RANKS OF ELLIPTIC CURVES OVER $\mathbb{Z}_p^2$-EXTENSIONS

BY

ANTONIO LEI

Département de mathématiques et de statistique, Université Laval
Pavillon Alexandre-Vachon, 1045 avenue de la médecine
Québec, QC G1V 0A6, Canada
e-mail: antonio.lei@mat.ulaval.ca

AND

FLORIAN SPRUNG

School of Mathematical and Statistical Sciences, Arizona State University
Tempe, AZ 85287-1804, USA
e-mail: florian.sprung@asu.edu

ABSTRACT

Let $E$ be an elliptic curve with good reduction at a fixed odd prime $p$ and $K$ an imaginary quadratic field where $p$ splits. We give a growth estimate for the Mordell–Weil rank of $E$ over finite extensions inside the $\mathbb{Z}_p^2$-extension of $K$.

1. Introduction

One fundamental question in the arithmetic of elliptic curves is to determine the Mordell–Weil rank of its rational points in a number field. While this question is hard, one can hope to answer a similar question in $p$-adic families of number fields: How does the Mordell–Weil rank grow in the finite layers of the maximal $p$-unramified extension$^1$ of a given number field $F$?

Received September 3, 2018 and in revised form March 3, 2019

$^1$ By the maximal $p$-unramified extension, we mean the maximal abelian pro-$p$ extension that is unramified outside $p$. 
When \( F \) is abelian over \( \mathbb{Q} \), works of Kato [Ka04] and Rohrlich [Ro84] show that the rank is bounded in the cyclotomic \( \mathbb{Z}_p \)-extension, i.e., the \( \mathbb{Z}_p \)-extension contained in \( \bigcup_n F(\zeta_{p^n}) \). Since the cyclotomic \( \mathbb{Z}_p \)-extension of \( \mathbb{Q} \) is its maximal \( p \)-unramified extension, an answer to the question is “It stays bounded” when \( F = \mathbb{Q} \).

The purpose of this article is to shed some light on the next simplest case, when \( F \) is an imaginary quadratic field \( K \). Such a \( K \) can have \( \mathbb{Z}_p \)-extensions in which the Mordell–Weil rank may be unbounded. In fact, Mazur formulated a precise conjecture in the case of ordinary primes \( p \), the Growth Number Conjecture [Ma83]. The Mordell–Weil rank at the \( n \)th layer of a \( \mathbb{Z}_p \)-extension of \( K \) is known to be of the form \( ap^n + O(1) \), i.e., it is governed mainly by an integer \( a \), the growth number. The conjecture gives a recipe to choose \( a \in \{0, 1, 2\} \) and predicts that \( a = 0 \) unless the \( \mathbb{Z}_p \)-extension one is scrutinizing is the anticyclotomic one. (The theorem of Kato–Rohrlich above is an instance for \( a = 0 \).) In work towards this conjecture, the theorems of Cornut and Vatsal [Co02, Va03] combined with Bertolini’s thesis [Be95] give scenarios in which \( a = 1 \) along anticyclotomic \( \mathbb{Z}_p \)-extensions, so that in particular the Mordell–Weil rank is not bounded. See also Bertolini [Be97] for a more precise growth pattern of the rank. For a counterpart to Bertolini’s result in the \( a_p = 0 \) case, see [LV19]. In the case where \( E \) has complex multiplication by \( K \), we remark that the growth patterns for the ordinary case and the supersingular case, as stated in [Gr01, discussion after Theorem 1.8], are different.

In this article, we develop methods to bound the Mordell–Weil rank in all subfields contained in the maximal \( p \)-unramified extension of \( K \). The main innovation is that we present methods for both the ordinary case and the supersingular case.

**Theorem 1.1:** Let \( E \) be an elliptic curve over \( \mathbb{Q} \), \( K \) an imaginary quadratic field along which an odd prime \( p \) coprime to the conductor of \( E \) splits and that the class number of \( K \) is coprime to \( p \). Let \( K_n \) be the subfield of the \( \mathbb{Z}_p^2 \)-extension of \( K \) so that \( \text{Gal}(K_n/K) \cong (\mathbb{Z}/p^n\mathbb{Z})^2 \). When \( p \) is supersingular, assume the cotorsion hypothesis (H.tor) introduced in Section 5.1, and when \( a_p = 0 \), assume it for all four signed Selmer groups. Then we have \( \text{rank } E(K_n) = O(p^n) \).

We may thus speak of a “2-dimensional growth number” that governs the rank of \( E(K_n) \) as one climbs along the two-dimensional tower of the \( \mathbb{Z}_p^2 \)-extension of \( K \). One strategy for proving a theorem like this is to employ a Control Theorem.
The idea of controlling, going back to Mazur, is the following: The $p^\infty$-Selmer group $\text{Sel}_p(E/K_n)$ at finite level should be controlled by easier Selmer groups at infinite level $K_\infty$. We directly succeed with this strategy when $p \nmid a_p$ (i.e., $p$ is ordinary). The appropriate control theorem is due to Greenberg and generalizes Mazur’s for the cyclotomic $\mathbb{Z}_p$-extension. A general growth lemma of Harris then allows us to deduce our main theorem.

When $a_p = 0$ (which is a subcase of the supersingular case $p \mid a_p$), Greenberg’s and Mazur’s control theorems fail. Kobayashi stated an analogue of Mazur’s control theorem by defining signed Selmer groups. He then realized that his signed Selmer groups control (in fact bound) the Mordell–Weil rank along the cyclotomic $\mathbb{Z}_p$-extension. In order to handle more than the cyclotomic $\mathbb{Z}_p$-extension, we employ a generalization—due to B. D. Kim—of the signed Selmer groups designed for $\mathbb{Z}_p^2$-extensions. After developing Kobayashi’s ideas further, we can secure the services of Kim’s Selmer groups to control the Mordell–Weil rank.

However, when $p \mid a_p \neq 0$, there is no control theorem available yet (even for the cyclotomic case), so we combine partial controlling with a different strategy. Recall that the idea behind the control theorem was to control the Selmer group at finite level via Selmer groups at the infinite level. Present technology does not allow us to do this, but we are able to control a quotient $\mathcal{X}_n^0$, the fine Selmer group (more precisely its dual), of the Selmer group dual $\mathcal{X}_n$. We deduce from this control theorem that the $\mathbb{Z}_p$-rank of $\mathcal{X}_n^0$ is $O(p^n)$. We thus have reduced the problem to showing that the $\mathbb{Z}_p$-rank of the kernel $\mathcal{Y}_n$ of the quotient map $\mathcal{X}_n \to \mathcal{X}_n^0$ is also $O(p^n)$.

The idea of shedding light on the Selmer group dual $\mathcal{X}_n$ via this kernel $\mathcal{Y}_n$ goes back to at least Kobayashi’s methods of estimating the growth of III in cyclotomic towers. One of Kobayashi’s key insights was to analyze $\mathcal{Y}_n$ via a similar but slightly more global Selmer-type group $\mathcal{Y}_n'$: While the defining condition for $\mathcal{Y}_n$ comes from the local points of $E$ inside the completions of $K_n$, $\mathcal{Y}_n'$ incorporates global information from the infinite level as well. (This extra global information is the $\text{Gal}(K_\infty/K_n)$-coinvariants of the Iwasawa cohomology at $K_\infty$.) From the point of view of $\mathbb{Z}_p$-ranks, $\mathcal{Y}_n'$ controls $\mathcal{Y}_n$ so that $\text{rk}_{\mathbb{Z}_p} \mathcal{Y}_n' \leq \text{rk}_{\mathbb{Z}_p} \mathcal{Y}_n$: Thus, we can control $\text{rk}_{\mathbb{Z}_p} \mathcal{X}_n$, and thus the Mordell–Weil rank at level $n$ if we could handle $\text{rk}_{\mathbb{Z}_p} \mathcal{Y}_n'$ directly. What is new in this work is that we handle $\text{rk}_{\mathbb{Z}_p} \mathcal{Y}_n'$ by relating it to Coleman maps that allows us to circumvent control theorems, and despite their absence show that $\text{rk}_{\mathbb{Z}_p} \mathcal{Y}_n' = O(p^n)$. 
To do this, we analyze the differences \( \text{rk}_{\mathbb{Z}_p} \mathcal{Y}'_{n+1} - \text{rk}_{\mathbb{Z}_p} \mathcal{Y}'_n \) by relating them to the \( \mathbb{Z}_p \)-ranks of the local modules that contain the defining conditions of \( \mathcal{Y}'_n \). We can break these local modules into (isotypical) components by a lemma of Cuoco and Monsky, and find that the rank of each component is \( c(p^{n+1} - p^n) \), where the possibilities for \( c \) are \( c = 0, 1, \) or \( 2 \). The crucial step in this paper is to show that among these isotypical components in question, \( c = 1 \) or \( c = 2 \) happens only finitely many times, in fact a number of times that is bounded independently of \( n \). Thus, the jump in ranks sums up to at most \( C(p^{n+1} - p^n) \) for a constant \( C \) independent of \( n \), giving the estimate \( \text{rk}_{\mathbb{Z}_p} \mathcal{Y}'_n \leq Cp^n \).

We accomplish this crucial step by showing that the localized Iwasawa cohomology vanishes—i.e., lies inside the Selmer condition—if and only if it connects to a zero of a \( p \)-adic power series via pairs of Coleman maps \( \text{Col}_p^\# \) and \( \text{Col}_p^\flat \) and a certain two by two matrix (the logarithm matrix). The localized Iwasawa cohomology vanishes when \( c \neq 0 \), while there can only be finitely many zeros of the power series it connects to. Therefore, we can have \( c \neq 0 \) only a finite number of times.

OUTLOOK. The ‘growth number conjecture’ [Ma83, Section 18] is one instance of the philosophy of Greenberg, Mazur, and Rubin that growth in the Mordell–Weil rank should come from zeros forced by functional equations (cf. [MR03]), but concerns the case of ordinary reduction. We write down a version that includes supersingular primes as well:

**Growth Number Vanishing Conjecture 1.2:** Let \( E \) be an elliptic curve with good reduction at a prime \( p \). The Mordell–Weil rank stays bounded along any \( \mathbb{Z}_p \)-extension of \( K \), unless the extension is anticyclotomic and the root number negative.

ACKNOWLEDGMENT. Parts of this work were carried out during the second-named author’s visit to Université Laval in spring 2017; he was supported by ERC grant 34061684 in fall 2017. The first-named author’s research is supported by the NSERC Discovery Grants Program 05710. We thank Henri Darmon, Ralph Greenberg, Meng Fai Lim, Bharathwaj Palvannan, and Karl Rubin for interesting discussions and helpful email correspondence. We thank Takenori Kataoka for his comments and suggestions for improvement on a previous version of the article, and for pointing out inaccuracies. We also thank

---

\(^2\) An upper bound for the “growth number”.
Meng Fai Lim for letting us know of a simplified proof of Theorem 4.3. Finally, we thank the anonymous referee for their comments and suggestions.

2. Setup and notation

Throughout this article, \( p \) is a fixed odd prime, \( E \) is an elliptic curve defined over \( \mathbb{Q} \) with good reduction at \( p \), and the Tate module of \( E \) at \( p \) will be denoted by \( T \). We also fix an imaginary quadratic field \( K \) in which \( p \) splits, i.e., \( (p) = pq \) with \( p \neq q \). For simplicity, we assume that the class number of \( K \) is coprime to \( p \). We fix embeddings \( \mathbb{Q} \hookrightarrow \mathbb{C} \) and \( \mathbb{Q} \hookrightarrow \mathbb{C}_p \) so that \( p \) lands inside the maximal ideal of \( \mathcal{O}_{\mathbb{C}_p} \).

Given a ideal \( a \) in the ring of integers of \( K \), we denote by \( K(a) \) its ray class field. Let \( K_{\infty} \) be the \( \mathbb{Z}_p^2 \)-extension of \( K \) and write \( \Gamma = \text{Gal}(K_{\infty}/K) \). Our assumption on the class number of \( K \) implies that \( K(1) \cap K_{\infty} = K \). If \( n \geq 0 \) is an integer, we write \( \Gamma_n = \Gamma^{p^n} \) and

\[
K_n = K^{\Gamma_n} = K(p^{n+1})^{\text{Gal}(K(p)/K)}.
\]

Note that \( \Gamma \cong \Gamma_p \times G_q \), where \( G_\star \) denotes the Galois group of the extension \( \text{Gal}(K(\star^{\infty}) \cap K_{\infty}/K) \).

We fix topological generators \( \gamma_p \) and \( \gamma_q \) for these groups. The Iwasawa algebra \( \Lambda := \mathbb{Z}_p[[\Gamma]] \) may be identified with the power series ring \( \mathbb{Z}_p[[\gamma_p - 1, \gamma_q - 1]] \). Given a \( \Lambda \)-module \( M \), we shall write \( M^\vee \) for its Pontryagin dual. We will employ the following theorem a number of times throughout the article.

**Theorem 2.1:** Let \( M \) be a finitely generated \( \Lambda \)-module of rank \( r \). Then we have

\[
\text{rank}_{\mathbb{Z}_p} M_{\Gamma_n} = rp^{2n} + O(p^n).
\]

**Proof.** This is a special case of [Ha00, Theorem 1.10]. \[\blacksquare\]

Let \( p^t \) be the number of primes of \( K_{\infty} \) above \( p \) and \( q \). We fix a choice of coset representatives \( \gamma_1, \ldots, \gamma_{p^t} \) and \( \delta_1, \ldots, \delta_{p^t} \) for \( \Gamma/\Gamma_p \) and \( \Gamma/\Gamma_q \) respectively, where \( \Gamma_\star \) denotes the decomposition group of \( \star \) in \( \Gamma \).

For an integer \( n \geq 1 \), we define

\[
\omega_n(X) := (1 + X)^{p^n} - 1,
\]
and the cyclotomic polynomial

\[ \Phi_n(X) := \frac{\omega_n(X)}{\omega_{n-1}(X)}. \]

We also define

\[ \omega_n^+(X) := X \prod_{1 < i \leq n, i \text{ even}} \Phi_i(X), \quad \omega_n^-(X) := X \prod_{1 \leq i \leq n, i \text{ odd}} \Phi_i(X). \]

3. The ordinary case

In this section, we assume that \( E \) has good ordinary reduction at \( p \) and we study the Mordell–Weil ranks of \( E \) over \( K_n \) as \( n \) varies. The result should be well-known among the experts, but to our knowledge it is not written down. We record it here in particular to illustrate the divergence in techniques between the supersingular case and the ordinary case.

Given an algebraic extension \( F \) of \( \mathbb{Q} \), the \((p\text{-primary})\) Selmer group of \( E \) over \( F \) is defined to be

\[ \text{Sel}_p(E/F) = \ker \left( H^1(F, E[p^\infty]) \to \prod_v \frac{H^1(F_v, E[p^\infty])}{E(F_v) \otimes \mathbb{Q}_p / \mathbb{Z}_p} \right), \]

where \( v \) runs through all places of \( F \) in the product. The Selmer group over \( K_\infty \) satisfies the following control theorem.

**Theorem 3.1:** Let \( E/\mathbb{Q} \) be an elliptic curve with good ordinary reduction at \( p \). For an integer \( n \geq 0 \), let \( s_n \) denote the restriction map

\[ \text{Sel}_p(E/K_n) \to \text{Sel}_p(E/K_\infty)^{\Gamma_n}. \]

Then \( \ker(s_n) \) and \( \text{coker}(s_n) \) are finite.

**Proof.** This is a special case of [Gr03, Theorem 2].

**Theorem 3.2:** Let \( E/\mathbb{Q} \) be an elliptic curve with good ordinary reduction at \( p \). Then we have

\[ \text{rank}_{\mathbb{Z}_p} \text{Sel}_p(E/K_n)^{\vee} = O(p^n) \]

for \( n \gg 0 \).
Proof. That the dual Selmer group $\text{Sel}_p(E/K_\infty)\vee$ is torsion over $\Lambda$ is [vO12, Theorem 3.8]. We may thus combine Theorems 2.1 and 3.1 to deduce that

$$\text{rank}_{\mathbb{Z}_p}\text{Sel}_p(E/K_n)\vee = \text{rank}_{\mathbb{Z}_p}(\text{Sel}_p(E/K_\infty))_{\Gamma_n} = O(p^n),$$

hence the result. 

4. The $a_p = 0$ case

Let $\hat{E}$ denote the formal group attached to $E$ over $\mathbb{Z}_p$. Let $\mathfrak{p}$ be a fixed prime of $K(p^\infty)$ lying above $p$. We abuse notation and denote the prime $L \cap \mathfrak{p}$ again by $\mathfrak{p}$ whenever $L$ is a sub-extension of $K(p^\infty)/K$. Kim [Ki14] defined the following groups, building on work of Kobayashi [Ko03].

$$E^+(K(p^m \mathfrak{q}^n)_{\mathfrak{p}}) = \{ P \in \hat{E}(K(p^m \mathfrak{q}^n)_{\mathfrak{p}}) : \text{Tr}_{m/l+1,n} P \in \hat{E}(K(p^l \mathfrak{q}^n)_{\mathfrak{p}}), 2|l < m \},$$

$$E^-(K(p^m \mathfrak{q}^n)_{\mathfrak{p}}) = \{ P \in \hat{E}(K(p^m \mathfrak{q}^n)_{\mathfrak{p}}) : \text{Tr}_{m/l+1,n} P \in \hat{E}(K(p^l \mathfrak{q}^n)_{\mathfrak{p}}), 2 \nmid l < m \}.$$ 

Here,

$$\text{Tr}_{m/l+1,n} : \hat{E}(K(p^m \mathfrak{q}^n)_{\mathfrak{p}}) \to \hat{E}(K(p^{l+1} \mathfrak{q}^n)_{\mathfrak{p}})$$

denotes the trace map and $m$ and $n$ are non-negative integers. Furthermore, we define

$$E^\pm((K_n)_{\mathfrak{p}}) := E^\pm(K(p^{n+1})_{\mathfrak{p}}) \Delta \subset E((K_n)_{\mathfrak{p}}),$$

where

$$\Delta := \text{Gal}(K(p)/K).$$

Given a prime $\mathfrak{Q}$ of $K(p^\infty)$ lying above $\mathfrak{q}$, we may define $E^\pm((K_\infty)_{\mathfrak{Q}})$ similarly. For $\bullet, \circ \in \{ +, - \}$, we define the signed Selmer group over $K_n$ by

$$\text{Sel}_{p}^\bullet(E/K_n)$$

$$:= \ker\left( \text{Sel}_p(E/K_n) \to \prod_{\mathfrak{p} \mid p} H^1((K_n)_{\mathfrak{p}}, E[p^\infty]) \otimes \mathbb{Q}_p / \mathbb{Z}_p \times \prod_{\mathfrak{Q} \mid \mathfrak{q}} H^1((K_n)_{\mathfrak{Q}}, E[p^\infty]) \otimes \mathbb{Q}_p / \mathbb{Z}_p \right).$$

We have a similar definition for $\text{Sel}_{p}^\bullet(E/K_\infty)$ on taking $E^\pm((K_\infty)_{\ast})$ to be the union of $E^\pm((K_n)_{\ast})$.

---

3 While van Order’s paper studies non-CM elliptic curves, the proof of Theorem 3.8 applies equally to CM curves.
Lemma 4.1: Let \( n \geq 0 \) and \( \star \in \{ p, q \} \). We put
\[
E_{\pm} = \bigoplus_{\mathfrak{p} \mid \star} E_{\pm}((K_n)_{\mathfrak{p}}), \quad E_{\pm}^1 = \bigoplus_{\mathfrak{p} \mid \star} \hat{E}(K_\star), \quad E_{\star} = \bigoplus_{\mathfrak{p} \mid \star} \hat{E}((K_n)_{\mathfrak{p}}),
\]
where \( \mathfrak{p} \) is a prime of \( K_n \). For \( \circ, \bullet \in \{ +, -, 1, \forall \} \), we write
\[
E_{\circ \bullet} = E_{\circ} \oplus E_{\bullet}.
\]
All horizontal and vertical sequences in the following commutative diagram are exact:

\[
\begin{array}{ccccccc}
0 & \rightarrow & E_{11} & \rightarrow & E_{1+} \oplus E_{1-} & \rightarrow & E_{1\forall} & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \rightarrow & E_{+1} & \rightarrow & E_{++} \oplus E_{+-} & \rightarrow & E_{+\forall} & \rightarrow & 0 \\
\oplus & & \ominus & & \oplus & & \ominus \\
0 & \rightarrow & E_{-1} & \rightarrow & E_{-+} \oplus E_{--} & \rightarrow & E_{-\forall} & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \rightarrow & E_{\forall 1} & \rightarrow & E_{\forall+} \oplus E_{\forall-} & \rightarrow & E_{\forall\forall} & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \rightarrow & 0 & \rightarrow & 0 & \rightarrow & 0 & \rightarrow & 0
\end{array}
\]

Proof. It follows from the definition of \( E_{\pm} \) that
\[
E_{\star}^{+} \cap E_{\star}^{-} = E_{\star}^1
\]
(cf. [Ko03, proof of Proposition 8.12]). The result follows from a repeated application of [Ki14, Proposition 2.15].

Proposition 4.2: Let \( n \geq 0 \). For \( \circ, \bullet \in \{ +, -, 1, \forall \} \), let \( E_{\circ \bullet} = E_{\circ} \oplus E_{\bullet} \) be as in Lemma 4.1. We write
\[
\text{Sel}_{\circ \bullet} = \ker \left( \text{Sel}_p(E/K_n) \rightarrow \bigoplus_{\mathfrak{p} \mid p} H^1((K_n)_{\mathfrak{p}}, E[p^\infty]) \times \bigoplus_{\mathfrak{q} \mid q} H^1((K_n)_{\mathfrak{q}}, E[p^\infty]) \right)
\]
\[
\rightarrow \frac{E_{\circ}}{E_{\circ} \otimes \mathbb{Q}_p / \mathbb{Z}_p} \oplus \frac{E_{\bullet}}{E_{\bullet} \otimes \mathbb{Q}_p / \mathbb{Z}_p}.
\]
Then the horizontal and vertical sequences of the following commutative diagram are exact:

\[
\begin{array}{cccccc}
0 & 0 & 0 & 0 & 0 & 0 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
0 & \text{Sel}^{11} & \text{Sel}^{1+} \oplus \text{Sel}^{1-} & \text{Sel}^{1\forall} & 0 & 0 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
0 & \text{Sel}^{+1} & \text{Sel}^{++} \oplus \text{Sel}^{+-} & \text{Sel}^{+\forall} & 0 & 0 \\
\oplus & \oplus & \oplus & 0 & 0 & 0 \\
0 & \text{Sel}^{-1} & \text{Sel}^{-+} \oplus \text{Sel}^{-} & \text{Sel}^{-\forall} & 0 & 0 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
0 & \text{Sel}^{\forall 1} & \text{Sel}^{\forall+} \oplus \text{Sel}^{\forall-} & \text{Sel}^{\forall\forall} & 0 & 0 \\
\end{array}
\]

Furthermore, the cokernel of the last map on all horizontal and vertical sequences are finite.

Note in particular that \( \text{Sel}^{\forall\forall} = \text{Sel}_p(E/K_n) \).

**Proof.** This follows from the same proof of [Ko03, Proposition 10.1]. □

**Theorem 4.3:** Let \( E/\mathbb{Q} \) be an elliptic curve with good supersingular reduction at \( p \) and \( a_p = 0 \). Suppose that the Selmer groups \( \text{Sel}_p^{\pm \pm}(E/K_\infty) \) are \( \Lambda \)-cotorsion. Then,

\[
\text{rank}_{\mathbb{Z}_p} \text{Sel}_p(E/K_n)^\forall = O(p^n)
\]

for \( n \gg 0 \).

**Proof.** Proposition 4.2 implies that

\[
\text{rank}_{\mathbb{Z}_p} \text{Sel}_p(E/K_n)^\forall \leq \sum_{\circ, \bullet \in \{+,-\}} \text{rank}_{\mathbb{Z}_p} \text{Sel}_p^{\circ \bullet}(E/K_n)^\forall.
\]

The inflation-restriction exact sequence induces the isomorphism

\[
H^1(K_n, E[p^\infty]) \xrightarrow{\sim} H^1(K_\infty, E[p^\infty])^\Gamma_n
\]

since \( E(K_\infty)[p^\infty] = 0 \) by [Ko03, proof of Proposition 8.7]. This gives the injection

\[
\text{Sel}_p^{\circ \bullet}(E/K_n) \hookrightarrow \text{Sel}_p^{\circ \bullet}(E/K_\infty)^\Gamma_n.
\]
Consequently,
\[
\text{rank}_{\mathbb{Z}_p} \text{Sel}^\bullet_p (E/K_n)^{\vee} \leq \text{rank}_{\mathbb{Z}_p} \text{Sel}^\bullet_p (E/K_\infty)^{\vee} = O(p^n)
\]
by Theorem 2.1 and our assumption that each Selmer group is $\Lambda$-cotorsion.

5. The general supersingular case

In this section, $E$ is an elliptic curve with good supersingular reduction at $p$ with $a_p \neq 0$. In particular, $a_p = \pm p$.

5.1. $\sharp/\flat$-Coleman maps and local properties. Let $F_\infty$ and $k_{cyc}$ be the unramified $\mathbb{Z}_p$-extension and the $\mathbb{Z}_p$-cyclotomic extension of $\mathbb{Q}_p$, respectively. Let $k_\infty$ be the compositum of $F_\infty$ and $k_{cyc}$. For $n \geq 0$, $k_n$ and $F_n$ denote the sub-extensions of $k_{cyc}$ and $F_\infty$ such that $[k_n : \mathbb{Q}_p] = p^n$ and $[F_n : \mathbb{Q}_p] = p^n$ respectively. Let
\[
\Gamma_p = \text{Gal}(k_\infty/\mathbb{Q}_p), \quad \Gamma_{ur} = \text{Gal}(F_\infty/\mathbb{Q}_p) = \langle \sigma \rangle \quad \text{and} \quad \Gamma_{cyc} = \text{Gal}(k_{cyc}/\mathbb{Q}_p) = \langle \gamma \rangle,
\]
where $\gamma$ is a fixed topological generator of $\Gamma_{cyc}$ and $\sigma$ is the arithmetic Frobenius.

We recall from [Sp12, LLZ10] that for $\bullet \in \{\sharp, \flat\}$, there is a Coleman map $\text{Col}_cyc^\bullet : H^1(\mathbb{Q}_p, T \otimes \mathbb{Z}_p[[\Gamma_{cyc}]]) \to \mathbb{Z}_p[[\Gamma_{cyc}]]$ decomposing Perrin–Riou’s big logarithm map
\[
\mathcal{L}_{cyc} = (\varphi(\varphi)) \cdot \text{M}_{\log} \begin{pmatrix} \text{Col}_{\sharp}^{cyc} \\ \text{Col}_{\flat}^{cyc} \end{pmatrix},
\]
where $\varphi$ is a basis of $\text{Fil}^0 \mathfrak{D}_{\text{cris}}(T)$, $\text{M}_{\log}$ is the logarithm matrix defined as
\[
\lim_{n \to \infty} A^{n+1} C_n \cdots C_1,
\]
with
\[
A = \begin{pmatrix} 0 & -1 \\ 1 & \frac{1}{p} \end{pmatrix} \quad \text{and} \quad C_n = \begin{pmatrix} a_p & 1 \\ \Phi_n(\gamma) & 0 \end{pmatrix}.
\]

As shown in [BL20, §2.3], we may take inverse limits of the Coleman maps over $F_n$ to define two-variable versions of these maps, decomposing the two-variable big logarithm map of Loeffler–Zerbes in [LZ14]. Furthermore, on choosing a basis of the Yager module defined in [LZ14, §3], we may assume that the Coleman maps land inside $\mathbb{Z}_p[[\Gamma_p]]$. More precisely, we have
\[
\text{Col}_{\sharp}, \text{Col}_{\flat} : H^1(\mathbb{Q}_p, T \otimes \mathbb{Z}_p[[\Gamma_p]]) \to \mathbb{Z}_p[[\Gamma_p]],
\]
such that

\[ L = (\omega \varphi(\omega)) M_{\log} \begin{pmatrix} \text{Col}_z \\ \text{Col}_y \end{pmatrix}, \]

where

\[ L : H^1(\mathbb{Q}_p, T \otimes \mathbb{Z}_p[[\Gamma_p]]) \to \mathcal{H}(\Gamma_p) \otimes \mathbb{D}_{\text{cris}}(T) \]

is Loeffler–Zerbes’ big logarithm map multiplied by the chosen basis of the Yager module. See [Sp16, §2] and [BL20, §2.3].

Let \( F = F_m \cdot k_n \) for some integers \( m \) and \( n \). The Coleman maps can be used to study Bloch–Kato’s Selmer condition over \( F \), which is commonly denoted by \( H^1_f(F, T) \). Note that in the case of elliptic curves, there is an isomorphism

\[ H^1_f(F, T) \cong \hat{E}(\mathfrak{M}_F), \]

where \( \hat{E} \) denotes the formal group attached to \( E \) at \( p \) and \( \mathfrak{M}_F \) denotes the maximal ideal of the ring of integers of \( F \) (cf. [BK90, Example 3.11]).

**Proposition 5.1:** Let \( z \in H^1(\mathbb{Q}_p, T \otimes \mathbb{Z}_p[[\Gamma_p]]) \) and \( \eta \) a be character on \( \Gamma_p \) whose cyclotomic part is of conductor \( p^{n+1} > 1 \). If we write \( e_\eta \) for the idempotent corresponding to the character \( \eta \), then, \( e_\eta \cdot z \) lies inside \( e_\eta \cdot H^1_f(F, T) \) if and only if the element in

\[ H^1_{z,n} \text{Col}_z(z)^{\sigma^{-n-1}} + H_{y,n} \text{Col}_y(z)^{\sigma^{-n-1}} \in \mathbb{Z}_p[[\Gamma_p]] \]

vanishes at \( \eta \), where \( H_{z,n} \) and \( H_{y,n} \) are given by the entries of the first row of \( C_n \cdots C_1 \).

**Proof.** Let \( \exp^* : H^1(F, T) \to F \otimes \mathbb{D}_{\text{cris}}(T) \) be Bloch–Kato’s dual exponential map. Then its kernel is exactly \( H^1_f(F, T) \). Recall from [LZ14, Theorem 4.15] that

\[ \Phi^{-n-1} \mathcal{L}(z)(\eta) = \varepsilon(\eta^{-1}) \exp^*(e_\eta \cdot z), \]

where \( \varepsilon(\eta^{-1}) \) denotes the \( \varepsilon \)-factor of \( \eta^{-1} \) and \( \Phi \) is the operator on \( F_m \otimes \mathbb{D}_{\text{cris}}(T) \) which acts as \( \sigma \) on \( F_m \) and \( \varphi \) on \( \mathbb{D}_{\text{cris}}(T) \). Hence, \( e_\eta \cdot z \) lies inside \( e_\eta \cdot H^1_f(F, T) \) if and only if \( \Phi^{-n-1} \mathcal{L}(z)(\eta) = 0 \).

By definition, \( M_{\log} \) is invariant under \( \sigma \). Furthermore, [LLZ17, Lemma 3.7] tells us that

\[ M_{\log}(\eta) = A^{n+1} C_n \cdots C_1(\eta). \]
Note that $A^{n+1}$ is the matrix of $\Phi^{n+1}$ with respect to the basis $\{\omega, \varphi(\omega)\}$. If we apply $\Phi^{-n-1}$ to (1), we obtain

$$
\Phi^{-n-1} L(z)(\eta) = (\omega \varphi(\omega)) C_n \cdots C_1(\eta) \left( \begin{array}{c} \text{Col}_p(z)^{\sigma^{-n-1}}(\eta) \\ \text{Col}_p(z)^{\sigma^{-n-1}}(\eta) \end{array} \right).
$$

Recall from the definition of $C_n$ that the second row of $C_n(\eta)$ vanishes as $\eta$ sends $\gamma$ to a primitive $p^n$-th root of unity. Consequently, the expression above simplifies to (2) and we are done.

5.2. $\sharp/b$-Selmer groups. Recall that $\gamma_1, \ldots, \gamma_{p^i}$ is a chosen set of coset representatives of $\Gamma/\Gamma_p$, where $\Gamma_p$ is the decomposition group at $p$. This gives the decomposition

$$
H^1(K_p, T \otimes \Lambda) = \bigoplus_{i=1}^{p^i} H^1(K_p, T \otimes \mathbb{Z}_p[[\Gamma_p]]) \cdot \gamma_i.
$$

We may identify $K_p$ with $\mathbb{Q}_p$, $\Gamma_p$ with $\Gamma_p$, and $G_p$ with $\Gamma_{cyc}$ (see Remark 5.2 below). Under this identification, define the $\sharp/b$-Coleman maps $\text{Col}_{p, \bullet}$ at $p$ by

$$
H^1(K_p, T \otimes \Lambda) = \bigoplus_{i=1}^{p^i} H^1(\mathbb{Q}_p, T \otimes \mathbb{Z}_p[[\Gamma_p]]) \cdot \gamma_i \mapsto \Lambda \\
\sum x_i \cdot \gamma_i \mapsto \sum \text{Col}_{\bullet}(x_i) \cdot \gamma_i.
$$

For $\bullet \in \{\sharp, b\}$, we define

$$
E^\bullet_p \subset \bigoplus_{i=1}^{p^i} H^1(K_{\infty, \gamma_i}, E[p^\infty])
$$
to be the orthogonal complement of $\ker \text{Col}_{p, \bullet}$ under local Tate duality. Similarly, we may define $\text{Col}_{q, \bullet}$ and $E^\bullet_q$ in the same way.

Remark 5.2: When we localize at $p$, the Galois group $G_q$ is sent to $\Gamma_{ur}$. We may thus identify the local image of $G_p$ with $\Gamma_{cyc}$ via the series of isomorphisms

$$
G_p \cong \text{Gal}(K_{\infty}/K(\mathfrak{q}^{\infty})) \cong \text{Gal}(k_{\infty}/F_{\infty}) \cong \Gamma_{cyc}.
$$

We record this identification by sending our topological generators $\gamma_p$ and $\gamma_q$ to $\gamma$ and $\sigma$ respectively.

When we localize at $q$, the identifications are reversed.
Let $N$ be the conductor of $E$ and let $S$ be the set of primes dividing $pN$. Given a number field $F$, we write $H^1_S(F, -)$ for the Galois cohomology of the Galois group of the maximal algebraic extension of $F$ that is unramified outside $S$. Recall that the classical $p$-Selmer group over $K_\infty$ is defined to be

$$\text{Sel}_p(E/K_\infty) = \ker \left( H^1_S(K_\infty, E[p^\infty]) \rightarrow \bigoplus_{v|pN} \frac{H^1(K_\infty, v, E[p^\infty])}{E(v) \otimes \mathbb{Q}_p / \mathbb{Z}_p} \right).$$

We define four $\sharp/\flat$-Selmer groups

$$\text{Sel}^\circ\bullet_p(E/K_\infty) = \ker \left( \text{Sel}_p(E/K_\infty) \rightarrow \bigoplus_{i=1}^{\rho^\circ} H^1(K_\infty, \gamma_i, E[p^\infty]) \oplus \bigoplus_{i=1}^{\rho^\circ} H^1(K_\infty, \delta_i, E[p^\infty]) \right)$$

for $\circ, \bullet \in \{\sharp, \flat\}$. We shall from now on assume the following hypothesis holds:

(H.tor) At least one of the four Selmer groups $\text{Sel}^\circ\bullet_p(E/K_\infty)$, $\circ, \bullet \in \{\sharp, \flat\}$, is $\Lambda$-cotorsion.

These Selmer groups can be linked to certain 2-variable $p$-adic $L$-functions constructed in [Le14]. When the latter is non-zero, then (H.tor) holds (see [CCSS17, §3.4]).

These Selmer groups generalize the signed Selmer groups of Kim. However, we do not know whether an analogue for Proposition 4.2 holds for these Selmer groups. Consequently, we cannot generalize the proof of Theorem 4.3 directly to this setting. Instead, we make use of ideas from [Sp13, LLZ17] to estimate the ranks of $E$ over $K_\infty$.

The strict/fine Selmer group over $K_\infty$

$$\text{Sel}^0_p(E/K_\infty) = \ker \left( \text{Sel}_p(E/K_\infty) \rightarrow \bigoplus_{v|p} H^1(K_\infty, v, E[p^\infty]) \right)$$

fits into the Poitou–Tate exact sequence

$$H^1_{Iw}(K_\infty, T) \xrightarrow{\text{ker } \text{Col}_{p, \circ}} H^1(K_\infty, T \otimes \Lambda) \oplus H^1(K_q, T \otimes \Lambda) \xrightarrow{\text{ker } \text{Col}_{q, \bullet}} \text{Sel}^\circ\bullet_p(E/K_\infty)^\vee \rightarrow \text{Sel}^0(E/K_\infty)^\vee \rightarrow 0,$$

where $H^1_{Iw}(K_\infty, T)$ is defined as the inverse limit $\lim_{\leftarrow} H^1_S(K_n, T)$ (see, for example, [Ko03, (7.20)]).
Lemma 5.3: Under the hypothesis (H.tor), the Iwasawa module $\text{Sel}_p^0(E/K_\infty)^\vee$ is $\Lambda$-torsion, whereas $H^1_{Iw}(K_\infty, T)$ is of rank 2.

Proof. The torsionness of $\text{Sel}_p^0(E/K_\infty)^\vee$ follows from that of $\text{Sel}_p^{\bullet}(E/K_\infty)^\vee$ and (3). The statement about $H^1_{Iw}(K_\infty, T)$ then follows from the weak Leopoldt conjecture, cf. [LZ14, Corollary A.8].

Remark 5.4: Let $c_1, c_2 \in H^1_{Iw}(K_\infty, T)$ be any elements such that $H^1_{Iw}(K_\infty, T)/\langle c_1, c_2 \rangle$ is $\Lambda$-torsion. Then, the cotorsionness of $\text{Sel}_p^{\bullet}(E/K_\infty)$ together with (3) imply that

$$\text{det}(\text{Col}_p, (\text{loc}_p(c_1)), \text{Col}_q, (\text{loc}_q(c_1))) \neq 0.$$ 

We shall denote this determinant by $\text{det} \text{Col}_\bullet(c_1 \wedge c_2)$ from now on.

5.3. Classical Selmer groups and Coleman maps. In this subsection, we relate modified Selmer-type groups to Coleman maps. The following cohomology groups were introduced when studying the growth of Sha in [Ko03] and [Sp13]:

For $n \geq 0$, we abbreviate $H^1(K_{n,v}, T)/H^1_f(K_{n,v}, T)$ by $H^1_f(K_{n,v}, T)$ and put

$$\mathcal{Y}_n := \text{coker} \left( H^1_{Iw}(K_\infty, T)_{\Gamma_n} \to \prod_{v|p} H^1_f(K_{n,v}, T) \right),$$

$$\mathcal{Y}_n := \text{coker} \left( H^1_{S}(K_n, T) \to \prod_{v|p} H^1_f(K_{n,v}, T) \right).$$

We also define the $\mathcal{X}_n^0$ and $\mathcal{X}_n$ to be the Pontryagin dual of the strict Selmer group $\text{Sel}_p^0(E/K_n)$ and the classical Selmer group $\text{Sel}_p(E/K_n)$ respectively. The Poitou–Tate exact sequence over $K_n$ gives the following exact sequence:

$$0 \to \mathcal{Y}_n \to \mathcal{X}_n \to \mathcal{X}_n^0 \to 0$$

(see, for example, [Ko03, (10.35)]).

Proposition 5.5: The $\mathbb{Z}_p$-rank of $\mathcal{X}_n^0$ is $O(p^n)$. 
Proof. We first show that the strict Selmer group satisfies a control theorem. Consider the following commutative diagram

\[
\begin{array}{ccccccc}
0 & \rightarrow & \text{Sel}_p^0(E/K_n) & \rightarrow & H^1(K_n, E[p^\infty]) & \rightarrow & \prod_{v_n} H^1(K_{v_n}, E[p^\infty]) \\
& & \downarrow{\alpha_n} & & \downarrow{\beta_n} & & \downarrow{\prod \gamma_{v_n}} \\
0 & \rightarrow & \text{Sel}_p^0(E/K_\infty) & \rightarrow & H^1(K_\infty, E[p^\infty]) & \rightarrow & \prod_{w} H^1(K_{\infty,w}, E[p^\infty])
\end{array}
\]

where the vertical maps are restriction maps; the product on the first row runs over all places \(v_n\) of \(K_n\), whereas that on the second row runs over all places \(w\) of \(K_\infty\). By definition, both rows are exact. Note that \(E(K_\infty,w)[p^\infty] = 0\) for all places \(w\) of \(K_\infty\) such that \(w|p\) (cf. [KO18, Proposition 3.1]). Therefore, \(\gamma_{v_n}\) is an isomorphism for all \(v_n|p\) by the inflation-restriction exact sequence. Similarly, \(\beta_n\) is also an isomorphism. If \(v_n \nmid p\), then the proof of [Gr03, Theorem 2] tells us that \(\ker \gamma_{v_n}\) is finite of bounded order (see also [Ki14, Proposition 2.19]). Therefore, on applying the snake lemma to (4), we deduce that \(\ker \alpha_n\) and \(\text{coker} \alpha_n\) are finite and of orders bounded independently of \(n\).

Lemma 5.3 tells us that \(X^0_n\) is \(\Lambda\)-torsion. Hence, Theorem 2.1 together with the control theorem above imply that

\[
\text{rank}_{\mathbb{Z}_p} X^0_n = \text{rank}_{\mathbb{Z}_p} (X^0_\infty)_{\Gamma_n} = O(p^n),
\]

as required. \(\blacksquare\)

In order to study \(\text{rank}_{\mathbb{Z}_p} X_n\), it is thus enough to study \(\text{rank}_{\mathbb{Z}_p} Y_n\). Furthermore, there is a natural surjection \(Y'_n \to Y_n\) (cf. [Ko03, diagram (10.36)]). In particular,

\[
\text{rank}_{\mathbb{Z}_p} Y_n = \text{rank}_{\mathbb{Z}_p} Y'_n
\]

for all \(n \geq 0\) and we are reduced to estimating \(\text{rank}_{\mathbb{Z}_p} Y'_n\). We shall do so via the \#/♭-Coleman maps. Let us first recall the following calculations from [CM81]. We shall write \(W = \mu_{p^\infty} \times \mu_{p^\infty}\). Given \(w = (w_1, w_2) \in W\), we shall write

\[
\mathbb{Z}_p[w] = \mathbb{Z}_p[w_1, w_2].
\]

If \(F \in \Lambda\), we may evaluate \(F\) at \(w\) in the following way. We may rewrite \(F\) as a power series in \(\gamma_p - 1\) and \(\gamma_q - 1\), say \(F_0(\gamma_p - 1, \gamma_q - 1)\). Then, we define

\[
F(w) = F_0(w_1 - 1, w_2 - 1) \in \mathbb{Z}_p[w].
\]

Given any \(\Lambda\)-module \(M\), we write \(M_w = M \otimes \mathbb{Z}_p[w]\) for the \(\mathbb{Z}_p[w]\)-module induced by this evaluation map.
Lemma 5.6: Let \( n \geq 0 \) be an integer and \( M \) a \( \Lambda \)-module. Then

\[
\text{rank}_{\mathbb{Z}_p} M_{\Gamma_n} = \text{rank}_{\mathbb{Z}_p} \bigoplus_w M_w,
\]

where the direct sum runs over the conjugacy classes of \( w \in W \) such that \( w^{p^n} = (1, 1) \).

Proof. This is an immediate consequence of [CM81, Lemma 2.7], which says that the kernel and cokernel of the morphism \( M_{\Gamma_n} \to \bigoplus_w M_w \) are both finite. \( \blacksquare \)

From now on, we fix two elements \( c_1, c_2 \) of \( H_1^{I_w}(K_{\infty}, T) \) such that \( H_1^{I_w}(K_{\infty}, T)/\langle c_1, c_2 \rangle \) is \( \Lambda \)-torsion (c.f. Remark 5.4). Let us write \( \text{loc}_{p,n}(c_i) \) for the image of \( c_i \) inside

\[
H_1^{I_f}(K_{n,p}, T) := \prod_{v|p} H_1^{I_f}(K_{n,v}, T).
\]

Corollary 5.7: Let \( n \geq 1 \) be an integer. Then,

\[
\text{rank}_{\mathbb{Z}_p} \mathcal{Y}_n' - \text{rank}_{\mathbb{Z}_p} \mathcal{Y}_{n-1}' \leq \sum_w \text{rank}_{\mathbb{Z}_p} \left( \frac{H_1^{I_f}(K_{n,p}, T)}{\langle \text{loc}_{p,n}(c_1), \text{loc}_{p,n}(c_2) \rangle} \right)_w,
\]

where the sum runs over the conjugacy classes of \( w \in W \) such that \( w^{p^n} = (1, 1) \), but \( w^{p^{n-1}} \neq (1, 1) \).

Proof. We scrutinize \( \mathbb{Z}_p \)-ranks by tensoring with \( \mathbb{Q}_p \). In this proof, denote \( H_1^{I_f}(K_{n,p}, T) \) by \( H_1^1 \) for simplicity. Notice that

\[
H_n^1 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \bigoplus_{v|p} K_{n,v}
\]

via the Bloch–Kato dual exponential map. This implies that

\[
(H_n^1 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)_{\Gamma_{n-1}} \cong H_{n-1}^1 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.
\]

Therefore,

\[
(H_n^1 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)_w = (H_{n-1}^1 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)_w
\]

if \( w^{p^{n-1}} = (1, 1) \). Thus, applying Lemma 5.6 to \( H_1^1 \) implies that

\[
\text{rank}_{\mathbb{Z}_p} H_n^1 = \text{rank}_{\mathbb{Z}_p} H_{n-1}^1 + \sum_w \text{rank}_{\mathbb{Z}_p} (H_1^1)_w,
\]

where the sum runs over the conjugacy classes of \( w \in W \) such that \( w^{p^n} = (1, 1) \), but \( w^{p^{n-1}} \neq (1, 1) \). We have a similar decomposition for \( H_{I_w}(K_{\infty}, T)_{\Gamma_n} \), which
we abbreviate by $H_{1w,n}^1$. Functoriality of coinvariants and tensor products gives us the commutative diagram

$$
\begin{array}{ccc}
(H_{1w,n}^1 \otimes \mathbb{Q}_p) & \cong & (H_{1w,n-1}^1 \otimes \mathbb{Q}_p) \oplus (\bigoplus_w (H_{1w,n}^1)_w \otimes \mathbb{Q}_p) \\
\downarrow & & \downarrow \\
(H_n^1 \otimes \mathbb{Q}_p) & \cong & (H_{n-1}^1 \otimes \mathbb{Q}_p) \oplus (\bigoplus_w (H_n^1)_w \otimes \mathbb{Q}_p),
\end{array}
$$

where the direct sums on the right are over the $w$ as above. From this, we conclude that

$$\text{rank}_{\mathbb{Z}_p} \mathcal{Y}_n' = \text{rank}_{\mathbb{Z}_p} \mathcal{Y}_{n-1}' + \sum_w \text{rank}_{\mathbb{Z}_p} (\mathcal{Y}_n')_w.$$

The corollary now follows from the fact that $\mathcal{Y}_n'$ is a quotient of

$$H_{1/f}^1(K_{n,p}, T) / \langle \text{loc}_{p,n}(c_1), \text{loc}_{p,n}(c_2) \rangle$$

(and hence the same is true after we tensor these modules by $\mathbb{Z}_p[w]$).

Let $\theta$ be a character of $\Gamma$ sending $(\gamma_p, \gamma_q)$ to $(w_1, w_2) \in W$. Then evaluating an element of $\mathbb{Z}_p[[X,Y]]$ at $X = w_1 - 1$ and $Y = w_2 - 1$ is equivalent to evaluating an element of $\Lambda$ at $\theta$. We will use these two evaluation maps interchangeably from now on.

Given an element $\zeta \in \mu_{p \infty}$, we shall write $\text{ord}(\zeta)$ for the smallest integer $t$ such that $\zeta^p^t = 1$. Note that if $w = (w_1, w_2) \in W$ with $\text{ord}(w_1) = r$ and $\text{ord}(w_2) = s$, the corresponding character on $\Gamma$ has conductor $p^{r+1}q^{s+1}$. When restricted to $\Gamma_p$ (respectively $\Gamma_q$), the series of isomorphisms in Remark 5.2 tells us that the character $\theta$ gives a character on $\Gamma_p$ whose cyclotomic part is of conductor $p^{r+1}$ (respectively $p^{s+1}$). The element in (2) then leads us to introduce the following notation. For $\star \in \{p, q\}$, $z \in H^1(K_\star, T \otimes \Lambda)$ and $t \geq 0$, we write

$$\text{Col}_{\star,t}(z) = H_{\star,\sharp,t} \text{Col}_{\star,\sharp}(z)^{\sigma^{-1}} + H_{\star,\flat,t} \text{Col}_{\star,\flat}(z)^{\sigma^{-t}}.$$

where $H_{\star,\sharp,t}$ and $H_{\star,\flat,t}$ are the entries of the first row in the matrix obtained by replacing $\gamma$ with $\gamma_\star$ in the product $C_t \cdots C_1$.  


Lemma 5.8: Let \( \theta \) be a character of \( \Gamma \) of conductor \( p^{r+1}q^{s+1} \) and write \( w = (\theta(\gamma_p), \theta(\gamma_q)) \in W \). Then
\[
\text{rank}_{\mathbb{Z}_p} \left( \frac{H^1_{/f}(K_{n,p},T)}{\langle \text{loc}_{p,n}(c_1), \text{loc}_{p,n}(c_2) \rangle} \right)_w > 0
\]
if and only if
\[
\det \begin{pmatrix} \text{Col}_{p,r}(\text{loc}_p(c_1)) & \text{Col}_{q,s}(\text{loc}_q(c_1)) \\ \text{Col}_{p,r}(\text{loc}_p(c_2)) & \text{Col}_{q,s}(\text{loc}_q(c_2)) \end{pmatrix}
\]
vanishes at \( \theta \). When the aforementioned determinant does vanish at \( \theta \), the \( \mathbb{Z}_p \)-rank of \( (\frac{H^1_{/f}(K_{n,p},T)}{\langle \text{loc}_{p,n}(c_1), \text{loc}_{p,n}(c_2) \rangle})_w \) is either \( \dim_{\mathbb{Q}_p} \mathbb{Q}_p(\theta) \) or \( 2\dim_{\mathbb{Q}_p} \mathbb{Q}_p(\theta) \), where \( \mathbb{Q}_p(\theta) \) is the extension of \( \mathbb{Q}_p \) generated by the image of \( \theta \).

Proof. For \( t \in \{r, s\} \) and \( * \in \{p, q\} \), the morphism \( \text{Col}_{*,t} \) induces
\[
\left( \prod_{v|*} H^1_{/f}(K_{n,v},T) \right)_w \otimes \mathbb{Q}_p \cong \mathbb{Q}_p(\theta)
\]
by Proposition 5.1. Consequently, if we write
\[
v_1 = (\text{Col}_{p,r}(\text{loc}_p(c_1))(\theta), \text{Col}_{q,s}(\text{loc}_q(c_1))(\theta)),
v_2 = (\text{Col}_{p,r}(\text{loc}_p(c_2))(\theta), \text{Col}_{q,s}(\text{loc}_q(c_2))(\theta)),
\]
then
\[
\left( \frac{H^1_{/f}(K_{n,p},T)}{\langle \text{loc}_{p,n}(c_1), \text{loc}_{p,n}(c_2) \rangle} \right)_w \otimes \mathbb{Q}_p \cong \frac{\mathbb{Q}_p(\theta)^{\oplus 2}}{\langle v_1, v_2 \rangle}
\]
as \( \mathbb{Q}_p(\theta) \)-vector spaces. Hence the result. \( \blacksquare \)

For simplicity, we shall write the determinant above as \( \det \text{Col}_{r,s}(c_1 \land c_2) \). A direct calculation tells us that this is related to the determinants \( \det \text{Col}_{\circ,s}(c_1 \land c_2) \) (as defined in Remark 5.4) for \( \circ, \bullet \in \{\#, \flat\} \), via the following equation:
\[
(6) \quad \det \text{Col}_{r,s}(c_1 \land c_2)(\theta) = \sum_{\circ, \bullet \in \{\#, \flat\}} H_{p,\circ,r} H_{q,\bullet,s} \det \text{Col}_{\circ,s}(c_1 \land c_2)(\theta).
\]

We shall study the \( p \)-adic valuations of the summands on the right-hand side of (6) to show that \( \det \text{Col}_{r,s}(c_1 \land c_2)(w) \neq 0 \) for a large family of characters \( \theta \).
5.4. \( p \)-adic valuations of power series. Recall that given an element \( \zeta \in \mu_{p^\infty} \), we write \( \text{ord}(\zeta) \) for the smallest integer \( t \) such that \( \zeta^{p^t} = 1 \).

**Proposition 5.9:** Let \( F(X, Y) \in Z_p[[X, Y]] \) be a non-zero power series. There exist integers \( a, b_1, b_2, c_1, c_2 \) and \( n_0 \) such that for all \( w = (w_1, w_2) \in W \setminus (\mu_{p^{n_0}} \times \mu_{p^{n_0}}) \),

\[
\text{ord}_p(F(w)) = a + \frac{b_i}{\varphi(p^n)} + \frac{c_i}{\varphi(p^n)},
\]

whenever \( |\text{ord}(w_1) - \text{ord}(w_2)| \gg 0 \), where \( \text{ord}(w_1) = m, \text{ord}(w_2) = n \) and \( i = 1 \) or \( 2 \) depending on whether \( m > n \) or \( n > m \).

**Proof.** Let us write

\[
F(X, Y) = p^a G(X, Y)
\]

for some integer \( a \geq 0 \) and \( G(X, Y) \in Z_p[[X, Y]] \setminus p\mathbb{Z}_p[[X, Y]] \). Following [Cu80, proof of Proposition 2.9], there exist integers \( b, c \geq 0 \) independent of \( m \) such that whenever \( m \gg 0 \), we have via the Weierstrass preparation theorem that

\[
G(w_1 - 1, Y) = u \times (w_1 - 1)^b(Y^c + d_{c-1}Y^{c-1} + \cdots + d_1Y + d_0),
\]

where \( u \in Z_p[w_1][Y]^{\times} \) and \( d_i \in (w_1 - 1)Z_p[w_1] \). In particular, \( \text{ord}_p(d_i) \geq \frac{1}{\varphi(p^m)} \) for all \( i \). Consequently, we have

\[
\text{ord}_p(G(w)) = \frac{b}{\varphi(p^m)} + \frac{c}{\varphi(p^n)},
\]

whenever \( \frac{c}{\varphi(p^n)} < \frac{1}{\varphi(p^m)} \) (which can be ensured by \( n - m \gg 0 \)).

Similarly, when \( m - n \gg 0 \), we may evaluate \( \text{ord}_p(G(w)) \) by applying the Weierstrass preparation theorem for \( G(X, w_2 - 1) \).

This can be translated to a result on elements in the Iwasawa algebra \( \Lambda \) as follows.

**Corollary 5.10:** Let \( F \in \Lambda \) be a non-zero element. There exist integers \( a, b_1, b_2, c_1, c_2 \) and \( n_0 \) such that whenever \( \theta \) is a character of \( \Gamma \) of conductor \( p^r q^{s+1} \) with \( r, s \geq n_0 \) and \( |r - s| \gg 0 \), we have

\[
\text{ord}_p(F(\theta)) = a + \frac{b_i}{\varphi(p^n)} + \frac{c_i}{\varphi(p^s)},
\]

where \( i = 1 \) or \( 2 \) depending on whether \( r > s \) or \( s > r \).
Let us now recall the following result from [Sp13, Lemma 4.5] and [LLZ17, Proposition 4.6].

**Proposition 5.11:** Let \( \eta \) be a character of \( \Gamma_{\text{cyc}} \) of conductor \( p^{n+1} > 1 \) and let \( H_{\overset{\ast}{}},n \) and \( H_{\overset{\flat}{}},n \) be as defined in (2). Then,

\[
\text{ord}_p(H_{\overset{\ast}{}},n(\eta)) = \begin{cases} 1 + \sum_{i=1}^{\frac{n-1}{2}} \frac{1}{p^{2i-1}}, & n \in 2\mathbb{Z} + 1, \\ \sum_{i=1}^{\frac{n}{2}} \frac{1}{p^{2i-1}}, & n \in 2\mathbb{Z}, \end{cases}
\]

whereas

\[
\text{ord}_p(H_{\overset{\flat}{}},n(\eta)) = \begin{cases} \sum_{i=1}^{\frac{n-1}{2}} \frac{1}{p^{2i}}, & n \in 2\mathbb{Z} + 1, \\ 1 + \sum_{i=1}^{\frac{n}{2} - 1} \frac{1}{p^{2i}}, & n \in 2\mathbb{Z}. \end{cases}
\]

We now combine all these calculations to study the \( p \)-adic valuations of the summands that appeared in (6).

**Proposition 5.12:** Let \( \theta \) be a character of \( \Gamma \) of conductor \( p^{r+1}q^{s+1} \). Let \( \circ, \bullet, \nabla, \nabla \in \{\ast, \flat\} \) with \( (\circ, \bullet) \neq (\nabla, \nabla) \) and assume that at least one of \( \det \text{Col}_\circ(\Theta(c_1 \land c_2)) \) and \( \det \text{Col}_\nabla(\Theta(c_1 \land c_2)) \) is non-zero. Then

\[
\text{ord}_p(H_{p,\circ,r}H_{q,\bullet,s} \det \text{Col}_\circ(\Theta(c_1 \land c_2)) \neq \text{ord}_p(H_{p,\nabla,r}H_{q,\nabla,s} \det \text{Col}_\nabla(\Theta(c_1 \land c_2)))
\]

whenever \( r, s, |r - s| \gg 0 \).

**Proof.** If either \( \det \text{Col}_\circ(\Theta(c_1 \land c_2)) \) or \( \det \text{Col}_\nabla(\Theta(c_1 \land c_2)) \) is zero, then the result is immediate. We may therefore assume that both values are non-zero.

Let us first consider the case where \( \circ = \nabla \) but \( \bullet \neq \nabla \). Let us say \( \bullet = \ast \) and \( \nabla = \flat \), \( r > s \) and \( s \) is odd. We would like to show that

\[
\text{ord}_p(H_{q,\ast,s} \det \text{Col}_{\circ,\ast}(\Theta(c_1 \land c_2)) \neq \text{ord}_p(H_{q,\flat,s} \det \text{Col}_{\circ,\flat}(\Theta(c_1 \land c_2))).
\]

Corollary 5.10 and Proposition 5.11 tell us that

\[
\text{ord}_p(H_{q,\ast,s} \det \text{Col}_{\circ,\ast}(\Theta(c_1 \land c_2))) = 1 + \sum_{i=1}^{\frac{s-1}{2}} \frac{1}{p^{2i-1}} + a + \frac{b}{\varphi(p^r)} + \frac{c}{\varphi(p^s)},
\]

\[
\text{ord}_p(H_{q,\flat,s} \det \text{Col}_{\circ,\flat}(\Theta(c_1 \land c_2))) = \sum_{i=1}^{\frac{s-1}{2}} \frac{1}{p^{2i}} + d + \frac{e}{\varphi(p^r)} + \frac{f}{\varphi(p^s)}.
\]
for some integers $a, b, c, d, e, f$ that are independent of $r$ and $s$ as long as $r, s, r - s \gg 0$. The difference of these two quantities is given by

$$1 + a - d + \frac{b - e}{\varphi(p^r)} + \frac{c - f}{\varphi(p^s)} + \frac{1 - p^{1-s}}{p + 1}.$$ 

The appearance of $p + 1$ in the denominator of the last term implies that this is non-zero. The cases $s$ is even or $s > r$ can be proved similarly. The same proof also works when $\circ = ▽$ and $\bullet \neq ▽$.

It remains to consider the case where $\circ \neq ▽$ and $\bullet \neq ▽$. Suppose that $(\circ, \bullet) = (\sharp, \flat), (\triangledown, \bigtriangledown) = (b, \sharp)$ and that both $r$ and $s$ are even. Then, the difference

$$\text{ord}_p(H_{p,\sharp, r} H_{q, \flat, s} \det \text{Col}_{\sharp, \flat} (c_1 \wedge c_2)(\theta)) - \text{ord}_p(H_{p,\flat, r} H_{q, \sharp, s} \det \text{Col}_{\flat, \sharp} (c_1 \wedge c_2)(\theta))$$

is of the form

$$\ast + \frac{\ast}{\varphi(p^r)} + \frac{\ast}{\varphi(p^s)} + \frac{p^{1-s} - p^{1-r}}{p + 1},$$

where the $\ast$’s represent some integers. Once again, this cannot be zero because of the presence of $p + 1$ in the denominator of the last term as long as $r \neq s$. Similar calculations show that the same is true for the other combinations of parities of $r$ and $s$. The same proof also works when $(\circ, \bullet) = (\sharp, \sharp), (\triangledown, \bigtriangledown)$.

**Corollary 5.13:** Suppose $(\mathcal{H}.\text{tor})$ holds. Let $n \geq 1$ be an integer and write $\Xi_n$ for the set of characters $\theta$ on $\Gamma$ which factor through $\Gamma_n$ but not $\Gamma_{n-1}$ such that $\det \text{Col}_{r, s} (c_1 \wedge c_2)(\theta) = 0$ (with the conductor of $\theta$ being $p^{r+1} q^{s+1}$). Then, the cardinality of $\Xi_n$ is bounded independently of $n$.

**Proof.** Recall from (6) that

$$\det \text{Col}_{r, s} (c_1 \wedge c_2)(\theta) = \sum_{\circ, \bullet \in \{\sharp, \flat\}} H_{p,\circ, r} H_{q, \bullet, s} \det \text{Col}_{\circ, \bullet} (c_1 \wedge c_2)(\theta)$$

if $\theta$ is a character on $\Gamma$ of conductor $p^{r+1} q^{s+1}$. If $\theta$ factors through $\Gamma_n$ but not $\Gamma_{n-1}$, then either $r$ or $s$ equals $n$.

If $\text{Sel}^\bullet(E/K_{\infty})^\vee$ is $\Lambda$-torsion, then Remark 5.4 says that $\det \text{Col}_{\circ, \bullet} (c_1 \wedge c_2) \neq 0$. Therefore, $(\mathcal{H}.\text{tor})$ ensures that when $r, s \gg 0$, at least one of the four determinants $\det \text{Col}_{\circ, \bullet} (c_1 \wedge c_2)(\theta)$ does not vanish. We may therefore apply Proposition 5.12, which tells us that for $r, s, |r - s| \gg 0$, the non-zero summands of the four-term sum have distinct $p$-adic valuations.
In short, there exists a fixed integer $n_0$ (independent of $n$), such that if $\det \Col_{r,s}(c_1 \wedge c_2)(\theta) = 0$, then $r, s, |r - s| \leq n_0$. If either $r$ or $s$ equals $n$, then the number of such $(r, s)$ is clearly bounded. Hence we are done.

We can now give the following bound on $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{Y}'_n$.

**Proposition 5.14:** $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{Y}'_n = O(p^n)$.

**Proof.** Lemma 5.8 tells us that

$$\mathrm{rank}_{\mathbb{Z}_p} \mathcal{Y}'_n - \mathrm{rank}_{\mathbb{Z}_p} \mathcal{Y}'_{n-1} \leq 2C_n \varphi(p^n),$$

where $C_n$ is the number of characters $\theta$ that factor through $\Gamma_n$ but not $\Gamma_{n-1}$ and that $\det \Col_{r,s}(c_1 \wedge c_2)(\theta) = 0$ ($C_n$ is the cardinality of $\Xi_n$.) Corollary 5.13 says that there exists a constant $C$ such that $C_n \leq C$ for all $n$. On summing the above inequality over $n$, we have

$$\mathrm{rank}_{\mathbb{Z}_p} \mathcal{Y}'_n - \mathrm{rank}_{\mathbb{Z}_p} \mathcal{Y}'_1 \leq \sum_{i=2}^{n} C \varphi(p^i) = O(p^n)$$

as required.

---

**References**

[Be95] M. Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions*, Compositio Mathematica **99** (1995), 153–182.

[Be97] M. Bertolini, *Growth of Mordell–Weil groups in anticyclotomic towers*, in *Arithmetic geometry (Cortona, 1994)*, Symposia Mathematica, Vol. 37, Cambridge University Press, Cambridge, 1997, pp. 23–44.

[BK90] S. Bloch and K. Kato, *$L$-functions and Tamagawa numbers of motives*, in *The Grothendieck Festschrift, Vol. I*, Progress in Mathematics, Vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[BL20] K. Büyükboduk and A. Lei, *Iwasawa theory of elliptic modular forms over imaginary quadratic fields at non-ordinary primes*, International Mathematics Research Notices, to appear, [https://doi.org/10.1093/imrn/rnz117](https://doi.org/10.1093/imrn/rnz117).

[CCSS17] F. Castella, M. Çiperiani, C. Skinner and F. Sprung, *On the Iwasawa main conjectures for modular forms at non-ordinary primes*, [https://arxiv.org/abs/1804.10993](https://arxiv.org/abs/1804.10993).

[Co02] C. Cornut, *Mazur’s conjecture on higher Heegner points*, Inventiones mathematicae **148** (2002), 495–523.

[CM81] A. Cuoco and P. Monsky, *Class numbers in $\mathbb{Z}_p^d$-extensions*, Mathematische Annalen **255** (1981), 235–258.
[Cu80] A. Cuoco, The growth of Iwasawa invariants in a family, Compositio Mathematica 41 (1980), 415–437.

[Gr01] R. Greenberg, Introduction to the Iwasawa Theory for elliptic curves, in Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Mathematics Series, Vol. 9, American Mathematical Society, Providence, RI, 2001, pp. 407–464.

[Gr03] R. Greenberg, Galois theory for the Selmer group of an abelian variety, Compositio Mathematica 136 (2003), 255–297.

[Ha00] M. Harris, Correction to: “p-adic representations arising from descent on abelian varieties”, Compositio Mathematica 121 (2000), 105–108.

[Ka04] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, Astérisque 295 (2004), 117–290.

[Ko03] S.-I. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, Inventiones Mathematicae 152 (2003), 1–36.

[Ki14] B. D. Kim, Signed-Selmer groups over the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field, Canadian Journal of Mathematics 66 (2014), 826–843.

[KO18] T. Kitajima and R. Otsuki, On the plus and minus Selmer groups for elliptic curves at supersingular primes, Tokyo Journal of Mathematics 41 (2018), 273–303.

[Le14] A. Lei, Factorisation of two-variable p-adic L-functions, Canadian Mathematical Bulletin 57 (2014), 845–852.

[LLZ17] A. Lei, D. Loeffler and S. L. Zerbes, On the asymptotic growth of Bloch–Kato–Shafarevich–Tate groups of modular forms over cyclotomic extensions, Canadian Journal of Mathematics 69 (2017), 826–850.

[LLZ10] A. Lei, D. Loeffler and S. L. Zerbes, Wach modules and Iwasawa theory for modular forms, Asian Journal of Mathematics 14 (2010), 475–528.

[LZ14] D. Loeffler and S. L. Zerbes, Iwasawa theory and p-adic L-functions over $\mathbb{Z}_p^2$-extensions, International Journal of Number Theory 10 (2014), 2045–2095.

[LV19] M. Longo and S. Vigni, Plus/minus Heegner points and Iwasawa theory of elliptic curves at supersingular primes, Bollettino dell’Unione Matematica Italiana 12 (2019), 315–347.

[Ma83] B. Mazur, Modular curves and arithmetic, in Proceedings of the International Congress of Mathematicians, Vols. 1, 2 (Warsaw, 1983), PWN, Warsaw, 1984, pp. 185–211.

[MR02] B. Mazur and K. Rubin, Elliptic curves and class field theory, in Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), Higher Ed. Press, Beijing, 2002, pp. 185–195.

[MR03] B. Mazur and K. Rubin, Studying the growth of Mordell–Weil, Documenta Mathematica Extra Volume (2003), 585–607.

[Ro84] D. E. Rohrlich, On L-functions of elliptic curves and cyclotomic towers, Inventiones Mathematicae 75 (1984), 409–423.

[Sp12] F. Sprung, Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures, Journal of Number Theory 132 (2012), 1483–1506.

[Sp13] F. Sprung, The Šafarevič–Tate group in cyclotomic $\mathbb{Z}_p$-extensions at supersingular primes, Journal für die Reine und Angewandte Mathematik 681 (2013), 199–218.
[Sp16] F. Sprung, The Iwasawa main conjecture for elliptic curves at odd supersingular primes, https://arxiv.org/abs/1610.10017.

[Va03] V. Vatsal, Special values of anticyclotomic $L$-functions, Duke Mathematical Journal 116 (2003), 219–261.

[vO12] J. Van Order, Some remarks on the two-variable main conjecture of Iwasawa theory for elliptic curves without complex multiplication, Journal of Algebra 350 (2012), 273–299.