INTEGRAL POINTS ON ELLIPTIC CURVES AND MODULARITY

FEDERICO AMADIO GUIDI

Abstract. In this paper we prove the finiteness of the set of \( S \)-integral points of a punctured rational elliptic curve without complex multiplication using the Chabauty-Kim method. This extends previous results of Kim [14] in the complex multiplication case. The key input of our approach is the use of modularity techniques to prove the vanishing of certain Selmer groups involved in the Chabauty-Kim method.

Introduction

Let \( E \) be an elliptic curve with no complex multiplication over \( \mathbb{Q} \), and let \( X \) be the hyperbolic genus 1 curve over \( \mathbb{Q} \) obtained by removing the origin from \( E \). Let \( \mathcal{E} \) be a Weierstrass minimal model for \( E \), and let \( \mathcal{X} \) be the integral model of \( X \) obtained as the complement in \( \mathcal{E} \) of the Zariski closure of the origin. Let \( S \) be a finite set of rational primes including \( \infty \) and the primes of bad reduction for \( E \). We consider the set \( \mathcal{X}(\mathbb{Z}_S) \) of \( S \)-integral points of \( X \).

A classical theorem of Siegel, see for instance [17], states that \( \mathcal{X}(\mathbb{Z}_S) \) is finite. In this paper, we reprove this finiteness result using the Chabauty-Kim method.

Given a prime \( p \) of good reduction for \( E \), this method produces a nested sequence

\[
\mathcal{X}(\mathbb{Z}_p) \supset \mathcal{X}(\mathbb{Z}_p)_1 \supset \mathcal{X}(\mathbb{Z}_p)_2 \supset \cdots \supset \mathcal{X}(\mathbb{Z}_p)_n \supset \cdots \supset \mathcal{X}(\mathbb{Z}_S)
\]

of sets of \( p \)-adic points, each containing \( \mathcal{X}(\mathbb{Z}_S) \). A precise description of these sets is given in \( \S 1 \). The main result of this paper is the following.

**Theorem (see Corollary 1.3).** The sets \( \mathcal{X}(\mathbb{Z}_p)_n \) are finite for \( n \) sufficiently large.

This clearly implies the finiteness of \( \mathcal{X}(\mathbb{Z}_S) \). Moreover, note that combining this with the results of [14] in the complex multiplication case we get finiteness of the set of \( S \)-integral points of any rational elliptic curve minus the origin via the Chabauty-Kim method.

The key advantage of proving a finiteness result of this kind using the Chabauty-Kim method is that the finiteness of \( \mathcal{X}(\mathbb{Z}_p)_n \), and hence of \( \mathcal{X}(\mathbb{Z}_S) \), is obtained by showing that \( \mathcal{X}(\mathbb{Z}_p)_n \) is contained inside the zero locus of a \( p \)-adic analytic function which can be described in terms of \( p \)-adic iterated integrals, see [13]. This zero locus turns out to be finite, and hence an effective bound on its cardinality naturally yields an effective bound on the cardinality of \( \mathcal{X}(\mathbb{Z}_S) \).

The structure of this paper is the following. In \( \S 1 \) we give a quick introduction to the Chabauty-Kim method, and state our main finiteness theorem. In \( \S 2 \) we prove the key vanishing result for Bloch-Kato Selmer groups using modularity techniques. From this, using some Iwasawa theory, we deduce in \( \S 3 \) a vanishing result for Selmer groups, which will allow us to prove the main theorem in \( \S 4 \).

2010 Mathematics Subject Classification. 14G05, 11G05, 11F80.
Acknowledgements. The author would like to thank Minhyong Kim and Andrew Wiles for their very helpful comments, suggestions, and feedbacks. The author would also like to thank Laura Capuano for checking a preliminary version of this manuscript.

Notation. For a field $M$, we fix an algebraic closure $\overline{M}$ of $M$, a separable closure $M^s$ of $M$ inside $\overline{M}$, and we let $G_M = \text{Gal}(M^s/M)$ be the absolute Galois group of $M$. If $M$ is an algebraic extension of $\mathbb{Q}$, and $T$ is a finite set of places of $M$, we let $M_T$ be the maximal extension of $M$ inside $\overline{M}$ which is unramified outside $T$, and we let $G_{M,T} = \text{Gal}(M_T/M)$.

1. The Chabauty-Kim method

In his papers [12] and [13], Kim introduces a nonabelian analogue of the method of Chabauty-Coleman, often called Chabauty-Kim method or nonabelian Chabauty. We give here a quick introduction to it, roughly following the exposition of [13].

Let $X$ be a smooth curve over $\mathbb{Q}$, and let $X'$ be a smooth projective genus $g \geq 0$ curve over $\mathbb{Q}$ with $X \subset X'$ and $D = X' \setminus X$. Assume that $X$ is hyperbolic, that is $2g - 2 + \#D(\overline{\mathbb{Q}}) > 0$. Also, assume that we are given smooth models $\mathcal{X}'$ of $X'$ and $\mathcal{D}$ of $D$ over $\mathbb{Z}_S$, for $S$ some finite set of primes, and let $\mathcal{X} = \mathcal{X}' \setminus \mathcal{D}$.

The Chabauty-Kim method studies the set of $S$-integral points $\mathcal{X}(\mathbb{Z}_S)$ of $\mathcal{X}$ through certain motivic unipotent Albanese maps. Roughly speaking, the idea of these maps is to fix an $S$-integral base point $b$, choose a motivic unipotent fundamental group $U$ of $X$ with base point $b$, and map any other point $x$ to the class of the motivic $U$-torsor of paths from $b$ to $x$ in a suitable classifying space. In [12] and [13], Kim considers the de Rham and the étale realisations of the fundamental group.

For the rest of this section, let us fix an $S$-integral base point $b$, a prime $p$ of good reduction for $\mathcal{X}'$, and an embedding of $\overline{\mathbb{Q}}$ inside $\overline{\mathbb{Q}}_p$. Also, let us set $T = S \cup \{p\}$.

Let $U_{dR} = \pi_1^{dR,\mathbb{Q}_p}(\mathcal{X}_{\mathbb{Q}_p}, b)$ be the $\mathbb{Q}_p$-pro-unipotent de Rham fundamental group of $X_{\mathbb{Q}_p}$ with base point $b$. Let $U_{dR,n}$ be the descending central series of $U_{dR}$, and consider the finite dimensional quotients $U_{dR}^n = U_{dR,n+1} \setminus U_{dR}$ of $U_{dR}$. Note that $U_{dR}$ is naturally endowed with a decreasing Hodge filtration

$$U_{dR}^n \supset \cdots \supset F^i U_{dR} \supset F^{i+1} U_{dR} \supset \cdots \supset F^0 U_{dR},$$

which in turn induces decreasing filtrations on each $U_{dR}^n$. The quotient $U_{dR} / F^0 U_{dR}$ naturally classifies de Rham path spaces, see [13], hence the de Rham unipotent Albanese map can be defined to be the map

$$j^{dR} : \mathcal{X}(\mathbb{Z}_p) \to U_{dR} / F^0 U_{dR}.$$
which sends each \( x \) to the class of the \( U^\text{dR} \)-torsor of de Rham paths from \( b \) to \( x \). By passing to the quotients \( U^\text{dR}_n \), we get finite level versions
\[
j^\text{dR}_n : \mathcal{X}(\mathbb{Z}_p) \to U^\text{dR}_n / F^0U^\text{dR}_n,
\]
which fit into a natural compatible tower. Kim proves, see [13, Theorem 1], that for each \( n \geq 2 \) the image of \( j^\text{dR}_n \) is Zariski dense. This property is of crucial importance for applications to Diophantine finiteness.

Let us now move to the étale side of the picture. Let \( U^\text{ét} = \pi^\text{ét}_1(X_{\overline{\mathbb{Q}}}, b) \) be the \( \mathbb{Q}_p \)-pro-unipotent étale fundamental group of \( X_{\overline{\mathbb{Q}}} \) with base point \( b \), let \( U^\text{ét},n \) be the descending central series of \( U^\text{ét} \), and let \( U^\text{ét}_n = U^\text{ét},n+1 \setminus U^\text{ét} \). In [13], Kim defines the Selmer variety to be the provariety
\[
H^1_f(G_{\mathbb{Q},T}, U^\text{ét})
\]
that classifies \( G_{\mathbb{Q},T} \)-equivariant \( U^\text{ét} \)-torsors that are unramified outside \( T \), and crystalline at \( p \), and the étale unipotent Albanese map to be the map
\[
j^\text{ét} : \mathcal{X}(\mathbb{Z}_S) \to H^1_f(G_{\mathbb{Q},T}, U^\text{ét})
\]
given by sending each \( x \) to the class of the \( G_{\mathbb{Q},T} \)-equivariant \( U^\text{ét} \)-torsor of étale paths from \( b \) to \( x \). Also in this case, we have finite level versions
\[
j^\text{ét}_n : \mathcal{X}(\mathbb{Z}_S) \to H^1_f(G_{\mathbb{Q},T}, U^\text{ét}_n).
\]
Moreover, we also have local maps
\[
j^\text{ét}_{n,v} : \mathcal{X}(\mathbb{Z}_v) \to H^1_f(G_{\mathbb{Q},v}, U^\text{ét}_n)
\]
for each prime \( v \neq p \), and
\[
j^\text{ét}_{n,p} : \mathcal{X}(\mathbb{Z}_p) \to H^1_f(G_{\mathbb{Q},p}, U^\text{ét}_n),
\]
where \( H^1_f(G_{\mathbb{Q},v}, U^\text{ét}_n) \) classifies \( G_{\mathbb{Q},v} \)-equivariant \( U^\text{ét}_n \)-torsors that are crystalline.

A result of Kim and Tamagawa, see [16, Corollary 0.2], gives that the maps \( j^\text{ét}_{n,v} \), for \( v \neq p \), have finite image. Following [3], we define
\[
\mathcal{X}(\mathbb{Z}_p)_n = (j^\text{ét}_{n,p})^{-1}((\text{loc}_{p^v}(\cap_{v \neq p} \text{loc}_{v}^{-1}(\text{im} j^\text{ét}_{n,v})))),
\]
where \( \text{loc}_v \) are the naturally defined restriction maps. These sets clearly fit into a nested sequence
\[
\mathcal{X}(\mathbb{Z}_p) \supset \mathcal{X}(\mathbb{Z}_p)_1 \supset \mathcal{X}(\mathbb{Z}_p)_2 \supset \cdots \supset \mathcal{X}(\mathbb{Z}_p)_n \supset \cdots \supset \mathcal{X}(\mathbb{Z}_S).
\]

Finally, Kim considers a nonabelian extension of Fontaine’s Dieudonné functor, which gives an isomorphism of varieties:
\[
D : H^1_f(G_{\mathbb{Q},\overline{\mathbb{Q}}}, U^\text{ét}) \xrightarrow{\sim} U^\text{dR}_n / F^0U^\text{dR}_n,
\]
see [15, Proposition 1.4]. All these maps fit into the following fundamental commutative diagram.

\[
\begin{array}{ccc}
\mathcal{X}(\mathbb{Z}_S) & \xrightarrow{j_n^\text{et}} & \mathcal{X}(\mathbb{Z}_p) \\
H^1_j(G_{\mathbb{Q},T}, U_{n}^{\text{et}}) & \xrightarrow{\text{loc}_p} & H^1_j(G_{\mathbb{Q}_p}, U_{n}^{\text{et}}) \\
& \xrightarrow{j_n^{\text{dR}}} & U_{n}^{\text{dR}} / F^0 U_{n}^{\text{dR}}.
\end{array}
\]

The key point is that the image of \(\mathcal{X}(\mathbb{Z}_S)\) inside \(U_{n}^{\text{dR}} / F^0 U_{n}^{\text{dR}}\) turns out to be contained inside the image of \(H^1_j(G_{\mathbb{Q},T}, U_{n}^{\text{et}})\). We summarise the relation to Diophantine finiteness in the following lemma.

**Lemma 1.1.** If for some \(n \geq 2\) we have

\[
\dim H^1_j(G_{\mathbb{Q},T}, U_{n}^{\text{et}}) < \dim U_{n}^{\text{dR}} / F^0 U_{n}^{\text{dR}},
\]

then \(\mathcal{X}(\mathbb{Z}_p)_n\) is finite.

**Proof.** We let \(Y\) be the Zariski closure of the image of \(H^1_j(G_{\mathbb{Q},T}, U_{n}^{\text{et}})\) inside \(U_{n}^{\text{dR}} / F^0 U_{n}^{\text{dR}}\). Since \(\dim H^1_j(G_{\mathbb{Q},T}, U_{n}^{\text{et}}) < \dim U_{n}^{\text{dR}} / F^0 U_{n}^{\text{dR}}\), then \(Y\) is a proper subset of \(U_{n}^{\text{dR}} / F^0 U_{n}^{\text{dR}}\), and so there exists an algebraic function \(\alpha \neq 0\) on \(U_{n}^{\text{dR}} / F^0 U_{n}^{\text{dR}}\) which vanishes on \(Y\).

Since \(j_n^{\text{dR}}\) has Zariski dense image, we have that \(\alpha \circ j_n^{\text{dR}} \neq 0\) on \(\mathcal{X}(\mathbb{Z}_p)\). Moreover, \(\mathcal{X}(\mathbb{Z}_p)_n = (j_n^{\text{dR}})^{-1}(Y)\) is contained inside the zero locus of \(\alpha \circ j_n^{\text{dR}}\). This is finite by the \(p\)-adic Weierstrass preparation theorem. \(\Box\)

For the purposes of this paper, it is more convenient to replace, as in [14] and [7], each motivic unipotent fundamental group \(U\) with its maximal metabelian quotient, that is the quotient

\[
W = U/[U^2, U^2].
\]

Its finite dimensional quotients by the descending central series, as well as the corresponding Selmer varieties and unipotent Albanese maps are defined accordingly. Replacing \(U\) with \(W\) yields the same fundamental commutative diagram

\[
\begin{array}{ccc}
\mathcal{X}(\mathbb{Z}_S) & \xrightarrow{j_n^\text{et}} & \mathcal{X}(\mathbb{Z}_p) \\
H^1_j(G_{\mathbb{Q},T}, W_{n}^{\text{et}}) & \xrightarrow{\text{loc}_p} & H^1_j(G_{\mathbb{Q}_p}, W_{n}^{\text{et}}) \\
& \xrightarrow{j_n^{\text{dR}}} & W_{n}^{\text{dR}} / F^0 W_{n}^{\text{dR}},
\end{array}
\]

and Lemma 1.1 works verbatim.

Let us go back to our original setting, that is the genus 1 hyperbolic curve \(X\) obtained by removing the origin from an elliptic curve \(E\) without complex multiplication. The main result of this paper is the following.

**Theorem 1.2.** We have

\[
\dim H^1_j(G_{\mathbb{Q},T}, W_{n}^{\text{et}}) < \dim W_{n}^{\text{dR}} / F^0 W_{n}^{\text{dR}}
\]

for \(n\) sufficiently large.

\(^1\)This result is presented in alternative versions in the literature, from which this version can be easily deduced. We present its proof anyway for the sake of completeness.
Theorem 2.1. Let
\[ B \] denote Fontaine’s crystalline ring.

\[ \rho_{E,p} : G_{\mathbb{Q}} \to \text{GL}_2(\mathbb{Z}_p) \] the representation of \( G_{\mathbb{Q}} \) on the \( p \)-adic Tate module \( T_p(E) \) of \( E \), and we let \( V_p(E) = T_p(E) \otimes \mathbb{Q}_p \). By a classical result of Serre, see [3] §4, for every finite extension \( F \) of \( \mathbb{Q} \) we have that for \( p \) large enough the representation \( \rho_{E,p}|_{G_F} \) is surjective. For the rest of this paper, given any finite extension \( F \) of \( \mathbb{Q} \), up to eventually choosing a bigger \( p \), we assume that this condition is satisfied. As above, we let \( T = S \cup \{ p \} \). For any algebraic extension \( F \) of \( \mathbb{Q} \), we still denote by \( T \), with a slight abuse of notation, the set of places of \( F \) above those in \( T \). We prove the following result\(^2\).

**Theorem 2.1.** Let \( F \) be an imaginary quadratic field. Then we have

\[ H^1_f(G_{\mathbb{Q}}, \text{Sym}^{2n}V_p) \otimes \epsilon^{-n} \delta_{F/Q}^{n+1} = 0 \]

for all \( n \geq 1 \).

**Proof.** For simplicity of notation, let us write \( V = V_p(E) \). The Weil pairing induces an isomorphism \( V^\vee \cong V \otimes \epsilon^{-1} \), and so we have isomorphisms \( (\text{Sym}^n V)^\vee \cong \text{Sym}^n V \otimes \epsilon^{-n} \) for every \( n \geq 1 \). It follows that the representation of \( G_{\mathbb{Q}} \) on \( \text{Sym}^n V \) factors through \( \text{GO}_{n+1}(\mathbb{Q}_p) \) with totally even multiplier when \( n \) is even, and through \( \text{GSp}_{n+1}(\mathbb{Q}_p) \) with totally odd multiplier when \( n \) is odd.

For every \( n \geq 1 \), the natural symmetric pairing \( \text{Sym}^n V \times \text{Sym}^n V \to \text{Sym}^{2n} V \) induces a surjection \( \text{Sym}^2(\text{Sym}^n V) \to \text{Sym}^{2n} V \), which in turn induces a surjection

\[ \text{Sym}^2(\text{Sym}^n V) \otimes \epsilon^{-n} \delta_{F/Q}^{n+1} \to \text{Sym}^{2n} V \otimes \epsilon^{-n} \delta_{F/Q}^{n+1} \]

which is \( G_{\mathbb{Q},T} \)-equivariant, and has a \( G_{\mathbb{Q},T} \)-equivariant splitting. It follows that it is enough to show that \( H^1_f(G_{\mathbb{Q}}, \text{Sym}^2(\text{Sym}^n V) \otimes \epsilon^{-n} \delta_{F/Q}^{n+1}) = 0 \) for all \( n \geq 1 \).

Note that we have a decomposition as \( G_{\mathbb{Q}} \)-representations

\[ \text{ad}(\text{Sym}^n V|_{G_p}) \cong \text{Sym}^2(\text{Sym}^n V) \otimes \epsilon^{-n} \delta_{F/Q} \oplus \lambda^2(\text{Sym}^n V) \otimes \epsilon^{-n} \]

\(^2\)This result improves a previous result by Allen, see [3] Theorem 3.3.1, using the potential automorphy results of [3] and the vanishing results for adjoint Bloch-Kato Selmer groups of [3].
if $n$ is even, and

$$\text{ad}(\text{Sym}^n V \mid_{G_F}) \cong \text{Sym}^2(\text{Sym}^n V) \otimes \epsilon^{-n} \oplus \lambda^2(\text{Sym}^n V) \otimes \epsilon^{-n} \delta_{F/Q}$$

if $n$ is odd. In both cases, we have that $\text{Sym}^2(\text{Sym}^n V) \otimes \epsilon^{-n} \delta_{F/Q}$ as a $G_\mathbb{Q}$-representation is a direct summand of $\text{ad}(\text{Sym}^n V \mid_{G_F})$. It therefore follows that it is enough to prove that $H^1_H(G_{\mathbb{Q},T}, \text{ad}(\text{Sym}^n V \mid_{G_F})) = 0$ for all $n \geq 1$.

By [2] Theorem 7.1.9 we have that for every $n \geq 1$ there exists a finite CM Galois extension $F'$ of $F$ such that the representation $\text{Sym}^n V \mid_{G_{F'}}$ is automorphic. Let us fix $n \geq 1$ and a CM field $F'$ as above, and let us denote by $F''$ the maximal totally real subfield of $F'$. By considering restriction-corestriction and inflation, we get an injection $H^1(G_{\mathbb{Q},T}, \text{ad}(\text{Sym}^n V \mid_{G_F})) \to H^1(G_{F'',T}, \text{ad}(\text{Sym}^n V \mid_{G_{F'}}))$ such that the following diagram commutes

$$\begin{array}{ccc}
H^1(G_{\mathbb{Q},T}, \text{ad}(\text{Sym}^n V \mid_{G_F})) & \longrightarrow & H^1(G_{\mathbb{Q},p}, B_{\text{cris}} \otimes \text{ad}(\text{Sym}^n V \mid_{G_F})) \\
\downarrow & & \downarrow \\
H^1(G_{F'',T}, \text{ad}(\text{Sym}^n V \mid_{G_{F'}})) & \longrightarrow & \prod_{\mathfrak{p} \mid p} H^1(G_{F'',\mathfrak{p}}, B_{\text{cris}} \otimes \text{ad}(\text{Sym}^n V \mid_{G_{F'}})).
\end{array}$$

We then get an injection $H^1_H(G_{\mathbb{Q},T}, \text{ad}(\text{Sym}^n V \mid_{G_F})) \to H^1_H(G_{F'',T}, \text{ad}(\text{Sym}^n V \mid_{G_{F'}}))$, and so it is enough to prove that $H^1_H(G_{F,T}, \text{ad}(\text{Sym}^n V \mid_{G_{F'}})) = 0$. In particular, up to eventually choosing a bigger $p$, we can assume that each $\text{Sym}^n V \mid_{G_F}$ is automorphic.

Since $\rho_{E,F} \mid_{G_F}$ is surjective, we have that $\text{Sym}^n \rho_{E,F}(G_{F,(q_n)})$ is an enormous subgroup of $\text{GL}_{n+1}(\mathbb{Z}_p)$ for every $n \geq 1$, see [13 Example 2.34]. Then, since $\text{Sym}^n V \mid_{G_F}$ is automorphic, by [13 Theorem 5.2] we get that $H^1_H(G_{\mathbb{Q},T}, \text{ad}(\text{Sym}^n V \mid_{G_F})) = 0$ for every $n \geq 1$. The conclusion follows.

\[\square\]

**Remark 2.2.** Note that our proof works verbatim when $\mathbb{Q}$ is replaced by any totally real number field.

3. **Iwasawa theory and vanishing of Selmer groups**

In this section, we prove a vanishing result for Selmer groups, using some Iwasawa theory and the vanishing results for Bloch-Kato Selmer groups proved in the previous section. Let us first of all introduce some notation. Given a representation $V$ of $G_F$ over $\mathbb{Q}_p$, unramified outside a finite set $S$ of places of $F$ containing the infinite places and no places above $p$, having set $T = S \cup \{v \mid p\}$, we recall that the $i$-th Selmer group of $V$ is defined as

$$\text{Sel}^i(G_{F,T}, V) = \ker(\text{Sel}^i(G_{F,T}, V) \to \prod_{v \in T} H^i(G_{F_v}, V)).$$

For $i = 1$, it is immediate to notice that we have an inclusion $\text{Sel}^1(G_{F,T}, V) \subset H^1_H(G_{F,T}, V)$. Moreover, we have

**Lemma 3.1.** Let $V^D = V^\vee \otimes \epsilon$ denote the Cartier dual of $V$. Then:

1. If $H^2(G_{F,T}, V^D) = 0$, then $\text{Sel}^1(G_{F,T}, V) = 0$.
2. If $V$ is geometric and pure of nonzero weight\(^\dagger\) and if $\text{Sel}^1(G_{F,T}, V) = 0$, then $H^2(G_{F,T}, V^D) = 0$.

\(^\dagger\)Recall that a geometric representation $V$ of $G_F$ over $\mathbb{Q}_p$ is said to be pure of weight $w \in \mathbb{R}$ if for each finite place $v$ of $F$ the Weil-Deligne representation attached to $V \mid_{G_{F_v}}$ is pure of weight $w$ in the sense of [21 §1].
Proof. By Poitou-Tate duality, we have an exact sequence
\[ H^2(G_{F,T}, V^D) \to H^1(G_{F,T}, V) \to \prod_{v \in T} H^1(G_{F_v}, V), \]
and so part (1) immediately follows.

Moving to part (2), again by Poitou-Tate duality, we have that \( \text{III}^2(G_{F,T}, V^D) \cong \text{III}^1(G_{F,T}, V)^{\vee} \), and so that \( \text{III}^2(G_{F,T}, V^D) = 0 \). It follows that the map
\[ H^2(G_{F,T}, V^D) \to \prod_{v \in T} H^2(G_{F_v}, V^D) \]
is injective. Now, by local Tate duality, for every \( v \in T \) we have an isomorphism
\[ H^2(G_{F_v}, V^D) \cong H^0(G_{F_v}, V)^{\vee}. \]
In order to get the conclusion, it is then enough to show that \( H^0(G_{F_v}, V) = 0 \) for each \( v \in T \).

Let \( v \in T \). If \( v \nmid p \), since the Weil-Deligne representation attached to \( V |_{G_{F_v}} \) is pure of nonzero weight by assumption, we have that \( H^0(G_{F_v}, V) = \text{Hom}_{G_{F_v}}(\mathbb{Q}_p, V) = 0 \).

If \( v \mid p \), since \( V |_{G_{F_v}} \) is unramified, then it is crystalline, and we have \( H^0(G_{F_v}, V) = \text{Hom}_{G_{F_v}}(\mathbb{Q}_p, \mathbb{Q}_p, V) = \text{Hom}_{\mathbb{MF}(\phi)}(F^\text{nr}_v, D_{\text{cris}}(V)) \), where \( \mathbb{MF}(\phi) \) denotes Fontaine’s category of admissible filtered \( \phi \)-modules, \( F^\text{nr}_v \) denotes the maximal absolutely unramified subfield of \( F_v \), and \( D_{\text{cris}} \) denotes Fontaine’s crystalline functor. Since the Weil-Deligne representation attached to \( V |_{G_{F_v}} \) is pure of nonzero weight by assumption, we get that \( \text{Hom}_{\mathbb{MF}(\phi)}(F^\text{nr}_v, D_{\text{cris}}(V)) = 0 \), and so the conclusion follows. \( \square \)

Back to our original setting, we let \( \mathbb{Q}^\infty \) be the field generated by the \( p \)-power torsion points of \( E \) over \( \mathbb{Q} \). Note that the Weil pairing gives an inclusion \( \mathbb{Q}(\zeta_p^\infty) \subset \mathbb{Q}^\infty \). Also, for our choice of \( p \) the representation \( \rho_{E,p} \) induces an isomorphism \( \text{Gal}(\mathbb{Q}^\infty/\mathbb{Q}) \cong \text{GL}_2(\mathbb{Z}_p) \).

Write \( \Gamma = \text{Gal}(\mathbb{Q}^\infty/\mathbb{Q}) \), and let \( \Lambda = \mathbb{Z}_p[\Gamma] \) be the Iwasawa algebra of \( \Gamma \). Let \( H^\wedge_\Gamma \) be the maximal unramified abelian pro-\( p \)-extension of \( \mathbb{Q}^\infty \) in which all primes above \( T \) split completely, and let \( \mathcal{X}^\wedge_\Gamma = \text{Gal}(H^\wedge_\Gamma/\mathbb{Q}^\infty) \), which is naturally a \( \Lambda \)-module. We prove the following lemma.

**Lemma 3.2.** Let \( V \) be a semisimple representation of \( \text{GL}(V_p(E)) \) over \( \mathbb{Q}_p \) which does not contain \( \mathbb{Q}_p \) as an irreducible subrepresentation. Then, considering \( V \) as a representation of \( G_{\mathbb{Q}} \) via \( \rho_{E,p} \), we have an isomorphism
\[ \text{III}^1(G_{\mathbb{Q},T}, V) \cong \text{Hom}_\Lambda(\mathcal{X}^\wedge_\Gamma, V). \]

**Proof.** Since \( \Gamma \) is isomorphic to \( \text{GL}_2(\mathbb{Z}_p) \) via \( \rho_{E,p} \), we have an isomorphism \( H^*(\Gamma, V) \cong H^*(\text{GL}_2(\mathbb{Z}_p), V) \). Now, since \( V \) does not contain \( \mathbb{Q}_p \) as an irreducible subrepresentation, by Lazard’s isomorphism, see for instance [20, Theorem 5.2.4], and the fact that for the Lie algebra cohomology we have \( H^i(\text{gl}_2(\mathbb{Z}_p), V) = 0 \) for \( i \geq 0 \) by [10, Theorem 10], we get that \( H^i(\text{GL}_2(\mathbb{Z}_p), V) = 0 \) for \( i \geq 0 \). It follows that \( H^i(\Gamma, V) = 0 \) for \( i \geq 0 \).

Since the induced action of \( G_{\mathbb{Q}^\infty,T} \) on \( V \) is trivial, the Hochschild-Serre spectral sequence for the closed normal subgroup \( G_{\mathbb{Q}^\infty,T} \) of \( G_{\mathbb{Q},T} \) gives an exact sequence
\[ H^1(\Gamma, V) \to H^1(G_{\mathbb{Q},T}, V) \to \text{Hom}(G_{\mathbb{Q}^\infty,T}, V)^\Gamma \to H^2(\Gamma, V). \]

We then get an isomorphism \( H^1(G_{\mathbb{Q},T}, V) \cong \text{Hom}(G_{\mathbb{Q}^\infty,T}, V)^\Gamma = \text{Hom}_\Lambda(G_{\mathbb{Q}^\infty,T}, V) \), which in turn induces an isomorphism \( \text{III}^1(G_{\mathbb{Q},T}, V) \cong \text{Hom}_\Lambda(\mathcal{X}^\wedge_\Gamma, V). \) \( \square \)

We prove the following result.
Theorem 3.3. We have

$$\text{III}^1(G_{\mathbb{Q},T}, \text{Sym}^n V_p(E) \otimes \epsilon^{-n}) = 0$$

for all $n \geq 2$.

Proof. By part (1) of Lemma 3.1 it is enough to prove that $H^2(G_{\mathbb{Q},T}, \text{Sym}^n V_p(E) \otimes \epsilon) = 0$. Let us write $n = 2k + h$, where $k \geq 1$ is odd, and $h \in \{0, 1, 2, 3\}$. The natural surjection $\text{Sym}^{2k} V_p(E) \otimes \text{Sym}^h V_p(E) \to \text{Sym}^n V_p(E)$ induces a surjection

$$\text{Sym}^{2k} V_p(E) \otimes \text{Sym}^h V_p(E) \otimes \epsilon \to \text{Sym}^n V_p(E) \otimes \epsilon$$

which is $G_{\mathbb{Q},T}$-equivariant. Since $G_{\mathbb{Q},T}$ has $p$-cohomological dimension 2, we get a surjection

$$H^2(G_{\mathbb{Q},T}, \text{Sym}^{2k} V_p(E) \otimes \text{Sym}^h V_p(E) \otimes \epsilon) \to H^2(G_{\mathbb{Q},T}, \text{Sym}^n V_p(E) \otimes \epsilon),$$

and so it is enough to prove that $H^2(G_{\mathbb{Q},T}, \text{Sym}^{2k} V_p(E) \otimes \text{Sym}^h V_p(E) \otimes \epsilon) = 0$. Moreover, since $\text{Sym}^{2k} V_p(E) \otimes \text{Sym}^h V_p(E) \otimes \epsilon^{-n}$ is pure of weight $n \neq 0$, by part (2) of Lemma 3.1 it is enough to prove that $\text{III}^1(G_{\mathbb{Q},T}, \text{Sym}^{2k} V_p(E) \otimes \text{Sym}^h V_p(E) \otimes \epsilon^{-n}) = 0$.

Let $V = \text{Sym}^{2k} V_p(E) \otimes \text{Sym}^h V_p(E) \otimes \epsilon^{-n}$ and $V' = \text{Sym}^{2k} V_p(E) \otimes \epsilon^{-k}$, and let $V = \text{Sym}^{2k} T_p(E) \otimes \text{Sym}^h T_p(E) \otimes \epsilon^{-n}$ and $V' = \text{Sym}^{2k} T_p(E) \otimes \epsilon^{-k}$ be $G_{\mathbb{Q},T}$-stable $\mathbb{Z}_p$-lattices, so that $V' \cong V \otimes \text{Sym}^h T_p(E) \otimes \epsilon^{-n+k}$. Since $V$ is pure of weight $n \neq 0$, and so it cannot contain $\mathbb{Q}_p$ as a $\text{GL}(V_p(E))$-subrepresentation, and $V'$ is nontrivial and irreducible as a $\text{GL}(V_p(E))$-representation, by Lemma 3.2 we have that $\text{III}^1(G_{\mathbb{Q},T}, V) = \text{Hom}_{\Lambda}(X^\infty_T, V)$ and $\text{III}^1(G_{\mathbb{Q},T}, V') = \text{Hom}_{\Lambda}(X^\infty_T, V')$. Since $\text{III}^1(G_{\mathbb{Q},T}, V') \subset H^1(G_{\mathbb{Q},T}, V')$, by Theorem 2.1 we have that $\text{III}^1(G_{\mathbb{Q},T}, V') = 0$, and hence that $\text{Hom}_{\Lambda}(X^\infty_T, V') = 0$.

On the other hand, since $\mathbb{Q}^\infty$ contains the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, we have that $X^\infty_T$ is a finitely generated torsion $\Lambda$-module by Lemma 3.4, and hence finitely presented, as $\Lambda$ is Noetherian. Moreover, $\text{Sym}^h T_p(E) \otimes \epsilon^{-n+k}$ is $\mathbb{Z}_p$-flat, and so $\text{Hom}_{\Lambda}(X^\infty_T, V) = \text{Hom}_{\Lambda}(X^\infty_T, V') \otimes \text{Sym}^h T_p(E) \otimes \epsilon^{-n+k}$, which in turn induces an isomorphism $\text{Hom}_{\Lambda}(X^\infty_T, V) \cong \text{Hom}_{\Lambda}(X^\infty_T, V') \otimes \text{Sym}^h V_p(E) \otimes \epsilon^{-n+k}$. It follows that $\text{Hom}_{\Lambda}(X^\infty_T, V) = 0$, hence that $\text{III}^1(G_{\mathbb{Q},T}, V) = 0$. \qed

Remark 3.4. We remark that also the results of this section can be immediately extended to any totally real base field.

4. Proof of Theorem 1.2

Let us start by proving the following lemma.

Lemma 4.1. We have a $G_{\mathbb{Q},T}$-equivariant isomorphism

$$W^{\text{ét}, n+1}\backslash W^{\text{ét}, n} \cong \text{Sym}^{n-2} V_p(E) \otimes \epsilon$$

for every $n \geq 2$.

Proof. Let us first of all prove that $W^{\text{ét}, n+1}\backslash W^{\text{ét}, n}$ is a quotient of $\text{Sym}^{n-2} V_p(E) \otimes \epsilon$ as a $G_{\mathbb{Q},T}$-module.\footnote{The proof of this fact has been suggested to us by Minhyong Kim, which we thank once more.}
Let $u^{\text{et}}$ be the Lie algebra of $U^{\text{et}}$, and let $u^{\text{et},n}$ be its descending central series. We have a natural $G_{\mathbb{Q},T}$-equivariant isomorphism

$$U^{\text{et},n+1}\backslash U^{\text{et},n} \cong u^{\text{et},n+1}\backslash u^{\text{et},n}.$$ 

Let $u^{\text{et}}_1 = u^{\text{et},2}\backslash u^{\text{et}}$, so that $u^{\text{et}}_n \cong V_p(E)$. By induction on $n \geq 2$, using the identity $u^{\text{et},n+1}\backslash u^{\text{et},n} = [u^{\text{et}}_1, u^{\text{et},n}\backslash u^{\text{et},n-1}]$, we see that $u^{\text{et},n+1}\backslash u^{\text{et},n}$ is generated as a $G_{\mathbb{Q},T}$-module by elements of the form $[a_1, [a_2, \cdots [a_{n-2}, b] \cdots ]]$, where $a_i \in u^{\text{et}}_1$, and $b \in u^{\text{et},2}\backslash u^{\text{et},1}$. Note that as a $G_{\mathbb{Q},T}$-module $u^{\text{et},3}\backslash u^{\text{et},2}$ is a quotient of $\wedge^2 u^{\text{et}}_1$.

Let now $w^{\text{et}}$ be the Lie algebra of $W^{\text{et}}$, and let $w^{\text{et},n}$ be its descending central series. For every generator $[a_1, [a_2, \cdots [a_{n-2}, b] \cdots ]]$ of $u^{\text{et},n+1}\backslash u^{\text{et},n}$ as above, we have that modulo $[u^{\text{et},2}, u^{\text{et},2}]$ the order of the $a_i$’s can be normalised to any fixed order. It follows that as a $G_{\mathbb{Q},T}$-module $W^{\text{et},n+1}\backslash W^{\text{et},n} \cong w^{\text{et},n+1}\backslash w^{\text{et},n}$ is a quotient of

$$\text{Sym}^{n-2} u^{\text{et}}_1 \otimes \wedge^2 u^{\text{et}}_1 \cong \text{Sym}^{n-2} V_p(E) \otimes \epsilon.$$ 

Since $\text{Sym}^{n-2} V_p(E) \otimes \epsilon$ is irreducible, and $W^{\text{et},n+1}\backslash W^{\text{et},n} \neq 0$, we conclude that as $G_{\mathbb{Q},T}$-modules $W^{\text{et},n+1}\backslash W^{\text{et},n} \cong \text{Sym}^{n-2} V_p(E) \otimes \epsilon$. \hfill $\square$

Combining this with the results of the previous section we immediately get

**Corollary 4.2.** We have

$$H^2(G_{\mathbb{Q},T}, W^{\text{et},n+1}\backslash W^{\text{et},n}) = 0$$

for all $n \geq 4$.

We can finally prove our main result.

**Proof of Theorem 1.2.** Assume that $n \geq 2$. For both the de Rham and the étale realisations, let us consider the exact sequence

$$0 \to W_{n+1}^{\text{dR}} \backslash W^n \to W_n \to W_{n-1} \to 0.$$ 

In the de Rham realisation, we get that

$$\dim(W_{n}^{\text{dR}}/F^0 W_{n}^{\text{dR}}) - \dim(W_{n-1}^{\text{dR}}/F^0 W_{n-1}^{\text{dR}}) = \dim(W_{n+1}^{\text{dR},n}\backslash W_{n+1}^{\text{dR},n}) - \dim(F^0(W_{n}^{\text{dR},n+1}\backslash W_{n}^{\text{dR},n})$$

for $n \geq 2$. Following [13, §3 and §4] and [14, §3], we get that

$$\dim(W_{2}^{\text{dR}}/F^0 W_{2}^{\text{dR}}) = 2$$

and that

$$\dim(F^0(W_{n}^{\text{dR},n+1}\backslash W_{n}^{\text{dR},n}) \leq 1$$

for $n \geq 3$, so that

$$\dim(W_{n}^{\text{dR}}/F^0 W_{n}^{\text{dR}}) \geq 3 + \frac{n(n-3)}{2}$$

for $n \geq 3$. 

Let us now move to the étale side of the picture. First of all, we have that
\[ \dim H^1_f(G_{Q,T}, W^{\text{ét}}_n) - \dim H^1_f(G_{Q,T}, W^{\text{ét}}_{n-1}) \leq \dim H^1_f(G_{Q,T}, W^{\text{ét}, n+1}_T \setminus W^{\text{ét}, n}) \]
for \( n \geq 2 \). Let now \( s \) be the cardinality of \( S \), and let \( r = \dim H^1_f(G_{Q,T}, V_p(E)) \). With these notations, following [14 §3], we get that
\[ \dim H^1_f(G_{Q,T}, W^{\text{ét}}_n) \leq r + s - 1, \]
and hence that
\[ \dim H^1_f(G_{Q,T}, W^{\text{ét}}_n) \leq r + s - 1 + \sum_{i=3}^n h^1(G_{Q,T}, W^{\text{ét}, i+1}_T \setminus W^{\text{ét}, i}) \]
for \( n \geq 3 \). By Lemma 4.1 we have a \( G_{Q,T} \)-equivariant isomorphism \( W^{\text{ét}, i+1}_T \setminus W^{\text{ét}, i} \cong \text{Sym}^{i-2} V_p(E) \otimes \epsilon \) for every \( i \geq 3 \). Let \( r' = h^1(G_{Q,T}, W^{\text{ét}, 4}_T \setminus W^{\text{ét}, 3}) = h^1(G_{Q,T}, V_p(E) \otimes \epsilon) \).
For \( i \geq 4 \) the Euler characteristic formula gives that
\[ h^1(G_{Q,T}, W^{\text{ét}, i+1}_T \setminus W^{\text{ét}, i}) = h^2(G_{Q,T}, W^{\text{ét}, i+1}_T \setminus W^{\text{ét}, i}) + \dim(W^{\text{ét}, i+1}_T \setminus W^{\text{ét}, i}) \epsilon^{i-1}, \]
where \( \epsilon \) denotes the complex conjugation induced by \( \infty \). By Corollary 4.2 we have that
\[ h^2(G_{Q,T}, W^{\text{ét}, i+1}_T \setminus W^{\text{ét}, i}) = 0. \]

Also, since \( \text{Sym}^{i-2} V_p(E) \) becomes automorphic over a finite totally real Galois extension of \( Q \) by [4 Theorem 7.1.4], so does \( \text{Sym}^{i-2} V_p(E) \otimes \epsilon \), and so we have that
\[ \dim(W^{\text{ét}, i+1}_T \setminus W^{\text{ét}, i}) \epsilon^{i-1} = \left\lfloor \frac{i-1}{2} \right\rfloor \text{ or } \left\lceil \frac{i-1}{2} \right\rceil \]
by [4 Theorem 1.1]. Moreover, since \( \text{Sym}^{i-2} V_p(E) \otimes \epsilon \) has determinant \( \epsilon^{i-1} \), and \( \epsilon^{-1}(\epsilon) = (-1)^{i-1} \), we deduce that
\[ \dim(W^{\text{ét}, i+1}_T \setminus W^{\text{ét}, i}) \epsilon^{i-1} = \left\lfloor \frac{i-1}{2} \right\rfloor + 1 \text{ if } i \equiv 2 \pmod{4}, \]
\[ \text{or } 0 \text{ otherwise.} \]

If \( n \) is divisible by 4, we then get that
\[ \dim H^1_f(G_{Q,T}, W^{\text{ét}}_n) \leq r + r' + s + n \left( \frac{n}{4} + 1 \right) + \frac{3n}{4}. \]

In conclusion, if we choose \( n_0 \) to be the smallest integer \( n \geq 4 \) divisible by 4 and such that
\[ r + r' + s + n \left( \frac{n}{4} + 1 \right) + \frac{3n}{4} < 3 + \frac{n(n-3)}{2}, \]
we get that
\[ \dim H^1_f(G_{Q,T}, W^{\text{ét}}_n) < \dim W^{dR}_n / E^{dR} W^{dR}_n \]
for every \( n \geq n_0 \) as required.

\[ \square \]

**Remark 4.3.** Keep notations as in the proof of Theorem 1.2. We remark that the Block-Kato conjectures, see for instance [5 §4.2.2], predict \( r \) to be equal to the analytic rank of \( E \) (nevertheless, using the Kummer map, we always have that \( r \) is greater than or equal to the algebraic rank of \( E \)), and a conjecture of Jannsen, see [11 §6], predicts that \( r' = 1 \).

\(^5\)We assume that \( n \) is divisible by 4 just to simplify the computations. Note that this assumption affects our final lower bound estimate only of an error term \( \leq 3 \).
REFERENCES

[1] P. Allen. Deformations of polarized automorphic Galois representations and adjoint Selmer groups. *Duke Math. J.*, 165(13):2407–2460, 2016.

[2] P. B. Allen, F. Calegari, A. Caraiani, T. Gee, D. Helm, B. V. Le Hung, J. Newton, P. Scholze, R. Taylor, and J. A. Thorne. Potential automorphy over CM fields. *ArXiv preprint arXiv:1812.09999*, 2018.

[3] J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers. A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves. *Math. Ann.*, 372(1-2):369–428, 2018.

[4] T. Barnet-Lamb, T. Gee, and D. Geraghty. The Sato-Tate conjecture for Hilbert modular forms. *J. Amer. Math. Soc.*, 24(2):411–469, 2011.

[5] N. Bourbaki. *Commutative Algebra*. Hermann, Paris, 1972.

[6] A. Caraiani and B. V. L. Hung. On the image of complex conjugation in certain Galois representations. *Compos. Math.*, 152(7):1476–1488, 2016.

[7] J. Coates and M. Kim. Selmer varieties for curves with CM Jacobians. *Kyoto J. Math.*, 50(4):827–852, 2010.

[8] J.-M. Fontaine and B. Perrin-Riou. Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions $L$. In U. Jannsen, S. Kleiman, and J.-P. Serre, editors, *Motives (Seattle, WA, 1991)*, volume 55, Part 1 of *Proc. Sympos. Pure Math.*, pages 599–706. American Mathematical Society, Providence, 1994.

[9] Y. Hachimori and R. T. Sharifi. On the failure of pseudo-nullity of Iwasawa modules. *J. Algebraic Geom.*, 14(3):567–591, 2005.

[10] G. Hochschild and J.-P. Serre. Cohomology of Lie algebras. *Ann. of Math.*, 57(3):591–603, 1953.

[11] U. Jannsen. On the $\ell$-adic cohomology of varieties over number fields and its Galois cohomology. In K. Ribet, Y. Ihara, and J.-P. Serre, editors, *Galois groups over $\mathbb{Q}$*, volume 16 of *Math. Sci. Res. Inst. Publ.*, chapter 5, pages 315–360. Springer, New York, 1989.

[12] M. Kim. The motivic fundamental group of the projective line minus three points and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[13] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS, Kyoto Univ.*, 45:89–133, 2009.

[14] M. Kim. $p$-adic $L$-functions and Selmer varieties associated to elliptic curves with complex multiplication. *Ann. of Math.*, 172(1):751–759, 2010.

[15] M. Kim. Tangential localization for Selmer varieties. *Duke Math. J.*, 161(2):173–199, 2012.

[16] M. Kim and A. Tamagawa. The $l$-component of the unipotent Albanese map. *Math. Ann.*, 340(1):223–235, 2008.

[17] S. Lang. *Fundamentals of Diophantine Geometry*. Springer-Verlag, New York Berlin Heidelberg Tokyo, 1983.

[18] J. Newton and J. A. Thorne. Adjoint Selmer groups of automorphic Galois representations of unitary type. *ArXiv preprint arXiv:1912.11265*, 2019.

[19] J.-P. Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972.

[20] P. Symonds and T. Weigel. Cohomology of $p$-adic analytic groups. In *New horizons in pro-$p$ groups*, pages 349–410. Springer, 2000.

[21] R. Taylor and T. Yoshida. Compatibility of local and global Langlands correspondences. *J. Amer. Math. Soc.*, 20:467–493, 2007.

Mathematical Institute, University of Oxford, Oxford, UK
E-mail address: federico.amadio@maths.ox.ac.uk