l+1,n}(P) \in \hat{E}((F_{\mathfrak{p}^l\overline{p}^n})_w), 2 \nmid l, l < m\},$$

where $\mathrm{tr}_{m/l+1,n} : \hat{E}(F(\mathfrak{p}^m\overline{\mathfrak{p}}^n)_w) \longrightarrow \hat{E}(F(\mathfrak{p}^{l+1}\overline{\mathfrak{p}}^n)_w)$ denotes the trace map. For a prime $\overline{w}$ of $F_\infty$ above $\overline{\mathfrak{p}}$, the groups $E^{\pm}(F(\mathfrak{p}^m\overline{\mathfrak{p}}^n)_{\overline{w}})$ are defined in a similar fashion as above. From now on, write $F_n = F(\mathfrak{p}^n\overline{\mathfrak{p}}^n)$. Let $s, z \in \{+,-\}$. The signed Selmer group of $E$ over $F_n$ (cf. [30]) is defined to be

$$\begin{aligned}&\mathrm{Sel}^{s,z}(E/F_n)\\ &= \ker\left(\mathrm{Sel}(E/F_n) \longrightarrow \left(\bigoplus_{w|\mathfrak{p}} \frac{H^1(F_{n,w}, E(p))}{E^s(F_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right) \oplus \left(\bigoplus_{\overline{w}|\overline{\mathfrak{p}}} \frac{H^1(F_{n,\overline{w}}, E(p))}{E^z(F_{n,\overline{w}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)\right).\end{aligned}$$

Set $\mathrm{Sel}^{s,z}(E/F_\infty) = \varinjlim_n \mathrm{Sel}^{s,z}(E/F_n)$, where $F_\infty$ is the $\mathbb{Z}_p^2$-extension of $F$. We then write $X^{s,z}(E/F_\infty)$ for the Pontryagin dual of $\mathrm{Sel}^{s,z}(E/F_\infty)$. We also write $G = \mathrm{Gal}(F_\infty/F)$ and $G_n = \mathrm{Gal}(F_\infty/F_n)$. Recently, Lei and Sprung have established the following result (see [35, Theorem 4.4]).

THEOREM 6.1 (Lei-Sprung). *Suppose that $X^{s,z}(E/F_\infty)$ is torsion over $\mathbb{Z}_p[\![G]\!]$ for every $s, z \in \{+,-\}$. Then one has $\mathrm{rank}_{\mathbb{Z}}(E(F_n)) = O(p^n)$.*

It is then natural to ask if one can give an explicit upper bound as in the ordinary setting. This is the goal of the remainder of this section. Before doing so, we need to make the following supersingular analogue of the $\mathfrak{M}_H(G)$-conjecture (also see [34, Conjecture 3.16] and [36, Conjecture 5.3]).

SUPERSINGULAR $\mathfrak{M}_H(G)$-CONJECTURE. *For every $s, z \in \{+,-\}$, the module $X_f^{s,z}(E/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$, where $X_f^{s,z}(E/F_\infty) = X^{s,z}(E/F_\infty)/X^{s,z}_f(E/F_\infty)(p)$.*

The next result records an important consequence of the above conjecture on the structure of the module $X_f^{s,z}(E/F_\infty)$ which we shall require later.

PROPOSITION 6.2. *Retain the settings and notation of this section. Assume further that the Supersingular $\mathfrak{M}_H(G)$-Conjecture is valid for every $s, z \in \{+,-\}$. Then $H_i\big(H_n, X_f^{s,z}(E/F_\infty)\big) = 0$ for every $i \geq 1$ and $n \geq 0$.*

*Proof.* We first show that $X_f^{s,z}(E/F_\infty)$ has no nonzero torsion $\mathbb{Z}_p[\![H]\!]$-submodules. By the Supersingular $\mathfrak{M}_H(G)$-Conjecture, $X^{s,z}(E/F_\infty)$ is in particular $\mathbb{Z}_p[\![G]\!]$-torsion. Therefore, a similar argument to that in [29, Theorem 1.1] can be applied to show that $X^{s,z}(E/F_\infty)$ has no nonzero pseudo-null $\mathbb{Z}_p[\![G]\!]$-submodules. By [51, Lemma 4.2], this in turn implies that $X_f^{s,z}(E/F_\infty)$ has no nonzero pseudo-null $\mathbb{Z}_p[\![G]\!]$-submodules. Now a well-known theorem of Venjakob [54] says that a $\mathbb{Z}_p[\![G]\!]$-module $M$ which is $\mathbb{Z}_p[\![H]\!]$-finitely generated is a pseudo-null $\mathbb{Z}_p[\![G]\!]$-module if and only if it is a torsion $\mathbb{Z}_p[\![H]\!]$-module. Since $X_f^{s,z}(E/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$ by the validity of the Supersingular $\mathfrak{M}_H(G)$-Conjecture, the claim of this paragraph then follows from a combination of these observations.

We now prove our proposition. Since $H_n \cong \mathbb{Z}_p$, we have that $H_i(H_n, X_f^{s,z}(E/F_\infty)) = 0$ for $i \geq 2$. Denoting by $\gamma_H$ a topological generator of $H$, we have an identification $H_1(H_n, X_f^{s,z}(E/F_\infty)) = X_f^{s,z}(E/F_\infty)[\gamma_H^{p^n} - 1]$. But as seen in the previous paragraph, $X_f^{s,z}(E/F_\infty)$ has no nonzero torsion $\mathbb{Z}_p[\![H]\!]$-submodules. Therefore, we must have $H_1(H_n, X_f^{s,z}(E/F_\infty)) = 0$. The proof of the proposition is now complete. □

We are in position to establish the following supersingular analogue of Theorem 3.2.

THEOREM 6.3. *Retain the settings and notation of this section. Assume further that Supersingular $\mathfrak{M}_H(G)$-Conjecture is valid for all $s, z \in \{+, -\}$. Then we have*

$$\mathrm{rank}_{\mathbb{Z}}\left(E(F_n)\right) \leq \left( \sum_{s,z \in \{+,-\}} \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\left(X^{s,z}(E/F_\infty)\right) \right) p^n.$$

*Proof.* By [35, Proposition 4.3], we have

$$\mathrm{corank}_{\mathbb{Z}_p}\left(\mathrm{Sel}(E/F_n)\right) \leq \sum_{s,z \in \{+,-\}} \mathrm{corank}_{\mathbb{Z}_p}\left(\mathrm{Sel}^{s,z}(E/F_n)\right).$$

For each $s, z \in \{+, -\}$, the kernel of the natural map

$$\mathrm{Sel}^{s,z}(E/F_n) \longrightarrow \mathrm{Sel}^{s,z}(E/F_\infty)^{G_n}$$

is contained in the kernel of the map

$$\mathrm{Sel}(E/F_n) \longrightarrow \mathrm{Sel}(E/F_\infty)^{G_n}$$

which in turn is contained in $H^1(G_n, E(F_\infty)(p))$ via a similar argument to that in the proof of Lemma 3.3. We claim that this latter group is trivial. Supposing for now the claim holds. Then we have the following inequality

$$\mathrm{corank}_{\mathbb{Z}_p}\left(\mathrm{Sel}^{s,z}(E/F_n)\right) \leq \mathrm{rank}_{\mathbb{Z}_p}\left(X^{s,z}(E/F_\infty)_{G_n}\right).$$

By Lemma 2.4, the term on the right is equal to $\mathrm{rank}_{\mathbb{Z}_p}\left(X_f^{s,z}(E/F_\infty)_{G_n}\right)$ which is less than or equal to $\mathrm{rank}_{\mathbb{Z}_p}\left(X_f^{s,z}(E/F_\infty)_{H_n}\right)$. By virtue of Proposition 6.2, we may apply Lemma 2.3 to obtain $\mathrm{rank}_{\mathbb{Z}_p}\left(X_f^{s,z}(E/F_\infty)_{H_n}\right) = \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\left(X_f^{s,z}(E/F_\infty)\right)p^n$. The conclusion of the theorem now follows from combining these observations.

It remains to verify our claim. To do this, it suffices to show that $E(F_\infty)(p) = 0$. Let $w$ be a prime of $F_\infty$ lying over $p$. Since $p$ splits completely over $F$, we have $F_w^{\mathrm{cyc}} = \mathbb{Q}_p^{\mathrm{cyc}}$, and so we may apply [31, Proposition 8.7] to conclude that $E(F_w^{\mathrm{cyc}})(p) = 0$. It follows from this that $E(F^{\mathrm{cyc}})(p) = 0$. Since $F_\infty/F^{\mathrm{cyc}}$ is a pro-$p$ extension, this in turn implies that $E(F_\infty)(p) = 0$ by [45, Corollary 1.6.13]. □

We now proceed to formulate a variant of Conjecture 1 in this modest setting. Recall that it is well-known by now that $E$ is modular (see [3, 56]). Therefore, one may apply the results of Kato [28] and Rohrlich [49] to conclude the following.

THEOREM 6.4 (Kato, Rohrlich). *Let $E$ be an elliptic curve over $\mathbb{Q}$ and $L$ a finite abelian extension of $\mathbb{Q}$. Then $E(L^{\mathrm{cyc}})$ is a finitely generated abelian group.*

In particular, the theorem implies that the quantity $\mathrm{rank}_{\mathbb{Z}}\left(E(F^{\mathrm{cyc}})\right)$ is well-defined. Thus, we are in position to state our conjecture on the growth of Mordell-Weil ranks for an elliptic curve with supersingular reduction at $p$ in this modest setting.

CONJECTURE 2. Let $E$ be an elliptic curve over $\mathbb{Q}$ which has good supersingular reduction at the prime $p$ with $a_p = 0$. Denote by $F$ an imaginary quadratic field of

$\mathbb{Q}$ at which the prime $p$ splits completely. Write $F_n$ for the intermediate subfield of the $\mathbb{Z}_p^2$-extension $F_\infty$ of $F$ with $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n \times \mathbb{Z}/p^n$. Then we have

$$\mathrm{rank}_{\mathbb{Z}}(E(F_n)) \leq 4\,\mathrm{rank}_{\mathbb{Z}}\left(E(F^{\mathrm{cyc}})\right)p^n.$$

Although we are not able to relate $\mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}\left(X^{s,z}(E/F_\infty)\right)$ to invariants coming from the cyclotomic level, we believe it should be related to certain cyclotomic invariants which bound the quantity $\mathrm{rank}_{\mathbb{Z}}\left(E(F^{\mathrm{cyc}})\right)$, henceforth the "4" appearing in our conjecture. In view of Conjecture 1′, one might even ask if the "4" can be removed. We do not have an answer at this point of the writing.

## REFERENCES


[1] M. Bertolini, *Iwasawa theory for elliptic curves over imaginary quadratic fields*, J. Théor. Nombres Bordeaux, 13:1 (2001), pp, 1–25.

[2] A. Bhave, *Analogue of Kida's formula for certain strongly admissible extensions*, J. Number Theory, 122:1 (2007), pp. 100–120.

[3] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over Q: wild 3-adic exercises*, J. Amer. Math. Soc., 14:4 (2001), pp. 843–939.

[4] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, *The $GL_2$ main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES, 101 (2005), pp. 163–208.

[5] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math., 124 (1996), pp. 129–174.

[6] J. Coates and S. Howson, *Euler characteristics and elliptic curves II*, J. Math. Soc. Japan, 53:1 (2001), pp. 175–235.

[7] J. Coates, P. Schneider and R. Sujatha, *Links between cyclotomic and $GL_2$ Iwasawa theory*, Doc. Math. (2003) pp. 187–215, Extra Volume: Kazuya Kato's fiftieth birthday.

[8] J. Coates, P. Schneider and R. Sujatha, *Modules over Iwasawa algebra*, J. Inst. Math. Jussieu, 2:1 (2003), pp. 73–108.

[9] J. Coates and R. Sujatha, *On the $\mathfrak{M}_H(G)$-conjecture*, in: Non-abelian Fundamental Groups and Iwasawa Theory, eds J. Coates, M. Kim, F. Pop, M. Saidi and P. Schneider, London Math. Soc. Lecture Note Ser. 393, Cambridge Univ. Press, 2012, pp. 132–161.

[10] C. Cornut and V. Vatsal, *Nontriviality of Rankin-Selberg L-functions and CM points*, in: Burns, Buzzard, Nekovář (Eds.), $L$-functions and Galois Representations, Cambridge University Press, 2007, pp. 121–186.

[11] H. Darmon and Y. Tian, *Heegner points over towers of Kummer extensions*, Canad. J. Math., 62:5 (2010), pp. 1060–1081.

[12] D. Delbourgo and A. Lei, *Transition formulae for ranks of abelian varieties*, Rocky Mt. J. Math., 45:6 (2015), pp. 1807–1838.

[13] D. Delbourgo and A. Lei, *Estimating the growth in Mordell-Weil ranks and Shaferevich-Tate groups over Lie extensions*, Ramanujan J., 43 (2017), pp. 29–68.

[14] J. Dixon, M. P. F. Du Sautoy, A. Mann and D. Segal, *Analytic Pro-p Groups*, 2nd edn, Cambridge Stud. Adv. Math. 38, Cambridge Univ. Press, Cambridge, UK, 1999.

[15] T. Dokchitser and V. Dokchitser, *Computations in non-commutative Iwasawa theory*, with an appendix by J. Coates and R. Sujatha. Proc. Lond. Math. Soc. (3), 94:1 (2007), pp. 211–272.

[16] M. Drinen, *Iwasawa $\mu$-invariants of elliptic curves and their symmetric powers*, J. Number Theory, 102 (2003), pp. 191–213.

[17] K. R. Goodearl and R. B. Warfield, *An introduction to non-commutative Noetherian rings*, London Math. Soc. Stud. Texts 61, Cambridge University Press, 2004.

[18] R. Greenberg, *Iwasawa theory for p-adic representations*, in: Algebraic Number Theory-in honor of K. Iwasawa, ed. J. Coates, R. Greenberg, B. Mazur and I. Satake, Adv. Std. in Pure Math. 17, 1989, pp. 97–137.

[19] R. Greenberg, *Iwasawa theory for elliptic curves*, in: Arithmetic theory of elliptic curves (Cetraro, 1997), ed. C. Viola, Lecture Notes in Math., Vol. 1716 (Springer, Berlin, 1999), pp. 51–144.

[20] Y. Hachimori and K. Matsuno, *An analogue of Kida's formula for the Selmer groups of elliptic curves*, J. Algebraic Geom., 8 (1999), pp. 581–601.

[21] Y. Hachimori and T. Ochiai, *Notes on non-commutative Iwasawa theory*, Asian J. Math., 14:1 (2010), pp. 11–17.
[22] Y. Hachimori and R. Sharifi, *On the failure of pseudo-nullity of Iwasawa modules*, J. Algebraic Geom., 14:3 (2005), pp. 567–591.
[23] Y. Hachimori and O. Venjakob, *Completely faithful Selmer groups over Kummer extensions*, Doc. Math., (2003), pp. 443–478, Extra Volume: Kazuya Kato's fiftieth birthday.
[24] M. Harris, *Correction to p-adic representations arising from descent on abelian varieties*, Comp. Math., 121 (2000), pp. 105–108.
[25] B. Howard, *Iwasawa theory of Heegner points on abelian varieties of $GL_2$-type*, Duke Math. J., 124:1 (2004), pp. 1–45.
[26] S. Howson, *Euler characteristics as invariants of Iwasawa modules*, Proc. London Math. Soc. (3), 85:3 (2002), pp. 634–658.
[27] H. Imai, *A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions*, Proc. Japan Acad., 51 (1975), pp. 12–16.
[28] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, in: Cohomologies $p$-adiques et applications arithmétiques. III., Astérisque, 295 (2004), ix, pp. 117–290.
[29] B. D. Kim, *The plus/minus Selmer groups for supersingular primes*, J. Aust. Math. Soc., 95:2 (2013), pp. 189–200.
[30] B. D. Kim, *Signed-Selmer groups over the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field*, Canad. J. Math., 66:4 (2014), pp. 826–843.
[31] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math., 152:1 (2003), pp. 1–36.
[32] T. Y. Lam, *Lectures on Modules and Rings*, Grad. Texts in Math. 189, Springer, 1999.
[33] C. Y. Lee, *Non-commutative Iwasawa theory of elliptic curves at primes of multiplicative reduction*, Math. Proc. Cambridge Philos. Soc., 154:2 (2013), pp. 303–324.
[34] A. Lei, *Non-commutative p-adic L-functions for supersingular primes*, Int. J. Number Theory, 8:8 (2012), pp. 1813–1830.
[35] A. Lei and F. Sprung, *Ranks of elliptic curves over $\mathbb{Z}_p^2$-extensions*, Israel J. Math, 236:1 (2020), pp. 183–206.
[36] A. Lei and S. L. Zerbes, *Signed Selmer groups over p-adic Lie extension*, J. Théor. Nombres Bordeaux, 24:2 (2012), pp. 377–403.
[37] M. F. Lim, *A remark on the $\mathfrak{M}_H(G)$-conjecture and Akashi series*, Int. J. Number Theory, 11:1 (2015), pp. 269–297.
[38] M. F. Lim, *Notes on the fine Selmer groups*, Asian J. Math., 21:2 (2017), pp. 337–362.
[39] M. F. Lim and V. K. Murty, *The growth of Selmer group of an elliptic curve with split multiplicative reduction*, Int. J. Number Theory, 10:3 (2014), pp. 675–687.
[40] M. F. Lim and R. Sharifi, *Nekovář duality over p-adic Lie extensions of global fields*, Doc. Math., 18 (2013), pp. 621–678.
[41] M. Longo and S. Vigni, *Plus/minus Heegner points and Iwasawa theory of elliptic curves at supersingular primes*, Boll. Unione Mat. Ital., 12:3 (2019), pp. 315–347.
[42] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math., 18 (1972), pp. 183–266.
[43] J. Nekovář, *On the parity of ranks of Selmer groups IV*, with an appendix by Jean-Pierre Wintenberger, Comp. Math., 145 (2009), pp. 1351–1359.
[44] J. Nekovář, *Level raising and anticyclotomic Selmer groups for Hilbert modular forms of weight two*, Canad. J. Math., 64:3 (2012), pp. 588–668.
[45] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, 2nd edn., Grundlehren Math. Wiss. 323 (Springer-Verlag, Berlin, 2008).
[46] A. Neumann, *Completed group algebras without zero divisors*, Arch. Math., 51:6 (1988), pp. 496–499.
[47] Y. Ochi and O. Venjakob, *On the ranks of Iwasawa modules over p-adic Lie extensions*, Math. Proc. Cambridge Philos. Soc., 135:1 (2003), pp. 25–43.
[48] K. Ribet, *Torsion points of abelian varieties in cyclotomic extensions*, Enseign. Math., 27 (1981), pp. 315–319.
[49] D. E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math., 75 (1984), pp. 409–423.
[50] P. Schneider, *p-adic height pairings. II*, Invent. Math., 79 (1985), pp. 329–374.
[51] R. Sujatha, *Iwasawa theory and modular forms*, Pure Appl. Math. Q., 2:2 (2006), pp. 519–538.
[52] J. Van Order, *Some remarks on the two-variable main conjecture of Iwasawa theory for elliptic curves without complex multiplication*, J. Algebra, 350 (2012), pp. 273–299.
[53] O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc., 4:3 (2002), pp. 271–311.

[54] O. Venjakob, *A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory*, J. Reine Angew. Math., 559 (2003), pp. 153–191.
[55] O. Venjakob, *Characteristic elements in noncommutative Iwasawa theory*, J. Reine Angew. Math., 583 (2005), pp. 193–236.
[56] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2), 141:3 (1995), pp. 443–551.
[57] S. L. Zerbes, *Generalised Euler characteristics of Selmer groups*, Proc. London Math. Soc., 98:3 (2009), pp. 775–796.