ON THE MORDELL-WEIL RANKS OF SUPERSINGULAR ABELIAN VARIETIES IN CYCLOTOMIC EXTENSIONS

ANTONIO LEI AND GAUTIER PONSINET

(Communicated by Romyar T. Sharifi)

ABSTRACT. Let F be a number field unramified at an odd prime p and let F_∞ be the $\mathbf{Z}_p$-cyclotomic extension of F. Let A be an abelian variety defined over F with good supersingular reduction at all primes of F above p. Büyükboduk and the first named author have defined modified Selmer groups associated to A over F_∞. Assuming that the Pontryagin dual of these Selmer groups is a torsion $\mathbf{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$-module, we give an explicit sufficient condition for the rank of the Mordell-Weil group $A(F_n)$ to be bounded as n varies.

Contents

Introduction

Let F be a number field. For an odd prime number p, let $(F_n)_{n \geq 0}$ be the tower of number fields such that $F_\infty = \bigcup_n F_n$ is the $\mathbf{Z}_p$-cyclotomic extension and $\mathrm{Gal}(F_n/F) \simeq \mathbf{Z}/p^n\mathbf{Z}$ (see §1.1).

Let A be an abelian variety defined over F. By Mordell-Weil's theorem, the groups $A(F_n)$ of F_n-rational points of A are finitely generated abelian groups [Mum85, Appendix II]. One may wonder how these groups vary as n varies.

To study the asymptotic growth of their ranks, a strategy (developed by Mazur [Maz72]) goes as follows. One studies the structure as a $\mathbf{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$-module of the Selmer group $\mathrm{Sel}_p(A/F_\infty)$ (see §2.2), as well as its relation to the Selmer groups $\mathrm{Sel}_p(A/F_n)$ over F_n through Galois descent. One then deduces information about the rational points via the exact sequence

$$(1) \qquad 0 \to A(F_n) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to \mathrm{Sel}_p(A/F_n) \to \text{Ш}_p(A/F_n) \to 0,$$

where $\text{Ш}_p(A/F_n)$ is the p-primary component of the Tate-Shafarevitch group of A over F_n.

When A has good ordinary reduction at primes above p, the Pontryagin dual of $\mathrm{Sel}_p(A/F_\infty)$ is conjectured to be a torsion $\mathbf{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$-module (proved by Kato when A is an elliptic curve defined over $\mathbf{Q}$ and $F/\mathbf{Q}$ is an abelian extension). Under this conjecture, Mazur's control theorem on the Selmer groups implies that the rank of the Mordell-Weil group $A(F_n)$ is bounded independently of n.

However, this approach does not work without the ordinarity assumption. First, Mazur's control theorem does not hold. Second, the Pontryagin dual of the Selmer group $\mathrm{Sel}_p(A/F_\infty)$ is no longer expected to be a torsion $\mathbf{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$-module. In the case where A is an elliptic curve with $a_p = 0$ and $F = \mathbf{Q}$, Kobayashi [Kob03] defined two modified Selmer groups (often referred to as plus and minus Selmer groups in the literature) and proved that they do satisfy the two aforementioned properties, namely, the cotorsioness over an appropriate Iwasawa algebra and a control theorem à la Mazur. As a consequence, one deduces that the rank of the Mordell-Weil group $A(F_n)$ is bounded independently of n (see [Kob03, Corollary 10.2]). Alternatively, it is possible to deduce the same result using Kato's Euler system in [Kat04] and Rohrlich's non-vanishing results on the complex L-values of A in [Roh84] (see the discussion after Theorems 1.19 and 1.20 in [Gre01]).

We note that a different approach was developed by Perrin-Riou [PR90, §6] to study the Mordell-Weil ranks of an elliptic curve with supersingular reduction and $a_p = 0$. She showed that when a certain algebraic p-adic L-function is non-zero and does not vanish at the trivial character, then the Mordell-Weil ranks of the elliptic curve over F_n are bounded independently of n. Kim [Kim18] as well as Im and Kim [IK19] have generalized this method to abelian varieties which can have mixed reduction types at primes above p. Furthermore, unlike the present article, they did not assume that p is unramified in F. Following Perrin-Riou's construction, Im and Kim defined certain algebraic p-adic L-functions and showed that when these are non-zero, then the Mordell-Weil ranks of the abelian variety over F_n are bounded by certain explicit polynomials in n.

The goal of the present article is to study the Mordell-Weil ranks of an abelian variety A over F_n under the assumptions that p is unramified in F and that A is supersingular at all primes of F above p. We make use of the signed Selmer groups developed by Büyükboduk and the first named author in [BL17] (see §2.1 for a

review of their constructions; these Selmer groups generalize Kobayashi's plus and minus Selmer groups). Our main result is the following.

Theorem (Theorem 3.4). *Assume that the Pontryagin duals of the signed Selmer groups of A over F_∞ are torsion $\mathbf{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$-modules. There exists an explicit sufficient condition on the Coleman maps attached to A which ensures that the rank of the Mordell-Weil group of the dual abelian variety $A^\vee(F_n)$ is bounded as n varies.*

We show further that when the Frobenius on the Dieudonné module of A at p can be expressed as certain block matrix, then the explicit condition in Theorem 3.4 can be verified (see Corollaries 3.7 and 3.10). We explain at the end of the paper that our result applies to abelian varieties of GL_2-type.

As opposed to the ordinary case, we do not have a direct relation between the signed Selmer groups and the Mordell-Weil group as in the exact sequence (1). However, we may nonetheless obtain information about the Selmer groups $\mathrm{Sel}_p(A/F_n)$ from the signed Selmer groups via the Poitou-Tate exact sequence and some calculations in multi-linear algebra.

1. Supersingular abelian varieties and Coleman maps

In this section, we set some notation and review results of [BL17] that we shall need.

1.1. **Cyclotomic extension and Iwasawa algebra.** Fix forever an odd prime p and a number field F unramified at p. We also fix $\overline{F}$ an algebraic closure of F and let $G_F = \mathrm{Gal}(\overline{F}/F)$ be the absolute Galois group of F. For each prime v of F, we denote by F_v the completion of F at v. Furthermore, we choose an algebraic closure $\overline{F_v}$ of F_v as well as an embedding $\overline{F} \hookrightarrow \overline{F_v}$ and set $G_{F_v} = \mathrm{Gal}(\overline{F_v}/F_v)$ to be the decomposition subgroup of v in G_F. We denote by $\mathcal{O}_F$ the ring of integers of F and by $\mathcal{O}_{F_v}$ the ring of integers of F_v when v is a non-archimedean prime of F.

Let μ_{p^n} be the group of p^n-th roots of unity in $\overline{F}$ for every $n \geq 1$ and $\mu_{p^\infty} = \bigcup_{n \geq 1} \mu_{p^n}$. We set $F(\mu_{p^\infty}) = \bigcup_{n \geq 1} F(\mu_{p^n})$ to be the p^∞-cyclotomic extension of F in $\overline{F}$. We shall write $\mathcal{G}_\infty = \mathrm{Gal}(F(\mu_{p^\infty})/F)$ for its Galois group. The group $\mathcal{G}_\infty$ is isomorphic to $\mathbf{Z}_p^\times$ and so it may be decomposed as $\Delta \times \Gamma$, where Δ is cyclic of order $p - 1$ and $\Gamma \simeq \mathbf{Z}_p$. For $n \geq 0$, we write Γ_n for the unique subgroup of Γ of index p^n. We set $F_\infty = F(\mu_{p^\infty})^\Delta$ to be the $\mathbf{Z}_p$-cyclotomic extension of F, and $F_n = F_\infty^{\Gamma_n}$ for $n \geq 0$.

Let $\Lambda = \mathbf{Z}_p[[\mathcal{G}_\infty]]$ be the Iwasawa algebra of $\mathcal{G}_\infty$ over $\mathbf{Z}_p$. The aforementioned decomposition of $\mathcal{G}_\infty$ tells us that $\Lambda = \mathbf{Z}_p[\Delta][[\Gamma]]$. Furthermore, on fixing a topological generator γ of Γ, we have an isomorphism $\mathbf{Z}_p[[\Gamma]] \simeq \mathbf{Z}_p[[X]]$ induced by $\gamma \mapsto X + 1$. For $n \geq 0$, we denote $\Lambda_n = \Lambda_{\Gamma_n} = \mathbf{Z}_p[\Delta][\Gamma/\Gamma_n]$. The previous isomorphism implies that $\mathbf{Z}_p[\Gamma/\Gamma_n] \simeq \mathbf{Z}_p[[X]]/(\omega_n(X))$, where $\omega_n(X) = (X + 1)^{p^n} - 1$. For a character η on Δ and a Λ-module M, let M^η be the η-isotypic component of M, which is given by $e_\eta \cdot M$, where $e_\eta = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \eta^{-1}(\delta)\delta$. Note that M^η is naturally a $\mathbf{Z}_p[[\Gamma]]$-module. We will say that a Λ-module M has rank r if M^η has rank r over $\mathbf{Z}_p[[\Gamma]]$ for all characters η on Δ.

1.2. **Supersingular abelian varieties.** From now on, we fix a g-dimensional abelian variety A defined over F with good supersingular reduction at every prime v of F dividing p, which means that A has good reduction at v and the slope of the Frobenius acting on the Dieudonné module associated to A at v is constant and equal to $-1/2$ (see §1.4). For all $n \geq 1$, we write $A[p^n]$ for the group of p^n-torsion

points in $A(\overline{F})$ and $A[p^\infty] = \bigcup_n A[p^n]$. Let $T = \varprojlim_{\times p} A[p^n]$ be the p-adic Tate module of A, which is a free $\mathbf{Z}_p$-module of rank $2g$ endowed with a continuous action of G_F and let $V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. For each prime v of F dividing p, V is a crystalline G_{F_v}-representation with Hodge-Tate weights 0 and 1, both with multiplicity g. Finally, we denote by $A^\vee$ the dual abelian variety of A.

Lemma 1.1. *For any prime v of F dividing p and w a prime of $F(\mu_{p^\infty})$ above v, the torsion part of $A(F(\mu_{p^\infty})_w)$ is finite and the group $A(F_{\infty,w})$ has no p-torsion (where we denote again by w the prime of F_∞ below w).*

Proof. The first statement is a theorem of Imai [Ima75].

Let k_{F_v} be the residual field of F_v. By [Maz72, Lemma 5.11], the reduction map induces an isomorphism of the p-torsion points in $A(F_v)$ with the p-torsion points in $A(k_{F_v})$. Since A is supersingular at v, this latter group is trivial. Therefore, $A(F_v)$ has no p-torsion. Furthermore, since $\Gamma_v = \mathrm{Gal}(F_{\infty,w}/F_v) \simeq \mathbf{Z}_p$ is a pro-p group, $A(F_{\infty,w})$ has no p-torsion. $\qquad\square$

1.3. Iwasawa cohomology. Let v be a non-archimedean prime of F and let w be a prime of F_∞ dividing v. We set v_n to be the prime of F_n below w. For $i \geq 0$, the projective limit of the Galois cohomology groups $\mathrm{H}^i(F_{n,v_n}, T)$ relative to the corestriction maps is denoted by $\mathrm{H}^i_{\mathrm{Iw}}(F_v, T)$. The structure of these $\mathbf{Z}_p[[\Gamma]]$-modules is well-known (see [PR00, A.2]).

Proposition 1.2.
  (1) *The groups $\mathrm{H}^i_{\mathrm{Iw}}(F_v, T)$ are finitely generated $\mathbf{Z}_p[[\Gamma]]$-modules, trivial if $i \notin \{1, 2\}$.*
  (2) *$\mathrm{H}^2_{\mathrm{Iw}}(F_v, T)$ is a torsion $\mathbf{Z}_p[[\Gamma]]$-module.*
  (3) *The rank of $\mathrm{H}^1_{\mathrm{Iw}}(F_v, T)$ is given by*

$$\mathrm{rank}_{\mathbf{Z}_p[[\Gamma]]} \mathrm{H}^1_{\mathrm{Iw}}(F_v, T) = \begin{cases} 0 & \text{if } v \nmid p, \\ 2g[F_v : \mathbf{Q}_p] & \text{if } v \mid p. \end{cases}$$

  (4) *The torsion sub-$\mathbf{Z}_p[[\Gamma]]$-module of $\mathrm{H}^1_{\mathrm{Iw}}(F_v, T)$ is isomorphic to $T^{G_{F_\infty}}$.*

1.4. Coleman maps and logarithmic matrices. Let v be a prime of F dividing p. We shall write $f_v = [F_v : \mathbf{Q}_p]$. As a G_{F_v}-representation, T admits a Dieudonné module $\mathbf{D}_{\mathrm{cris},v}(T)$ [Ber04], which is a free $\mathcal{O}_{F_v}$-module of rank $2g$ equipped with a Frobenius after tensoring by $\mathbf{Q}_p$ and a filtration of $\mathcal{O}_{F_v}$-modules $(\mathrm{Fil}^i \mathbf{D}_{\mathrm{cris},v}(T))_{i\in\mathbf{Z}}$ such that

$$\mathrm{Fil}^i \mathbf{D}_{\mathrm{cris},v}(T) = \begin{cases} 0 & \text{for } i \geq 1, \\ \mathbf{D}_{\mathrm{cris},v}(T) & \text{for } i \leq -1. \end{cases}$$

We may choose a $\mathbf{Z}_p$-basis $\{u_1, \ldots, u_{2gf_v}\}$ of $\mathbf{D}_{\mathrm{cris},v}(T)$ such that $\{u_1, \ldots, u_{gf_v}\}$ is a basis for $\mathrm{Fil}^0 \mathbf{D}_{\mathrm{cris},v}(T)$. The matrix of φ with respect to this basis is of the form

$$C_{\varphi,v} = C_v \left(\begin{array}{c|c} I_{gf_v} & 0 \\ \hline 0 & \frac{1}{p} I_{gf_v} \end{array} \right),$$

where I_{gf_v} denotes the identity matrix of dimension gf_v and C_v is some matrix inside $\mathrm{GL}_{2gf_v}(\mathbf{Z}_p)$. As in [BL17, Definition 2.4], we may define for $n \geq 1$,
(2)
$$C_{v,n} = \left(\begin{array}{c|c} I_{gf_v} & 0 \\ \hline 0 & \Phi_{p^n}(1+X) I_{gf_v} \end{array} \right) C_v^{-1} \quad \text{and} \quad M_{v,n} = (C_{\varphi,v})^{n+1} C_{v,n} \cdots C_{v,1},$$

where Φ_{p^n} denotes the p^n-th cyclotomic polynomial.

Let w be a prime of $F(\mu_{p^\infty})$ dividing v. For $i \geq 0$, denote by $\mathrm{H}^i_{\mathrm{Iw,cyc}}(F_v, T)$ the projective limit of $\mathrm{H}^i(F(\mu_{p^n})_{v_n}, T)$ relative to the corestriction maps.

We set $\mathcal{H} = \mathbf{Q}_p[\Delta] \otimes_{\mathbf{Q}_p} \mathcal{H}(\Gamma)$ where $\mathcal{H}(\Gamma)$ is the set of elements $f(\gamma - 1)$ with $\gamma \in \Gamma$ and $f(X) \in \mathbf{Q}_p[[X]]$ is convergent on the p-adic open unit disk. Perrin-Riou's big logarithm map is a Λ-homomorphism [PR94]

$$\mathcal{L}_{T,v} : \mathrm{H}^1_{\mathrm{Iw,cyc}}(F_v, T) \to \mathcal{H} \otimes \mathbf{D}_{\mathrm{cris},v}(T),$$

which interpolates Kato's dual exponential maps [Kat93, II, §1.2]

$$\exp^*_{v,n} : \mathrm{H}^1(F_v(\mu_{p^n}), T) \to F_v(\mu_{p^n}) \otimes \mathrm{Fil}^0 \mathbf{D}_{\mathrm{cris},v}(T).$$

In [BL17, Theorem 1.1], the big logarithm map is decomposed into

$$\mathcal{L}_{T,v} = (u_1, \ldots, u_{2gf_v}) \cdot M_v \cdot \begin{pmatrix} \mathrm{Col}_{T,v,1} \\ \vdots \\ \mathrm{Col}_{T,v,2gf_v} \end{pmatrix},$$

where M_v is a $2gf_v \times 2gf_v$ logarithmic matrix defined over $\mathcal{H}$ given by $\lim_{n\to\infty} M_{v,n}$ and $\mathrm{Col}_{T,v,i}$, $i \in \{1, \ldots, 2gf_v\}$, are Λ-homomorphisms from $\mathrm{H}^1_{\mathrm{Iw,cyc}}(F_v, T)$ to Λ.

If I_v is a subset of $\{1, \ldots, 2gf_v\}$, we set

$$\mathrm{Col}_{T,I_v} : \mathrm{H}^1_{\mathrm{Iw,cyc}}(F_v, T) \to \prod_{k=1}^{|I_v|} \Lambda,$$

$$\mathbf{z} \mapsto (\mathrm{Col}_{T,v,i}(\mathbf{z}))_{i \in I_v}.$$

Let $\underline{I} = (I_v)_{v|p}$ be a tuple of sets indexed by the primes of F dividing p with $I_v \subset \{1, \ldots, 2gf_v\}$. We set $\mathcal{I}$ to be the set of all such tuples such that $\sum_{v|p} |I_v| = g[F : \mathbf{Q}]$. We write $\underline{I}_0 = (I_{v,0})$ where $I_{v,0} = \{1, \ldots, gf_v\}$. Given any $\underline{I} \in \mathcal{I}$ and $\mathbf{z} = z_1 \wedge \cdots \wedge z_{g[F:\mathbf{Q}]} \in \bigwedge^{g[F:\mathbf{Q}]} \prod_{v|p} \mathrm{H}^1_{\mathrm{Iw,cyc}}(F_v, T)$, we define

$$\mathrm{Col}_{T,\underline{I}}(\mathbf{z}) = \det(\mathrm{Col}_{T,v,i}(z_j))_{i \in I_v, 1 \leq j \leq g[F:\mathbf{Q}]}.$$

For all $n \geq 1$, let $H_{v,n} = C_{v,n} \cdots C_{v,1}$, where the matrices $C_{v,i}$ are defined as in (2). Let H_n be the block diagonal matrix where the blocks on the diagonal are given by $H_{v,n}$. Given a pair $\underline{I} = (I_v), \underline{J} = (J_v) \in \mathcal{I}$, we define $H_{\underline{I},\underline{J},n}$ to be the $(\underline{I}, \underline{J})$-minor of $H_{v,n}$.

Proposition 1.3. *Let $\mathbf{z} \in \bigwedge^{g[F:\mathbf{Q}]} \prod_{v|p} \mathrm{H}^1_{\mathrm{Iw,cyc}}(F_v, T)$ and let θ be a character on $\mathcal{G}_\infty$ of conductor p^{n+1}. The natural image of $\mathbf{z}$ in $e_\theta \cdot \bigwedge^{g[F:\mathbf{Q}]} \prod_{v|p} \frac{\mathrm{H}^1(F_v(\mu_{p^{n+1}}), V)}{A(F_v(\mu_{p^{n+1}})) \otimes \mathbf{Q}_p}$ is zero if and only if*

$$\sum_{\underline{J} \in \mathcal{I}} \left(H_{\underline{I}_0, \underline{J}, n} \, \mathrm{Col}_{T,\underline{J}}(\mathbf{z}) \right)(\theta) = 0.$$

Proof. Let us write $\mathbf{z} = z_1 \wedge \cdots \wedge z_{g[F:\mathbf{Q}]}$, $\mathcal{L}_T = \prod_{v|p} \mathcal{L}_{T,v}$, and $\exp^*_{n+1} = \prod_{v|p} \exp^*_{v,n+1}$. Since the image of $A(F_v(\mu_{p^{n+1}})) \otimes \mathbf{Q}_p$ inside $\mathrm{H}^1(F_v(\mu_{p^{n+1}}), V)$ is precisely the kernel of the dual exponential map $\exp^*_{v,n+1}$, the image of $\mathbf{z}$ in

$$e_\theta \cdot \bigwedge^{g[F:\mathbf{Q}]} \prod_{v|p} \frac{\mathrm{H}^1(F_v(\mu_{p^{n+1}}), V)}{A(F_v(\mu_{p^{n+1}})_v) \otimes \mathbf{Q}_p}$$

is zero if and only if

$$e_\theta \cdot \bigwedge_{1 \le j \le g[F:\mathbf{Q}]} \exp_{n+1}^*(z_j) = 0.$$

Via the interpolation formula of Perrin-Riou's big logarithm map (see for example [LZ14, Theorem B.5]), this is equivalent to

$$(3) \qquad \bigwedge_{1 \le j \le g[F:\mathbf{Q}]} (1 \otimes \varphi^{-n-1}) \circ \mathcal{L}_T(z_j)(\theta) = 0.$$

For all $1 \le j \le g[F:\mathbf{Q}]$, we may write $\mathcal{L}_T(z_j) = (\mathcal{L}_{T,v}(z_j))_{v|p}$, where $\mathcal{L}_{T,v}(z_j)$ is understood to be the composition of $\mathcal{L}_{T,v}$ with the projection $\prod_{w|p} \mathrm{H}^1_{\mathrm{Iw,cyc}}(F_w, T) \to \mathrm{H}^1_{\mathrm{Iw,cyc}}(F_v, T)$. Recall from [BL17, Proof of Proposition 2.5] that

$$\mathcal{L}_{T,v}(z_j) \equiv \big(u_1 \cdots u_{2gf_v}\big) \cdot M_{v,n} \cdot \begin{pmatrix} \mathrm{Col}_{T,v,1}(z_j) \\ \vdots \\ \mathrm{Col}_{T,v,2gf_v}(z_j) \end{pmatrix} \quad \bmod \omega_n \mathcal{H} \otimes \mathbf{D}_{\mathrm{cris},v}(T).$$

But the right-hand side is equal to

$$\big(\varphi^{n+1}(u_1) \cdots \varphi^{n+1}(u_{2gf_v})\big) H_{v,n} \begin{pmatrix} \mathrm{Col}_{T,v,1}(z_j) \\ \vdots \\ \mathrm{Col}_{T,v,2gf_v}(z_j) \end{pmatrix},$$

which implies that

$$(1 \otimes \varphi^{-n-1}) \circ \mathcal{L}_{T,v}(z_j)$$
$$\equiv \big(u_1 \cdots u_{2gf_v}\big) \cdot H_{v,n} \cdot \begin{pmatrix} \mathrm{Col}_{T,v,1}(z_j) \\ \vdots \\ \mathrm{Col}_{T,v,2gf_v}(z_j) \end{pmatrix} \quad \bmod \omega_n \mathcal{H} \otimes \mathbf{D}_{\mathrm{cris},v}(T).$$

On taking wedge products, (3) is thus equivalent to the vanishing of

$$\sum_{\underline{I},\underline{J} \in \mathcal{I}} \bigwedge_{i \in I_v} u_i \left(H_{\underline{I},\underline{J},n} \, \mathrm{Col}_{T,\underline{J}}(\mathbf{z}) \right)(\theta).$$

It remains to show that $H_{\underline{I},\underline{J},n}$ vanishes at θ unless $\underline{I} = \underline{I}_0$ and $\underline{J} \in \mathcal{I}$. Indeed, if $i \in \{gf_v+1, \ldots, 2gf_v\}$, the entire i-th row of $C_{v,n}$ is divisible by $\Phi_{p^n}(1+X)$. Hence, the same is true for $H_{v,n}$. In particular, when we evaluate it at θ, the whole row becomes zero. In other words, the lower half of $H_{v,n}(\theta)$ is entirely zero. Therefore, in order for a $g[F:\mathbf{Q}] \times g[F:\mathbf{Q}]$ minor to be non-zero, we must take the upper half of $H_{v,n}$. In other words, $\underline{I} = \underline{I}_0$. □

2. Selmer groups

In this section, we introduce various Selmer groups associated to $A^\vee$, gather some of their properties that we shall need, and finish by using the Poitou-Tate exact sequence to relate them to one another.

2.1. **Signed Selmer groups.** Let v be a prime of F dividing p and w a prime of $F(\mu_{p^\infty})$ above v and fix $\underline{I} = (I_v) \in \mathcal{I}$. We define

$$\mathrm{H}^1_{I_v}(F(\mu_{p^\infty})_w, A^\vee[p^\infty]) \subset \mathrm{H}^1(F(\mu_{p^\infty})_w, A^\vee[p^\infty])$$

to be the orthogonal complement of $\mathrm{Ker}\,\mathrm{Col}_{T, I_v}$ under Tate's local pairing

$$\mathrm{H}^1(F(\mu_{p^\infty})_w, A^\vee[p^\infty]) \times \mathrm{H}^1_{\mathrm{Iw,cyc}}(F_v, T) \to \mathbf{Q}_p/\mathbf{Z}_p.$$

Since $A^\vee[p^\infty](F(\mu_{p^\infty})_w)$ is a finite p-group by Lemma 1.1 and the order of Δ is $p - 1$, the groups $\mathrm{H}^1(\Delta, A^\vee[p^\infty](F(\mu_{p^\infty})_w))$ and $\mathrm{H}^2(\Delta, A^\vee[p^\infty](F(\mu_{p^\infty})_w))$ are trivial. Therefore, by the inflation-restriction exact sequence, the restriction map

$$\mathrm{H}^1(F_{\infty,w}, A^\vee[p^\infty]) \to \mathrm{H}^1(F(\mu_{p^\infty})_w, A^\vee[p^\infty])^\Delta$$

is an isomorphism. We use this isomorphism to define $\mathrm{H}^1_{I_v}(F_{\infty,w}, A^\vee[p^\infty]) \subset \mathrm{H}^1(F_{\infty,w}, A^\vee[p^\infty])$ by

$$\mathrm{H}^1_{I_v}(F_{\infty,w}, A^\vee[p^\infty]) = \mathrm{H}^1_{I_v}(F(\mu_{p^\infty})_w, A^\vee[p^\infty])^\Delta.$$

The $\underline{I}$-Selmer group of $A^\vee$ over F_∞ is then defined by

$$\mathrm{Sel}_{\underline{I}}(A^\vee/F_\infty)$$

$$= \mathrm{Ker}\left(\mathrm{H}^1(F_\infty, A^\vee[p^\infty]) \to \prod_{w \nmid p} \mathrm{H}^1(F_{\infty,w}, A^\vee[p^\infty]) \times \prod_{w | p} \frac{\mathrm{H}^1(F_{\infty,w}, A^\vee[p^\infty])}{\mathrm{H}^1_{I_v}(F_{\infty,w}, A^\vee[p^\infty])} \right).$$

Remark 2.1. When $F = \mathbf{Q}$ and A is an elliptic curve with $a_p = 0$, for an appropriate choice of basis for the Dieudonné module of T, the signed Selmer groups coincide with Kobayashi [Kob03] plus and minus Selmer groups. See [BL17, Appendix 4].

We denote by $\mathcal{X}_{\underline{I}}(A^\vee/F_\infty)$ the Pontryagin dual of $\mathrm{Sel}_{\underline{I}}(A^\vee/F_\infty)$. As in [Kob03], we have the following conjecture.

Conjecture 2.2. *For all $\underline{I} \in \mathcal{I}$, the $\mathbf{Z}_p[[\Gamma]]$-module $\mathcal{X}_{\underline{I}}(A^\vee/F_\infty)$ is torsion.*

When A is an elliptic curve defined over $\mathbf{Q}$, Conjecture 2.2 is known to be true (cf. [Kob03, Spr12]). See also [LLZ10], where a similar conjecture has been proved for modular forms.

2.2. **p-Selmer groups.** The p-Selmer group of $A^\vee$ over an algebraic extension K of F is defined by

$$\mathrm{Sel}_p(A^\vee/K) = \mathrm{Ker}\left(\mathrm{H}^1(K, A^\vee[p^\infty]) \to \prod_v \frac{\mathrm{H}^1(K_v, A^\vee[p^\infty])}{A^\vee(K_v) \otimes \mathbf{Q}_p/\mathbf{Z}_p} \right),$$

where the injection $A^\vee(K_v) \otimes \mathbf{Q}_p/\mathbf{Z}_p \hookrightarrow \mathrm{H}^1(K_v, A^\vee[p^\infty])$ is the Kummer map. Note that $A^\vee(K_v) \otimes \mathbf{Q}_p/\mathbf{Z}_p = 0$ when v does not divide p. Furthermore, the orthogonal complement of $A^\vee(K_v) \otimes \mathbf{Q}_p/\mathbf{Z}_p$ under Tate's local pairing

$$\mathrm{H}^1(K_v, A^\vee[p^\infty]) \times \mathrm{H}^1(K_v, T) \to \mathbf{Q}_p/\mathbf{Z}_p$$

is $A(K_v) \otimes \mathbf{Z}_p$. The p-Selmer group then fits into a short exact sequence

$$(4) \qquad 0 \to A^\vee(K) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to \mathrm{Sel}_p(A^\vee/K) \to \text{Ш}(A^\vee/K)[p^\infty] \to 0,$$

where $\text{Ш}(A^\vee/K)$ is the Tate-Shafarevich group of $A^\vee$ over K. We denote by $\mathcal{X}_p(A^\vee/K)$ the Pontryagin dual of $\mathrm{Sel}_{\underline{I}}(A^\vee/K)$.

2.3. **Fine Selmer groups.** The fine Selmer group of $A^\vee$ over an algebraic extension K of F is defined by

$$\mathrm{Sel}_0(A^\vee/K) = \mathrm{Ker}\left(\mathrm{H}^1(K, A^\vee[p^\infty]) \to \prod_v \mathrm{H}^1(K_v, A^\vee[p^\infty])\right).$$

We denote by $\mathcal{X}_0(A^\vee/K)$ its Pontryagin dual.

One has a "control theorem" for the fine Selmer groups in the cyclotomic extension, which we prove following closely Greenberg [Gre99, §3] and [Gre03].

Lemma 2.3. *The kernel and cokernel of the restriction map*

$$\mathrm{Sel}_0(A^\vee/F_n) \to \mathrm{Sel}_0(A^\vee/F_\infty)^{\Gamma_n}$$

are finite and have bounded orders as n varies.

Proof. The diagram

(5)
$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_0(A^\vee/F_n) & \longrightarrow & \mathrm{H}^1(F_n, A^\vee[p^\infty]) & \longrightarrow & \prod_{v_n} \mathrm{H}^1(F_{n,v_n}, A^\vee[p^\infty]) \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Sel}_0(A^\vee/F_\infty)^{\Gamma_n} & \longrightarrow & \mathrm{H}^1(F_\infty, A^\vee[p^\infty])^{\Gamma_n} & \longrightarrow & \prod_w \mathrm{H}^1(F_{\infty,w}, A^\vee[p^\infty])^{\Gamma_n}
\end{array}$$

is commutative.

One has the inflation-restriction exact sequence

$$0 \to \mathrm{H}^1(\Gamma_n, A^\vee(F_\infty)[p^\infty]) \to \mathrm{H}^1(F_n, A^\vee[p^\infty]) \to \mathrm{H}^1(F_\infty, A^\vee[p^\infty])^{\Gamma_n}$$
$$\to \mathrm{H}^2(\Gamma_n, A^\vee(F_\infty)[p^\infty]).$$

By Lemma 1.1, the groups $\mathrm{H}^1(\Gamma_n, A^\vee(F_\infty)[p^\infty])$ and $\mathrm{H}^2(\Gamma_n, A^\vee(F_\infty)[p^\infty])$ are trivial. Thus, the central vertical map of the diagram is an isomorphism.

We now study the rightmost vertical map prime by prime. Let v be any prime of F and let v_n be any prime of F_n above v. Let r_n be the restriction map

$$\mathrm{H}^1(F_{n,v_n}, A^\vee[p^\infty]) \to \mathrm{H}^1(F_{\infty,w}, A^\vee[p^\infty]),$$

where w is any prime of F_∞ dividing v_n. If v is archimedean, then v splits completely in F_∞/F. Thus, $\mathrm{Ker}(r_n) = 0$. If v is a non-archimedean prime, by the inflation-restriction exact sequence

$$\mathrm{Ker}(r_n) \simeq \mathrm{H}^1(\Gamma_{v_n}, A^\vee(F_{\infty,w})[p^\infty]).$$

By Lemma 1.1, if v divides p, this last group is trivial. We assume that v does not divide p. Then v is unramified and finitely decomposed in F_∞. Thus, $F_{\infty,w}/F_v$ is an unramified $\mathbf{Z}_p$-extension. Let γ_{v_n} be a topological generator of Γ_{v_n}. Then

$$\mathrm{Ker}(r_n) \simeq \mathrm{H}^1(\Gamma_{v_n}, A^\vee(F_{\infty,w})[p^\infty]) \simeq A^\vee(F_{\infty,w})[p^\infty]/(\gamma_{v_n}-1)A^\vee(F_{\infty,w})[p^\infty].$$

As a group $A^\vee(F_{\infty,w})[p^\infty] \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^t \times (\text{a finite group})$ for some $0 \leq t \leq 2g$. Since $A^\vee(F_{n,v_n})$ is finitely generated, the kernel of $(\gamma_{v_n}-1)$ acting on $A^\vee(F_{\infty,w})[p^\infty]$ is finite. Thus, the restriction of $(\gamma_{v_n}-1)$ on the maximal divisible subgroup, which we write $(A^\vee(F_{\infty,w})[p^\infty])_{\mathrm{div}}$, is surjective and we have

$$(A^\vee(F_{\infty,w})[p^\infty])_{\mathrm{div}} \subset (\gamma_{v_n}-1)A^\vee(F_{\infty,w})[p^\infty].$$

Therefore, the cardinality of $\mathrm{Ker}(r_n)$ is bounded by

$$[A^\vee(F_{\infty,w})[p^\infty] : (A^\vee(F_{\infty,w})[p^\infty])_{\mathrm{div}}],$$

which is independent of n. Furthermore, if $A^\vee$ has good reduction at v, then the inertia subgroup of G_{F_v} acts trivially and $A^\vee(F_{\infty,w})[p^\infty]$ is divisible. Hence, $\mathrm{Ker}(r_n)$ is trivial.

Now the set of non-archimedean primes of F where $A^\vee$ has bad reduction is finite, and for each of these primes, the order of $\mathrm{Ker}(r_n)$ is bounded as n varies and the number of primes v_n of F_n dividing v is also bounded. Hence, the order of the kernel of the right-most vertical map in the diagram is bounded as n varies.

We conclude by applying the snake lemma to the diagram (5). $\square$

2.4. **Poitou-Tate exact sequences.** Let Σ be a finite set of primes of F containing the primes dividing p, the archimedean primes, and the primes of bad reduction of $A^\vee$. If K is an extension of F, we say by abuse that a prime of K is in Σ if it divides an element of Σ and we denote by K_Σ the maximal extension of K unramified outside Σ. The cyclotomic extension $F(\mu_{p^\infty})$ is contained in F_Σ since only archimedean primes and primes dividing p can ramify in $F(\mu_{p^\infty})$. Furthermore, the action of G_F on $A^\vee[p^\infty]$ factorizes through $\mathrm{Gal}(F_\Sigma/F)$. In particular, for F' any extension of F contained in F_∞ and $* \in \{p, 0, \underline{I}\}$, we have that $\mathrm{Sel}_*(A^\vee/F') \subset \mathrm{H}^1(F_\Sigma/F', A^\vee[p^\infty])$. Therefore, all the Pontryagin duals $\mathcal{X}_*(A^\vee[p^\infty]/F_\infty)$ are finitely generated $\mathbf{Z}_p[[\Gamma]]$-modules (see [Gre89]).

For $i \geq 0$, let $\mathrm{H}^i_{\mathrm{Iw},\Sigma}(F,T)$ be the projective limit of the groups $\mathrm{H}^i(F_\Sigma/F_n,T)$ relative to the corestriction maps. By [PR00, Proposition A.3.2], we have the exact sequences

$$(6) \qquad 0 \to \mathcal{X}_0(A^\vee/F_\infty) \to \mathrm{H}^2_{\mathrm{Iw},\Sigma}(F,T) \to \prod_{w \in \Sigma} \mathrm{H}^2_{\mathrm{Iw}}(F_v,T),$$

$$(7) \qquad \mathrm{H}^1_{\mathrm{Iw},\Sigma}(F,T) \to \prod_{w \in \Sigma} \frac{\mathrm{H}^1_{\mathrm{Iw}}(F_v,T)}{\mathrm{Ker}\,\mathrm{Col}_{I_v}} \to \mathcal{X}_{\underline{I}}(A^\vee/F_\infty) \to \mathcal{X}_0(A^\vee/F_\infty) \to 0,$$

and, for any $n \geq 0$,

$$(8) \qquad \mathrm{H}^1(F_{n,\Sigma},T) \to \prod_{v|p} \frac{\mathrm{H}^1(F_{n,v},T)}{A(F_{n,v}) \otimes \mathbf{Z}_p} \to \mathcal{X}_p(A^\vee/F_n) \to \mathcal{X}_0(A^\vee/F_n) \to 0.$$

Lemma 2.4. *Assume that Conjecture* 2.2 *holds. Then*
- (1) $\mathcal{X}_0(A^\vee/F_\infty)$ *is a torsion* $\mathbf{Z}_p[[\Gamma]]$-*module,*
- (2) $\mathrm{H}^2_{\mathrm{Iw},\Sigma}(F,T)$ *is a torsion* $\mathbf{Z}_p[[\Gamma]]$-*module,*
- (3) $\mathrm{H}^1_{\mathrm{Iw},\Sigma}(F,T)$ *is a* $\mathbf{Z}_p[[\Gamma]]$-*module of rank* $g[F:\mathbf{Q}]$.

Proof. The exact sequence (7) tells us that Conjecture 2.2 implies (1).

By Proposition 1.2, for every $w \in \Sigma$, $\mathrm{H}^2_{\mathrm{Iw}}(F_v,T)$ is a torsion $\mathbf{Z}_p[[\Gamma]]$-module. Hence, using the exact sequence (6), the first statement of the lemma implies the second.

Finally, thanks to [PR00, Proposition 1.3.2(i) $\Rightarrow$ (ii)], we conclude that (2) implies (3). $\square$

3. GROWTH OF RANKS

3.1. **Bounding Mordell-Weil ranks using logarithmic matrices.** We define

$$\mathcal{X}_{\mathrm{loc}}(F_n) = \mathrm{Coker}\left(\mathrm{H}^1_{\mathrm{Iw},\Sigma}(F,T) \to \prod_{v|p} \frac{\mathrm{H}^1(F_{n,v},T)}{A(F_{n,v}) \otimes \mathbf{Z}_p}\right).$$

Lemma 3.1. *For $n \gg 0$,*

$$\operatorname{rank}_{\mathbf{Z}_p} \mathcal{X}_{\operatorname{loc}}(F_n) = \operatorname{rank}_{\mathbf{Z}_p} \mathcal{X}_p(A^\vee/F_n) + O(1).$$

Proof. By Lemma 2.3,

$$\operatorname{rank}_{\mathbf{Z}_p} \mathcal{X}_0(A^\vee/F_n) = \operatorname{rank}_{\mathbf{Z}_p} \mathcal{X}_0(A^\vee/F_\infty)_{\Gamma_n}.$$

Since Lemma 2.4(1) says that $\mathcal{X}_0(A^\vee/F_\infty)$ is $\mathbf{Z}_p[[\Gamma]]$-torsion, we have

$$\operatorname{rank}_{\mathbf{Z}_p} \mathcal{X}_0(A^\vee/F_\infty)_{\Gamma_n} = O(1)$$

for $n \gg 0$. Hence, the lemma follows from (8). $\qquad\square$

Therefore, in order to bound the Mordell-Weil rank of $A^\vee(F_n)$, it is enough to bound $\operatorname{rank}_{\mathbf{Z}_p} \mathcal{X}_{\operatorname{loc}}(F_n)$ thanks to (4). We explain below how we may obtain a bound on $\operatorname{rank}_{\mathbf{Z}_p} \mathcal{X}_{\operatorname{loc}}(F_n)$ using the logarithmic matrices we studied in §1.4.

From now on, we fix a family of classes $c_1, c_2, \ldots, c_{g[F:\mathbf{Q}]} \in \mathrm{H}^1_{\mathrm{Iw},\Sigma}(F, T)$ such that $\mathrm{H}^1_{\mathrm{Iw},\Sigma}(F, T)/\langle c_1, \ldots, c_{g[F:\mathbf{Q}]}\rangle$ is $\mathbf{Z}_p[[\Gamma]]$-torsion (their existence is guaranteed by Lemma 2.4(3)).

The composition

$$\mathrm{H}^1_{\mathrm{Iw},\Sigma}(F, T) \xrightarrow{(\operatorname{loc}_v)_v} \prod_{v|p} \mathrm{H}^1_{\mathrm{Iw},\operatorname{cyc}}(F_v, T) \xrightarrow{(\operatorname{Col}_{T,J_v})_v} \prod_{k=1}^{g[F:\mathbf{Q}]} \Lambda$$

is a Λ-homomorphism between two Λ-modules of rank $g[F : \mathbf{Q}]$. Let us write

$$\operatorname{Col}_{T,\underline{J}}(\mathbf{c}) = \det\left(\operatorname{Col}_{T,J_v} \circ \operatorname{loc}_v(c_i)\right)_{v|p, 1 \le i \le g[F:\mathbf{Q}]}.$$

Lemma 3.2. *Let $\underline{J} \in \mathcal{I}$. Suppose that the Selmer group $\operatorname{Sel}_{\underline{J}}(A^\vee/F_\infty)$ is $\mathbf{Z}_p[[\Gamma]]$-cotorsion. Then, $\operatorname{Col}_{T,\underline{J}}(\mathbf{c}) \ne 0$.*

Proof. Recall from Lemma 2.4(1) that $\mathcal{X}_0(A^\vee/F_\infty)$ is $\mathbf{Z}_p[[\Gamma]]$-torsion. By assumption, $\mathcal{X}_{\underline{J}}(A^\vee/F_\infty)$ is also $\mathbf{Z}_p[[\Gamma]]$-torsion. Therefore, our result follows from (7). $\quad\square$

Proposition 3.3. *Let θ a character on Γ of conductor p^{n+1} which is trivial on Δ. Then, $e_\theta \cdot \mathcal{X}_{\operatorname{loc}}(F_n) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p = 0$ if*

$$\sum_{\underline{J} \in \mathcal{I}} \left(H_{\underline{I}_0, \underline{J}, n} \operatorname{Col}_{T,\underline{J}}(\mathbf{c})\right)(\theta) \ne 0.$$

Proof. Note that

$$\frac{\mathrm{H}^1(F_v(\mu_{p^{n+1}}), V)}{A(F_v(\mu_{p^{n+1}})) \otimes \mathbf{Q}_p} \cong F_v[\operatorname{Gal}(F_v(\mu_{p^{n+1}})/F_v)]^{\oplus g} \cong \mathbf{Q}_p[\operatorname{Gal}(F_v(\mu_{p^{n+1}})/F_v)]^{\oplus g f_v}$$

as Γ-modules via the Bloch-Kato dual exponential map. Thus,

$$\bigwedge^{g[F:\mathbf{Q}]} \left(\prod_{v|p} \frac{\mathrm{H}^1(F_v(\mu_{p^{n+1}}), V)}{A(F_v(\mu_{p^{n+1}})) \otimes \mathbf{Q}_p}\right) \cong \mathbf{Q}_p[\operatorname{Gal}(F(\mu_{p^{n+1}})/F)].$$

In particular,

$$e_\theta \cdot \bigwedge^{g[F:\mathbf{Q}]} \left(\prod_{v|p} \frac{\mathrm{H}^1(F_v(\mu_{p^{n+1}}), V)}{A(F_v(\mu_{p^{n+1}})) \otimes \mathbf{Q}_p}\right) = e_\theta \cdot \bigwedge^{g[F:\mathbf{Q}]} \left(\prod_{v|p} \frac{\mathrm{H}^1(F_{n,v}, V)}{A(F_{n,v}) \otimes \mathbf{Q}_p}\right)$$

is a one-dimensional $\mathbf{Q}_p(\theta)$-vector space. By Proposition 1.3, our hypothesis on $\bigwedge c_i$ tells us that its image in this vector space is non-zero. Therefore, the e_θ-component of the cokernel of

$$\bigwedge^{g[F:\mathbf{Q}]} \mathrm{H}^1_{\mathrm{Iw},\Sigma}(F,T) \otimes \mathbf{Q}_p \to \bigwedge^{g[F:\mathbf{Q}]} \prod_{v\mid p} \frac{\mathrm{H}^1(F_{n,v},V)}{A(F_{n,v}) \otimes \mathbf{Q}_p}$$

is zero. Hence the result. $\qquad\square$

Theorem 3.4. *Let θ be a character as in the statement of Proposition 3.3. Suppose that*

$$(9) \qquad \sum_{\underline{J}} \left(H_{\underline{L_0},\underline{J},n} \operatorname{Col}_{T,\underline{J}}(\mathbf{c}) \right)(\theta) \neq 0$$

for $n \gg 0$. Then

$$\operatorname{rank}_{\mathbf{Z}_p} A^\vee(F_n) = O(1).$$

Proof. Proposition 3.3 says that $e_\theta \cdot \mathcal{X}_{\mathrm{loc}}(F_n) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p = 0$ for $n \gg 0$. But

$$\operatorname{rank}_{\mathbf{Z}_p} \mathcal{X}_{\mathrm{loc}}(F_n) - \operatorname{rank}_{\mathbf{Z}_p} \mathcal{X}_{\mathrm{loc}}(F_{n-1}) = \dim_{\mathbf{Q}_p} e_\theta \cdot \mathcal{X}_{\mathrm{loc}}(F_n) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p,$$

where θ is any character of Γ of conductor p^{n+1}. In particular, $\operatorname{rank}_{\mathbf{Z}_p} \mathcal{X}_{\mathrm{loc}}(F_n) = O(1)$. Lemma 3.1 now implies that $\operatorname{rank}_{\mathbf{Z}_p} \mathcal{X}_p(A^\vee/F_n) = O(1)$, and our theorem follows from (4). $\qquad\square$

In other words, the key to showing that the Mordell-Weil ranks of $A^\vee$ are bounded inside F_∞ is to establish (9).

3.2. Special cases.

If Conjecture 2.2 holds, Lemma 3.2 tells us that $\operatorname{Col}_{T,\underline{J}}(\mathbf{c})(\theta) \neq 0$ if θ is a character whose conductor is sufficiently large. However, this is not enough to verify (9) since we do not have an explicit description of $H_{\underline{L_0},\underline{J},n}$ in the most general setting. In this section, we will show that when the matrices $C_{\varphi,v}$ are explicit enough, it is possible to establish (9) by calculating the p-adic valuations of $H_{\underline{L_0},\underline{J},n}(\theta)$.

3.2.1. *Block anti-diagonal matrices.*

We suppose in this section that for each v, we may find a basis of $\mathbf{D}_{\mathrm{cris},v}(T)$ such that the matrix C_v is of the form $\left(\begin{array}{c|c} 0 & * \\ \hline * & 0 \end{array} \right)$, where $*$ represents a $gf_v \times gf_v$ matrix defined over $\mathbf{Z}_p$. This is the same as saying that $\varphi(v_i) \notin \mathrm{Fil}^0 \mathbf{D}_{\mathrm{cris},v}(T)$ and $\varphi^2(v_i) \in \mathrm{Fil}^0 \mathbf{D}_{\mathrm{cris},v}(T)$ for all $i \in \{1,\ldots,gf_v\}$. It can be thought of as the analogue of $a_p = 0$ for supersingular elliptic curves. In particular,

$$(10) \qquad C_{v,n} = \left(\begin{array}{c|c} 0 & B_{v,1} \\ \hline \Phi_{p^n}(1+X)B_{v,2} & 0 \end{array} \right)$$

for some invertible $gf_v \times gf_v$ matrices $B_{v,1}$ and $B_{v,2}$ that are defined over $\mathbf{Z}_p$ with $\det(B_{v,1}B_{v,2}) = 1$ (since $\det C_{\varphi,v} = p^{-gf_v}$). For all $n \geq 1$, we fix a primitive p^n-th root of unity ζ_{p^n} and we write $\varepsilon_n = \zeta_{p^n} - 1$.

Lemma 3.5. *Suppose that C_v is block anti-diagonal for all v. Then, for all $n \geq 1$, we have*

$$H_{v,n}(\zeta_{p^n} - 1) = \begin{cases} \left(\begin{array}{c|c} 0 & \delta_n(B_{v,1}B_{v,2})^{(n-1)/2}B_{v,1} \\ \hline 0 & 0 \end{array} \right) & \text{if } n \text{ odd,} \\[12pt] \left(\begin{array}{c|c} \delta_n(B_{v,1}B_{v,2})^{n/2} & 0 \\ \hline 0 & 0 \end{array} \right) & \text{if } n \text{ even.} \end{cases}$$

Here, the constant δ_n is given by

$$\delta_n = \begin{cases} \frac{\varepsilon_1}{\varepsilon_2} \cdot \frac{\varepsilon_3}{\varepsilon_4} \cdots \frac{\varepsilon_{n-2}}{\varepsilon_{n-1}} & \text{if } n \text{ odd,} \\[6pt] \frac{\varepsilon_1}{\varepsilon_2} \cdot \frac{\varepsilon_3}{\varepsilon_4} \cdots \frac{\varepsilon_{n-1}}{\varepsilon_n} & \text{if } n \text{ even.} \end{cases}$$

Proof. Thanks to (10), we have explicitly

$H_{v,n}(\varepsilon_n)$

$$= \left(\begin{array}{c|c} 0 & B_{v,1} \\ \hline 0 & 0 \end{array} \right) \cdot \left(\begin{array}{c|c} 0 & B_{v,1} \\ \hline \frac{\varepsilon_1}{\varepsilon_2}B_{v,2} & 0 \end{array} \right) \cdot \left(\begin{array}{c|c} 0 & B_{v,1} \\ \hline \frac{\varepsilon_2}{\varepsilon_3}B_{v,2} & 0 \end{array} \right) \cdots \left(\begin{array}{c|c} 0 & B_{v,1} \\ \hline \frac{\varepsilon_{n-1}}{\varepsilon_n}B_{v,2} & 0 \end{array} \right).$$

Hence the result on multiplying out these matrices. $\square$

Recall that $\underline{I}_0 = (I_{v,0})_{v|p}$, where $I_{v,0} = \{1, \ldots, gf_v\}$. Let $\underline{I}_1$ be the complement of $\underline{I}_0$; that is, $\underline{I}_1 = (I_{v,1})_{v|p}$, where $I_{v,1} = \{gf_v + 1, \ldots, 2gf_v\}$.

Lemma 3.6. *Suppose that C_v is block anti-diagonal for all v and that the Selmer groups $\mathrm{Sel}_{\underline{I}_0}(A/F_\infty)$ and $\mathrm{Sel}_{\underline{I}_1}(A/F_\infty)$ are both $\mathbf{Z}_p[[\Gamma]]$-cotorsion. Then, (9) holds whenever n is sufficiently large.*

Proof. Suppose that θ sends the fixed topological generator to ζ_{p^n}. By Lemma 3.5,

$$H_{\underline{I}_0, \underline{J}, n}(\theta) = 0$$

unless $\underline{J} = \underline{I}_0$ and n is even or $\underline{J} = \underline{I}_1$ and n is odd. Let us write $\underline{J}_n = \underline{I}_{\frac{1-(-1)^n}{2}}$. Then, the left-hand side of (9) is equal to

$$\left(H_{\underline{I}_0, \underline{J}_n, n} \mathrm{Col}_{T, \underline{J}_n}(\mathbf{c}) \right)(\theta).$$

Lemma 3.5 says that $H_{\underline{I}_0, \underline{J}_n, n}(\theta)$ is never zero. Our hypothesis on the $\underline{J}_n$-Selmer group and Lemma 3.2 tell us that $\left(\mathrm{Col}_{T, \underline{J}_n}(\mathbf{c}) \right)(\theta) \neq 0$ when n is sufficiently large. Hence the result follows. $\square$

If we combine this with Theorem 3.4, we deduce our first result on the Mordell-Weil ranks of $A^\vee$.

Corollary 3.7. *Suppose that C_v is block anti-diagonal for all v and that the Selmer groups $\mathrm{Sel}_{\underline{I}_0}(A/F_\infty)$ and $\mathrm{Sel}_{\underline{I}_1}(A/F_\infty)$ are both $\mathbf{Z}_p[[\Gamma]]$-cotorsion. Then,*

$$\mathrm{rank}_{\mathbf{Z}_p} A^\vee(F_n) = O(1).$$

3.2.2. *Block anti-diagonal modulo p matrices.* We suppose in this section that for each v, we may find a basis of $\mathbf{D}_{\mathrm{cris},v}(T)$ such that the matrix C_v is of the form

$$C_v = \left(\begin{array}{c|c} pA_{v,1} & B_{v,1} \\ \hline B_{v,2} & pA_{v,2} \end{array} \right),$$

where $A_{v,1}, A_{v,2}, B_{v,1}$ $B_{v,2}$ are some $gf_v \times gf_v$ matrices over $\mathbf{Z}_p$ with $\det(B_{v,1})$, $\det(B_{v,2}) \in \mathbf{Z}_p^\times$. In other words, C_v is congruent to a block anti-diagonal matrix modulo p. Note that in the case of elliptic curves, given a basis of v_1 of

$\mathrm{Fil}^0 \mathbf{D}_{\mathrm{cris},v}(T)$, the pair $v_1, \varphi(v_1)$ forms a basis of $\mathbf{D}_{\mathrm{cris},v}(T)$ by Fontaine-Laffaille theory. The matrix of φ is given by $\begin{pmatrix} 0 & -\frac{1}{p} \\ 1 & \frac{a_p}{p} \end{pmatrix}$. Thus, $C_v = \begin{pmatrix} 0 & -1 \\ 1 & a_p \end{pmatrix}$ is a block anti-diagonal matrix mod p whenever $p|a_p$. We shall discuss in this next section that the same holds for abelian varieties of GL_2-type in the next section.

From now on, for each prime v, ord_p denotes the normalized p-adic valuation on $\overline{F_v}$ with $\mathrm{ord}_p(p) = 1$. Recall from the previous section that $\underline{J}_n = \underline{I}_{\frac{1-(-1)^n}{2}}$.

Lemma 3.8. *Suppose that C_v is block anti-diagonal mod p for all v. Then,*

$$\mathrm{ord}_p\left(H_{\underline{I}_0,\underline{J},n}(\zeta_{p^n} - 1)\right) - \mathrm{ord}_p\left(H_{\underline{I}_0,\underline{J}_n,n}(\zeta_{p^n} - 1)\right) \geq 1 - \frac{1}{p^2 - 1}$$

for all $\underline{J} \neq \underline{J}_n$ and $n \geq 1$.

Proof. By the calculations of Lemma 3.5,

$$H_{v,n}(\zeta_{p^n} - 1) = \begin{cases} \left(\begin{array}{c|c} O(p) & \delta_n(B_{v,1}B_{v,2})^{(n-1)/2}B_{v,1} + O(p) \\ \hline 0 & 0 \end{array} \right) & \text{if } n \text{ odd,} \\ \left(\begin{array}{c|c} \delta_n(B_{v,1}B_{v,2})^{n/2} + O(p) & O(p) \\ \hline 0 & 0 \end{array} \right) & \text{if } n \text{ even.} \end{cases}$$

Here, $O(p)$ denotes a matrix whose entries all have p-adic valuation ≥ 1. The explicit formula of δ_n is given by

$$\mathrm{ord}_p(\delta_n) < \frac{1}{p^2} + \frac{1}{p^4} + \cdots = \frac{1}{p^2 - 1} < 1.$$

Therefore,

$$H_{\underline{I}_0,\underline{J}_n,n}(\zeta_{p^n} - 1) = \det(\delta_n \star),$$

where $\star$ is a matrix given by a product of $B_{v,1}$ and $B_{v,2}$. But the determinants of these matrices are p-adic units, so

$$\mathrm{ord}_p\left(H_{\underline{I}_0,\underline{J}_n,n}(\zeta_{p^n} - 1)\right) = g[F : \mathbf{Q}] \mathrm{ord}_p(\delta_n).$$

If $\underline{J} \neq \underline{J}_n$, then there is at least one v where the $(I_{v,0}, J_v)$-minor contains a column whose entries all have p-adic valuation ≥ 1. In the other columns, the entries all have p-adic valuation $\geq \mathrm{ord}_p(\delta_n)$. Therefore,

$$\mathrm{ord}_p\left(H_{\underline{I}_0,\underline{J},n}(\zeta_{p^n} - 1)\right) \geq 1 + (g[F : \mathbf{Q}] - 1)\mathrm{ord}_p(\delta_n).$$

Hence,

$$\mathrm{ord}_p\left(H_{\underline{I}_0,\underline{J},n}(\zeta_{p^n} - 1)\right) - \mathrm{ord}_p\left(H_{\underline{I}_0,\underline{J}_n,n}(\zeta_{p^n} - 1)\right) \geq 1 - \mathrm{ord}_p(\delta_n) > 1 - \frac{1}{p^2 - 1},$$

as required. $\square$

Lemma 3.9. *Suppose that C_v is block anti-diagonal mod p for all v and that $\mathrm{Col}_{T,\underline{I}_0}(\mathbf{c})$ and $\mathrm{Col}_{T,\underline{I}_1}(\mathbf{c})$ are both non-zero. Furthermore, suppose that for all $\underline{J}$ such that $\mathrm{Col}_{T,\underline{J}}(\mathbf{c}) \neq 0$, the μ-invariant of $\mathrm{Col}_{T,\underline{J}}(\mathbf{c})$ is independent of $\underline{J}$. Then (9) holds for $n \gg 0$.*

Proof. Let μ be the common μ-invariant among the non-zero $\mathrm{Col}_{T,\underline{J}}(\mathbf{c})$ and write $\lambda_{\underline{J}}$ for the λ-invariant of $\mathrm{Col}_{T,\underline{J}}(\mathbf{c})$. For $n \gg 0$, by Weierstrass' preparation theorem [Was97, Theorem 7.3],

$$\mathrm{ord}_p\left(\mathrm{Col}_{T,\underline{J}}(\mathbf{c})(\zeta_{p^n}-1)\right) = \mu + \frac{\lambda_{\underline{J}}}{p^n - p^{n-1}}.$$

Note that $\frac{\lambda_{\underline{J}}}{p^n - p^{n-1}}$ becomes arbitrarily small as $n \to \infty$. Therefore, on combining this with Lemma 3.8, we deduce that

$$0 \neq \mathrm{ord}_p\left(H_{\underline{I}_0,\underline{J}_n,n}\,\mathrm{Col}_{T,\underline{J}_n}(\mathbf{c})(\zeta_{p^n}-1)\right) < \mathrm{ord}_p\left(H_{\underline{I}_0,\underline{J},n}\,\mathrm{Col}_{T,\underline{J}}(\mathbf{c})(\zeta_{p^n}-1)\right)$$

for all $\underline{J} \neq \underline{J}_n$ and $n \gg 0$. Hence (9) holds. $\square$

Corollary 3.10. *Suppose that C_v is block anti-diagonal mod p for all v and that $\mathrm{Sel}_{\underline{I}_0}(A/F_\infty)$ and $\mathrm{Sel}_{\underline{I}_1}(A/F_\infty)$ are both $\mathbf{Z}_p[[\Gamma]]$-cotorsion. Furthermore, suppose that for all $\underline{J}$ such that $\mathrm{Sel}_{\underline{J}}(A/F_\infty)$ is $\mathbf{Z}_p[[\Gamma]]$-cotorsion, the μ-invariant of $\mathrm{Sel}_{\underline{J}}(A/F_\infty)^\vee$ is independent of $\underline{J}$. Then,*

$$\mathrm{rank}_{\mathbf{Z}_p}\,A^\vee(F_n) = O(1).$$

Proof. By Lemmas 3.2 and 3.9, it is enough to establish the statement on the μ-invariants. But (7) tells us that

$$\mu\left(\mathrm{Col}_{T,\underline{J}}(\mathbf{c})\right) - \mu\left(\mathrm{Sel}_{\underline{J}}(A/F_\infty)^\vee\right)$$

is independent of $\underline{J}$, so we are done. $\square$

Remark 3.11. In the case of elliptic curves with supersingular reduction at p, it is conjectured that the signed Selmer groups have zero μ-invariants [Pol03, Conjecture 6.3] [PR03, Conjecture 7.1].

3.3. **Abelian varieties of GL_2-type.** We now assume that A is an abelian variety defined over $\mathbf{Q}$ of GL_2-type as defined in [Rib92]; that is, the algebra of $\mathbf{Q}$-endomorphisms of A contains a number field E of degree $[E : \mathbf{Q}] = \dim A$. We also assume that the ring of integers $\mathcal{O}_E$ of E is the ring of $\mathbf{Q}$-endomorphisms of A and that p is unramified in E. In particular, the p-adic Tate module of A splits into

$$T \cong \bigoplus_{\mathfrak{p}|p} T_{\mathfrak{p}}(A),$$

where the direct sum runs over all primes $\mathfrak{p}$ of E above p and $T_{\mathfrak{p}}(A)$ is a free $\mathcal{O}_{\mathfrak{p}}$-module of rank 2 with $\mathcal{O}_{\mathfrak{p}}$ the completion of $\mathcal{O}_E$ at $\mathfrak{p}$.

Since A is defined over $\mathbf{Q}$, we have $\mathbf{D}_{\mathrm{cris},v}(T_{\mathfrak{p}}(A)) = \mathbf{D}_{\mathrm{cris}}(T_{\mathfrak{p}}(A)) \otimes \mathcal{O}_v$, where $\mathbf{D}_{\mathrm{cris}}(-)$ denotes the Dieudonné module over $\mathbf{Q}_p$. Therefore, it is sufficient to study the matrix of φ over $\mathbf{D}_{\mathrm{cris}}(T_{\mathfrak{p}}(A))$. The action of φ on $\mathbf{D}_{\mathrm{cris}}(T_{\mathfrak{p}}(A))$ is $\mathcal{O}_{\mathfrak{p}}$-linear, turning $\mathbf{D}_{\mathrm{cris}}(T_{\mathfrak{p}}(A))$ into a rank-two filtered $\mathcal{O}_{\mathfrak{p}}$-module.

By considering the image of the Kummer map in $\mathrm{H}^1(\mathbf{Q}_p, T_{\mathfrak{p}}(A))$, we see that the Hodge-Tate weights for this filtration are 0 and 1, each with multiplicity one. Fontaine-Laffaille theory tells us that there exists an $\mathcal{O}_{\mathfrak{p}}$-basis of the form $\omega_{\mathfrak{p}}, \varphi(\omega_{\mathfrak{p}})$, where $\omega_{\mathfrak{p}}$ generates $\mathrm{Fil}^0\,\mathbf{D}_{\mathrm{cris}}(T_{\mathfrak{p}}(A))$. As A is supersingular at p, the eigenvalues of φ are of the form $\zeta_i/\sqrt{p}$ $i = 1, 2$, where ζ_i is a root of unity. But p is unramified in $E_{\mathfrak{p}}$. For the trace of φ to be an element of $E_{\mathfrak{p}}$, $\zeta_1 + \zeta_2$ must be an element of $p\mathcal{O}_{\mathfrak{p}}$. Therefore, the matrix of φ with respect to the basis $\{\omega_{\mathfrak{p}}, \varphi(\omega_{\mathfrak{p}})\}$ is of the

form $\begin{pmatrix} 0 & \frac{b_{\mathfrak{p}}}{p} \\ 1 & \frac{a_{\mathfrak{p}}}{p} \end{pmatrix}$ for some $a_{\mathfrak{p}} \in p\mathcal{O}_{\mathfrak{p}}$ and $b_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times}$. If we choose a $\mathbf{Z}_p$-basis of $\mathcal{O}_{\mathfrak{p}}$, say $\{x_1, \ldots, x_{[E_{\mathfrak{p}}:\mathbf{Q}_p]}\}$, then this gives rise to a $\mathbf{Z}_p$-basis of $\mathbf{D}_{\mathrm{cris}}(T_{\mathfrak{p}}(A))$, namely,

$$\{x_i \omega_{\mathfrak{p},v}, x_i \varphi(\omega_{\mathfrak{p},v}) : i = 1, \ldots, [E_{\mathfrak{p}} : \mathbf{Q}_p]\}.$$

Under this choice of bases, we see that the resulting matrix C_v will be block anti-diagonal mod p for all v, in particular, Corollary 3.10. Furthermore, if $a_{\mathfrak{p},v} = 0$ for all $\mathfrak{p}$ and v, then C_v will even be block anti-diagonal. In this case, Corollary 3.7 applies.

Acknowledgments

References

[Ber04] Laurent Berger, *Limites de représentations cristallines* (French, with English and French summaries), Compos. Math. **140** (2004), no. 6, 1473–1498, DOI 10.1112/S0010437X04000879. MR2098398

[BL17] Kâzım Büyükboduk and Antonio Lei, *Integral Iwasawa theory of Galois representations for non-ordinary primes*, Math. Z. **286** (2017), no. 1-2, 361–398, DOI 10.1007/s00209-016-1765-z. MR3648502

[Gre89] Ralph Greenberg, *Iwasawa theory for p-adic representations*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 97–137, DOI 10.2969/aspm/01710097. MR1097613

[Gre99] Ralph Greenberg, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 51–144, DOI 10.1007/BFb0093453. MR1754686

[Gre01] Ralph Greenberg, *Introduction to Iwasawa theory for elliptic curves*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 407–464. MR1860044

[Gre03] Ralph Greenberg, *Galois theory for the Selmer group of an abelian variety*, Compositio Math. **136** (2003), no. 3, 255–297, DOI 10.1023/A:1023251032273. MR1977007

[IK19] Bo-Hae Im and Byoung Du Kim, *Ranks of rational points of the Jacobian varieties of hyperelliptic curves*, J. Number Theory **195** (2019), 23–50, DOI 10.1016/j.jnt.2018.08.002. MR3867432

[Ima75] Hideo Imai, *A remark on the rational points of abelian varieties with values in cyclotomic Z_p-extensions*, Proc. Japan Acad. **51** (1975), 12–16. MR371902

[Kat93] Kazuya Kato, *Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_dR. I*, Arithmetic algebraic geometry (Trento, 1991), Lecture Notes in Math., vol. 1553, Springer, Berlin, 1993, pp. 50–163, DOI 10.1007/BFb0084729. MR1338860

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms* (English, with English and French summaries), Cohomologies p-adiques et applications arithmétiques. III, Astérisque **295** (2004), ix, 117–290. MR2104361

[Kim18] Byoung Du Kim, *Ranks of the rational points of abelian varieties over ramified fields, and Iwasawa theory for primes with non-ordinary reduction*, J. Number Theory **183** (2018), 352–387, DOI 10.1016/j.jnt.2017.07.021. MR3715241

[Kob03] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36, DOI 10.1007/s00222-002-0265-4. MR1965358

[LLZ10] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Wach modules and Iwa-sawa theory for modular forms*, Asian J. Math. **14** (2010), no. 4, 475–528, DOI 10.4310/AJM.2010.v14.n4.a2. MR2774276

[LZ14]   David Loeffler and Sarah Livia Zerbes, *Iwasawa theory and p-adic L-functions over $\mathbb{Z}_p^2$-extensions*, Int. J. Number Theory **10** (2014), no. 8, 2045–2095, DOI 10.1142/S1793042114500699. MR3273476

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266, DOI 10.1007/BF01389815. MR444670

[Mum85] David Mumford, *Abelian varieties*, with appendices by C. P. Ramanujam and Yuri Manin, corrected reprint of the second (1974) edition, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. MR2514037

[Pol03] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558, DOI 10.1215/S0012-7094-03-11835-9. MR1983040

[PR90]   Bernadette Perrin-Riou, *Théorie d'Iwasawa p-adique locale et globale* (French), Invent. Math. **99** (1990), no. 2, 247–292, DOI 10.1007/BF01234420. MR1031902

[PR94]   Jean-Marc Fontaine, *Appendice: Sur un théorème de Bloch et Kato (lettre à B. Perrin-Riou)* (French), Invent. Math. **115** (1994), no. 1, 151–161, DOI 10.1007/BF01231756. MR1248080

[PR00]   Bernadette Perrin-Riou, *p-adic L-functions and p-adic representations*, translated from the 1995 French original by Leila Schneps and revised by the author, SMF/AMS Texts and Monographs, vol. 3, American Mathematical Society, Providence, RI; Société Mathématique de France, Paris, 2000. MR1743508

[PR03]   Bernadette Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersin-gulière en p* (French, with English and French summaries), Experiment. Math. **12** (2003), no. 2, 155–186. MR2016704

[Rib92] Kenneth A. Ribet, *Abelian varieties over **Q** and modular forms*, Algebra and topology 1992 (Taejŏn), Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, pp. 53–79. MR1212980

[Roh84] David E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), no. 3, 409–423, DOI 10.1007/BF01388636. MR735333

[Spr12] Florian E. Ito Sprung, *Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures*, J. Number Theory **132** (2012), no. 7, 1483–1506, DOI 10.1016/j.jnt.2011.11.003. MR2903167

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575

DÉPARTEMENT DE MATHÉMATIQUES ET DE STATISTIQUES, UNIVERSITÉ LAVAL, PAVILLON ALEXANDRE-VACHON, 1045 AVENUE DE LA MÉDECINE, QUÉBEC, QUEBEC, CANADA G1V 0A6
    Email address: antonio.lei@mat.ulaval.ca

MAX PLANCK INSTITUT FOR MATHEMATICS, VIVATSGASSE 7, 53111 BONN, GERMANY
    Email address: gautier.ponsinet@mpim-bonn.mpg.de