Selmer varieties for curves with CM Jacobians

John Coates and Minhyong Kim

February 3, 2010

Abstract

We study the Selmer variety associated to a canonical quotient of the $\mathbb{Q}_p$-pro-unipotent fundamental group of a smooth projective curve of genus at least two defined over $\mathbb{Q}$ whose Jacobian decomposes into a product of abelian varieties with complex multiplication. Elementary multivariable Iwasawa theory is used to prove dimension bounds, which, in turn, lead to a new proof of Diophantine finiteness over $\mathbb{Q}$ for such curves.

Let $X/\mathbb{Q}$ be a smooth proper curve of genus $g \geq 2$ and $b \in X(\mathbb{Q})$ a rational point. We assume that X has good reduction outside a finite set S of primes and choose an odd prime $p \notin S$. In earlier papers ([14], [15], [16], [17], [18]), a p-adic *Selmer variety*

$$H^1_f(G, U)$$

was defined and studied, with the hope of applying its structure theory to the Diophantine geometry of X. Here, $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$,

$$U = \pi_1^{\mathbb{Q}_p, un}(\bar{X}, b)$$

is the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of

$$\bar{X} = X \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\bar{\mathbb{Q}}),$$

and the subscript f refers to a collection of local 'Selmer conditions,' carving out a moduli space of torsors for U on the étale topology of $\mathrm{Spec}(\mathbb{Z}[1/S, 1/p])$ that satisfy the condition of being *crystalline* at p.

The Selmer variety is actually a pro-variety consisting of a projective system

$$\cdots \to H^1_f(G, U_{n+1}) \to H^1_f(G, U_{n+1}) \to \cdots \to H^1_f(G, U_2) \to H^1_f(G, U_1)$$

of varieties over $\mathbb{Q}_p$ associated to the descending central series filtration

$$U = U^1 \supset U^2 \supset U^n \supset U^{n+1} = [U, U^n] \supset \cdots$$

of U and the corresponding system of quotients

$$U_n = U^{n+1} \backslash U$$

that starts out with

$$U_1 = V = T_p J \otimes \mathbb{Q}_p,$$

the $\mathbb{Q}_p$-Tate module of the Jacobian J of X.

As a natural extension of the map

$$\begin{tikzcd} X(\mathbb{Q}) \arrow[r] & J(\mathbb{Q}) \arrow[r] & H^1_f(G, V) \end{tikzcd}$$

visible in classical Kummer theory, the Selmer variety is endowed with a system of *unipotent Albanese maps* emanating from the points of X:

$$\begin{tikzcd}
 & \vdots \\
\vdots & H^1_f(G,U_4) \arrow[d] \\
 & H^1_f(G,U_3) \arrow[d] \\
 & H^1_f(G,U_2) \arrow[d] \\
X(\mathbb{Q}) \arrow[r] \arrow[ur] \arrow[uur] \arrow[uuur] & H^1_f(G,U_1)
\end{tikzcd}$$

These maps fit into commutative diagrams

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d] & X(\mathbb{Q}_p) \arrow[d] \arrow[dr] & \\
H^1_f(G,U_n) \arrow[r, "\mathrm{loc}_p"] & H^1_f(G_p,U_n) \arrow[r, "D"] & U_n^{DR}/F^0
\end{tikzcd}$$

involving the local Selmer varieties $H^1_f(G_p,U_n)$ and their De Rham realizations U_n^{DR}/F^0. Here, F^0 refers to the zeroth level of the Hodge filtration

$$U^{DR} \supset \cdots \supset F^i \supset F^{i+1} \supset \cdots \supset F^0$$

on the De Rham fundamental group U^{DR} of $X \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\mathbb{Q}_p)$. Recall that the De Rham fundamental group is defined using the Tannakian category of unipotent vector bundles with flat connections on $X \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\mathbb{Q}_p)$ ([15], section 1), and that the Hodge filtration F^{-i} on U^{DR} is the subvariety defined by the ideal $F^{i+1}\mathcal{A}^{DR}$ in the coordinate ring $\mathcal{A}^{DR}$ of U^{DR} (loc. cit. and [4]). F^0U^{DR} turns out to be a subgroup. The filtration on $\mathcal{A}^{DR}$ is defined over $\mathbb{C}$ using the $(d, \bar{d})$ decomposition on iterated integrals of differential forms, but descends to any field of characteristic zero [32]. Here and in the following, we will suppress from the notation the object that the Hodge filtration filters when the context provides sufficient clarity.

Diophantine motivations oblige us to study the localization map $D \circ \mathrm{loc}_p$ with some care. In fact, one could formulate the *dimension hypothesis*

$$\mathrm{dim} H^1_f(G,U_n) < \mathrm{dim} U_n^{DR}/F^0 \qquad (DH_n)$$

for each n, and show that DH_n for any fixed n implies the finiteness of $X(\mathbb{Q})$ [15]. Throughout this paper, dimension will refer to that of algebraic varieties over $\mathbb{Q}_p$ [14], although the dimensions of various associated graded objects, e.g., U^n/U^{n+1}, are just the naive ones of $\mathbb{Q}_p$-vector spaces. Given any X, it seems reasonable to believe that DH_n should be true for n sufficiently large [15].

An eventual goal is to use the Selmer variety to arrive at a structural understanding of the Diophantine set $X(\mathbb{Q})$, or at least some means of effective computation. The hope for effective computation is associated with classical method of Chabauty and Coleman [3], which the study of the unipotent Albanese map generalizes. The related issue of structural understanding, on the other hand, should concern an implication of the form

control of L-values $\Rightarrow$ control of Selmer varieties

following a pattern familiar from the theory of elliptic curves ([2], [25]).

It should be admitted right away that our current intuition for the nature of such an implication is in a very tentative state. Nevertheless, the cases studied previously of hyperbolic curves of genus zero and one seem to suggest that our expectations are not entirely without ground.

The purpose of the present paper is to augment our list of examples where something can be worked out with the case where J is isogenous over $\bar{\mathbb{Q}}$ to a product

$$J \sim \prod_i A_i$$

of abelian varieties A_i that have complex multiplication by CM fields K_i of degree $2\mathrm{dim}A_i$. For this discussion we choose the prime p to further satisfy the condition that p is split in the compositum K of the fields K_i, and hence, in each field K_i.

Let $\mathbb{Q}_T$ be the maximal extension of $\mathbb{Q}$ unramified outside $T = S \cup \{p, \infty\}$ and $G_T = \mathrm{Gal}(\mathbb{Q}_T/\mathbb{Q})$. Now let

$$W = U/[U^2, U^2]$$

be the quotient of U by the third level of its derived series and let

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

Of course W itself has a descending central series

$$W = W^1 \supset W^2 \supset \cdots \supset W^{n+1} = [W, W^n] \supset \cdots$$

and associated quotients $W_n = W/W^{n+1}$.

Theorem 0.1 *There is a constant B (depending on X and T) such that*

$$dim \sum_{i=1}^{n} H^2(G_T, W^i/W^{i+1}) \leq Bn^{2g-1}.$$

We will derive this inequality as a rather elementary consequence of multi-variable Iwasawa theory. The key point is to control the distribution of zeros of a *reduced algebraic p-adic L-function* of sorts, namely an annihilator of a natural ideal class group.

In accordance with the 'motivic nature' of the construction, W also has a De Rham realization

$$W^{DR} = U^{DR}/[(U^{DR})^2, (U^{DR})^2]$$

over $\mathbb{Q}_p$, endowed with a Hodge filtration. The upper bound of theorem 0.1 combines with an easy linear independence argument for sufficiently many elements in $(W^{DR})^n/(W^{DR})^{n+1}$, yielding a lower bound for the De Rham realization

$$W_n^{DR}/F^0$$

of its local Selmer variety. We obtain thereby the easy but important corollary:

Corollary 0.2 *For n sufficiently large, we have the bound*

$$dim H^1_f(G, W_n) < dim W_n^{DR}/F^0.$$

Of course, this implies:

Corollary 0.3 *(Faltings' theorem, special case.) $X(\mathbb{Q})$ is finite.*

For explicit examples where the hypothesis is satisfied, we have of course the Fermat curves

$$x^m + y^m = z^m$$

for $m \geq 4$ ([26], VI, Satz 1.2, Satz 1.5), but also the twisted Fermat curves

$$ax^m + by^m = cz^m$$

for $a, b, c, \in \mathbb{Q} \setminus \{0\}$, $m \geq 4$. One might hope (optimistically) that the methods of this paper will eventually lead to some effective understanding of these twists. Some relatively recent examples of hyperelliptic curves with CM Jacobians can be found in [30]. One from the list there is

$$y^2 = -243x^6 + 2223x^5 - 1566x^4 - 19012x^3 + 903x^2 + 19041x - 5882$$

whose Jacobian has CM by

$$\mathbb{Q}(\sqrt{-13 + 3\sqrt{13}}).$$

The results here conclude the crude application of Selmer varieties to finiteness over $\mathbb{Q}$ in situations where the controlling Galois group of the base is essentially abelian. It remains then to work out the appropriate interaction between non-commutative geometric fundamental groups and the non-commutative Iwasawa theory of number fields.

Of course, as far as a refined study of defining ideals for the image of $D \circ \mathrm{loc}_p$ is concerned, work of any serious nature has not yet commenced. In this regard, we note that there is little need in this paper for specific information about the annihilator that occurs in the proof of theorem 0.1. However, it is our belief that structure theorems of the 'Iwasawa main conjecture' type will have an important role to play in eventual refinements of the theory.

1 Preliminaries on complex multiplication

Let $F/\mathbb{Q}$ be a finite extension with the property that the isogeny decomposition

$$J \sim \prod_i A_i$$

as well as the complex multiplication on each A_i are defined over F. We assume further that $F \supset \mathbb{Q}(J[4p])$, so that $F_\infty := F(J[p^\infty])$ has Galois group $\Gamma \simeq \mathbb{Z}_p^r$ over F. Denote by $G_{F,T}$, the Galois group $\mathrm{Gal}(\mathbb{Q}_T F/F)$.

As a representation of $G_{F,T}$, we have

$$V := T_pJ \otimes \mathbb{Q}_p \simeq \oplus_i V_i$$

where

$$V_i := T_pA_i \otimes \mathbb{Q}_p.$$

Let m be a modulus of F that is divisible by the conductor of all the representations V_i. Each factor representation

$$\rho_i : G_{F,T} \rightarrow (K_i \otimes \mathbb{Q}_p)^* \subset \mathrm{Aut}(V_i)$$

corresponds to an algebraic map

$$f_i : S_m \rightarrow \mathrm{Res}_{\mathbb{Q}}^{K_i}(\mathbb{G}_m),$$

where S_m is the Serre group of F with modulus m ([29], II) and $\mathrm{Res}_{\mathbb{Q}}^{K_i}$ is the restriction of scalars from K_i to $\mathbb{Q}$. That is, there is a universal representation (op. cit. II.2.3)

$$\epsilon_p : G_{F,T} \rightarrow S_m(\mathbb{Q}_p)$$

such that

$$\rho_i = f_i \circ \epsilon_p : G_{F,T} \longrightarrow S_m(\mathbb{Q}_p) \longrightarrow \mathrm{Res}_{\mathbb{Q}}^{K_i}(\mathbb{G}_m)(\mathbb{Q}_p) = (K_i \otimes \mathbb{Q}_p)^*.$$

Since we have chosen p to split in each K_i, we have

$$\mathrm{Res}_{\mathbb{Q}}^{K_i}(\mathbb{G}_m) \otimes \mathbb{Q}_p \simeq \prod [\mathbb{G}_m]_{\mathbb{Q}_p}.$$

Each of the algebraic characters

$$f_{ij} = pr_j \circ \rho_i : [S_m]_{\mathbb{Q}_p} \longrightarrow [\mathrm{Res}_{\mathbb{Q}_p}^{K_i}(\mathbb{G}_m)]_{\mathbb{Q}_p} \simeq \prod [\mathbb{G}_m]_{\mathbb{Q}_p} \xrightarrow{pr_j} [\mathbb{G}_m]_{\mathbb{Q}_p}$$

correspond to Galois characters

$$\chi_{ij} = f_{ij} \circ \epsilon_p : G_{F,T} \rightarrow \mathbb{Q}_p^*$$

in such a way that

$$\rho_i \simeq \oplus_j \chi_{ij}.$$

Recall that S_m fits into an exact sequence

$$0 \rightarrow T_m \rightarrow S_m \rightarrow C_m \rightarrow 0$$

with C_m finite and T_m an algebraic torus (op. cit. II.2.2). Hence, there is an integer N such that the kernel and cokernel of the restriction map on characters

$$X^*([S_m]_{\mathbb{Q}_p}) \rightarrow X^*([T_m]_{\mathbb{Q}_p})$$

is killed by N. On the other hand, $X^*([T_m]_{\mathbb{Q}_p})$ is a finitely generated torsion free abelian group. Let $\{\beta'_1, \ldots, \beta'_d\}$ be a basis for the subgroup of $X^*([T_m]_{\mathbb{Q}_p})$ generated by the restrictions $f_{ij}|[T_m]_{\mathbb{Q}_p}$ as we run over all i and j. Then the set $\{(\beta'_1)^N, \ldots, (\beta'_d)^N\}$ can be lifted to characters $\{\beta_1, \ldots, \beta_d\}$ of $[S_m]_{\mathbb{Q}_p}$ so that each $f_{ij}^{N^2}$ is a product

$$f_{ij}^{N^2} = \prod_k \beta_k^{n_{ijk}}$$

for integers n_{ijk}. For ease of notation, we will now change the indexing and write $\{f_1, \ldots, f_{2g}\}$ for the set of f_{ij} and $\{\chi_i\}_{i=1}^{2g}$ for the characters of $G_{F,T}$ that they induce. We have shown that there are integers n_{ij} such that

$$f_i^{N^2} = \prod_j \beta_j^{n_{ij}}.$$

Thus, if we denote by ξ_i the character

$$\beta_i \circ \epsilon_p : G_{F,T} \rightarrow \mathbb{Q}_p^*,$$

then

$$\chi_i^{N^2} = \prod_j \xi_j^{n_{ij}}.$$

Lemma 1.1 *The characters ξ_i are $\mathbb{Z}_p$-linearly independent.*

Proof. The image of the map $\epsilon_p : G_{F,T} \rightarrow S_m(\mathbb{Q}_p)$ contains an open subgroup O_m of $T_m(\mathbb{Q}_p)$ ([29] II.2.3, Remark). Suppose

$$\prod \xi_i^{a_i} = 1$$

for some $a_i \in \mathbb{Z}_p$ as a function on $G_{F,T}$ (and, say, the choice of p-adic log such that $\log(p) = 0$). Then

$$\prod_i \beta_i^{a_i} = 1$$

as a function on O_m. Since the $\beta_i|[T_m]_{\mathbb{Q}_p} = (\beta_i')^N$ are $\mathbb{Z}$-linearly independent, for each j, there exists a cocharacter

$$c_j : [\mathbb{G}_m]_{\mathbb{Q}_p} \rightarrow [T_m]_{\mathbb{Q}_p}$$

such that $\beta_i \circ c_j = 1$ for $i \neq j$ and

$$\beta_j \circ c_j : [\mathbb{G}_m]_{\mathbb{Q}_p} \rightarrow [\mathbb{G}_m]_{\mathbb{Q}_p}$$

is non-trivial, and hence, an isogeny. But $c_j^{-1}(O_m)$ is an open subgroup of $\mathbb{Q}_p^*$. Hence, it contains an element of the form $x = 1 + p^n u$, with $n > 0$ and $u \in \mathbb{Z}_p^*$. Therefore, $c = \beta_j(c_j(x)) \in 1 + p\mathbb{Z}_p$ also has infinite order and $c^{a_j} = 1$. Therefore, we get $a_j = 0$. □

Since the kernel of

$$\rho = \oplus_j \rho_j = \oplus_{i=1}^{2g} \chi_i$$

is the same as that of $\xi := \oplus_{i=1}^{d} \xi_i$, ξ maps Γ isomorphically to a subgroup of $\oplus_{i=1}^{d}(1 + p\mathbb{Z}_p)$ of finite-index. After enlarging F if necessary, we can assume that there is a basis $\{\gamma_1, \ldots, \gamma_d\}$ for Γ such that $\xi_i(\gamma_j) = 1$ for $j \neq i$ and $\xi_i(\gamma_i)$ is a generator for $\xi_i(G_{F,T})$, which we can take to be a fixed element $g \in \mathbb{Z}_p*$. Here, we abuse notation a bit and write ξ_i for the character of $G_{F,T}$ as well as that of the quotient group Γ that it induces.

In the following, for any character ϕ, we will frequently use the notation 'ϕ' for the one-dimensional vector space $\mathbb{Q}_p(\phi)$ on which $G_{F,T}$ acts via ϕ, as well as for the character itself. Choose a basis

$$B = \{e_1, e_2, \ldots, e_{2g}\}$$

of V so that e_i is a basis of $\mathbb{Q}_p(\chi_i)$. Write ψ_i for the dual of χ_i.

Note that over F, the abelian variety J has good reduction everywhere [28].

2 Preliminaries on dimensions

For a (pro-algebraic) group or a Lie algebra A, we define the descending central series by

$$A^1 = A; \quad A^{n+1} = [A, A^n]$$

and the derived series by

$$A^{(1)} = A; \quad A^{(n+1)} = [A, A^{(n)}].$$

The corresponding quotients are denoted by

$$A_n := A/A^{n+1}$$

and

$$A_{(n)} := A/A^{(n+1)}.$$

Also, we denote by

$$Z_n(A) := A^n/A^{n+1}$$

the associated graded objects so that we have an exact sequence

$$0 \rightarrow Z_n(A) \rightarrow A_n \rightarrow A_{n-1} \rightarrow 0.$$

Denote by

$$Z(A) := \sum_{n=1}^{\infty} Z_i(A)$$

the associated graded Lie algebra, described in [27], II.1, in the case of a group.

According to [23], Appendix 3, the $\mathbb{Q}$-pro-unipotent completion of a finitely-presented discrete group E can be constructed as follows: take the group algebra $\mathbb{Q}[E]$, and complete it with respect to the augmentation ideal K:

$$\mathbb{Q}[[E]] := \varprojlim_n \mathbb{Q}_p[E]/K^n.$$

Since the co-product

$$\Delta : \mathbb{Q}_p[E] \rightarrow \mathbb{Q}_p[E] \otimes \mathbb{Q}_p[E]$$

defined by sending an element $g \in E$ to

$$g \otimes g \in \mathbb{Q}[E] \otimes \mathbb{Q}[E]$$

takes K to the ideal

$$K \otimes \mathbb{Q}[E] + \mathbb{Q}[E] \otimes K,$$

there is an induced co-product

$$\Delta : \mathbb{Q}[[E]] \longrightarrow \mathbb{Q}[[E]] \hat{\otimes} \mathbb{Q}[[E]] := \varprojlim{}_n (\mathbb{Q}[[E]] \otimes \mathbb{Q}[[E]])/(K \otimes \mathbb{Q}[E] + \mathbb{Q}[E] \otimes K)^n.$$

The unipotent completion $U(E)$ can be realized as the group like elements in $\mathbb{Q}[[E]]$:

$$U(E) = \{g \in \mathbb{Q}[[E]] \ \mid \ \Delta(g) = g \otimes g\}.$$

This turns out to define the $\mathbb{Q}$-points of a pro-algebraic group over $\mathbb{Q}$. Its Lie algebra, $LieU(E)$, consists of the primitive elements

$$LieU(E) = \{X \in \mathbb{Q}[[E]] \ \mid \ \Delta(X) = X \otimes 1 + 1 \otimes X\}.$$

For any element $g \in U(E)$,

$$\log(g) = (g-1) - (g-1)^2/2 + (g-1)^3/3 - \cdots$$

defines an element of $LieU(E)$, and an elementary computation starting from

$$\Delta(g-1) = (g-1) \otimes 1 + 1 \otimes (g-1) + (g-1) \otimes (g-1)$$

shows that $\log(g) \in LieU(E)$. In fact, this map is a bijection (loc. cit.)

$$\log : U(E) \simeq LieU(E).$$

When E is a topologically finitely presented pro-finite group, the $\mathbb{Q}_p$-pro-unipotent completion $U_{\mathbb{Q}_p}(E)$ is defined in an entirely analogous manner, except that the group algebra $\mathbb{Q}_p[[E]]$ is defined somewhat differently: First, let E^{pro-p} be the maximal pro-p quotient of E, and let

$$\mathbb{Z}_p[[E^{pro-p}]] := \varprojlim_N \mathbb{Z}_p[E^{pro-p}/N],$$

where N runs over the normal subgroups of E^{prop} of finite-index, be its Iwasawa algebra. Then

$$\mathbb{Q}_p[[E]] = \varprojlim_n [(\mathbb{Z}_p[[E^{pro-p}]]/K^n) \otimes \mathbb{Q}_p],$$

where $K \subset \mathbb{Z}_p[[E^{pro-p}]]$ again denotes the augmentation ideal. Then

$$U_{\mathbb{Q}_p}(E) \subset \mathbb{Q}_p[[E]]$$

and its Lie algebra are defined exactly as above. Consider the category $\mathrm{Un}(E, \mathbb{Q}_p)$ of unipotent continuous $\mathbb{Q}_p$-representations of E, that is, finite-dimensional continuous representations

$$\rho : E \rightarrow \mathrm{Aut}(M)$$

that possess a filtration

$$M = M^0 \supset M^1 \supset M^2 \supset \cdots$$

such that each M^i/M^{i+1} is a direct sum of the copies of the trivial representation. We see that U acting on the left on $\mathbb{Q}_p[[E]]/K^n$ turns the system $\{\mathbb{Q}_p[[E]]/K^n\}$ into a pro-object of $\mathrm{Un}(E, \mathbb{Q}_p)$. Given any pair (M, m) where M is a continuous unipotent $\mathbb{Q}_p$-representation of E and $m \in M$, there is a unique map of pro-representations

$$(\mathbb{Q}_p[[E]], e) \rightarrow (M, m)$$

where $e \in \mathbb{Q}_p[[E]]$ comes from the identity of E, making the pair $(\mathbb{Q}_p[[E]]/K^n, e)$ universal among such pairs. Therefore, if we let

$$F : \mathrm{Un}(E, \mathbb{Q}_p) \longrightarrow \mathrm{Vect}_{\mathbb{Q}_p}$$

be the forgetful functor from the category of unipotent continuous $\mathbb{Q}_p$-representations of E to the category of finite-dimensional $\mathbb{Q}_p$-vectors spaces, the map

$$f \mapsto fe \in \mathbb{Q}_p[[E]]$$

defines an isomorphism

$$\mathrm{End}(F) \simeq \mathbb{Q}_p[[E]].$$

Meanwhile, the condition of being group-like corresponds to the compatibility with tensor products [5], so that we have

$$U_{\mathbb{Q}_p}(E) = \mathrm{Aut}^{\otimes}(F),$$

the tensor-compatible automorphisms of F.

Since it will be our main object of interest, we denote simply by U the $\mathbb{Q}_p$-pro-unipotent completion of the pro-finite fundamental group $\pi_1^{et}(\bar{X}, b)$ of $\bar{X}$ with base-point at b. Fix a rational tangent vector $v \in T_b X$, and let $X' = X \setminus \{b\}$. Let

$$U' := \pi_1^{\mathbb{Q}_p, un}(\bar{X}', v),$$

the $\mathbb{Q}_p$-pro-unipotent completion of the profinite fundamental group of $\bar{X}'$ with tangential base-point at v as defined in [4]. These groups come with corresponding Lie algebras $L' =: LieU'$ and $L := LieU$.

Let

$$\mathrm{Un}(\bar{X}, \mathbb{Q}_p)$$

be the category of unipotent lisse sheaves on the étale site of $\bar{X}$. Then the fiber functor

$$F_b : \mathrm{Un}(\bar{X}, \mathbb{Q}_p) \rightarrow \mathrm{Vect}_{\mathbb{Q}_p},$$

which associates to any sheaf $\mathcal{F}$ its stalk $\mathcal{F}_b$, factors through the tensor equivalence of categories

$$\mathrm{Un}(\bar{X}, \mathbb{Q}_p) \simeq \mathrm{Un}(\pi_1^{et}(\bar{X}, b), \mathbb{Q}_p) \overset{F}{\rightarrow} \mathrm{Vect}_{\mathbb{Q}_p},$$

so that we also have

$$U = \mathrm{Aut}^{\otimes}(F_b).$$

Similarly,

$$U' = \mathrm{Aut}^{\otimes}(F'_b),$$

where

$$F'_b : \mathrm{Un}(\bar{X}', \mathbb{Q}_p) \rightarrow \mathrm{Vect}_{\mathbb{Q}_p}$$

is again the fiber functor defined by stalks.

As explained in [11], Appendix A, there are natural isomorphisms

$$U' \simeq U'_B \otimes \mathbb{Q}_p$$

and

$$U \simeq U_B \otimes \mathbb{Q}_p,$$

where U'_B and U_B denote the $\mathbb{Q}$-unipotent completions of the topological fundamental groups $\pi' = \pi_1(X(\mathbb{C}), v)$ and $\pi = \pi_1(X(\mathbb{C}), b)$ of $X'(\mathbb{C})$ and $X(\mathbb{C})$. (Appendix A of op. cit. is recommended in general for background on pro-unipotent completions, while its section 2 contains a nice discussion of pro-algebraic groups.) Therefore, $L'_B =: LieU'_B$, and $L_B := LieU_B$ also satisfy comparison isomorphisms

$$L' \simeq L'_B \otimes \mathbb{Q}_p$$

and

$$L \simeq L_B \otimes \mathbb{Q}_p.$$

The natural maps

$$\pi' \longrightarrow U'_B$$

and

$$\pi \longrightarrow U_B$$

induce isomorphisms

$$Z(\pi') \otimes \mathbb{Q} \simeq Z(U'_B)$$

and

$$Z(\pi) \otimes \mathbb{Q} \simeq Z(U_B).$$

(See, for example, [1], Prop. 1.2. In that reference, real coefficients are used. But this obviously implies that same result for $\mathbb{Q}$-coefficients.) On the other hand, the bijections

$$\log : U'_B \rightarrow L'_B$$

and

$$\log : U_B \rightarrow L_B$$

take $ghg^{-1}h^{-1}$ to $[\log g, \log h]$ modulo higher commutators by the Baker-Campbell-Hausdorff formula ([27], Chap. 4). Hence, there is a bijection of the descending central series filtrations on the two sides, and the brackets agree modulo terms of higher order. Therefore, the log map also induces isomorphisms

$$Z(U'_B) \simeq Z(L'_B)$$

and

$$Z(U_B) \simeq Z(L'_B),$$

this time respecting the brackets. From this, we also get

$$Z(\pi') \otimes \mathbb{Q}_p \simeq Z(L')$$

and

$$Z(\pi) \otimes \mathbb{Q}_p \simeq Z(L).$$

It follows from this that $Z(L')$ is the free Lie algebra on $2g$ generators. Hence, L' is free on generators obtained from any lift of a basis for $(L')_1 = V$. That is, we can take a lift $\tilde{S}$ of any basis S for V, then the map

$$F(\tilde{S}) \rightarrow L'$$

from the free Lie algebra on $\tilde{S}$ to L' induces isomorphisms

$$F(\tilde{S})/F(\tilde{S})^n \simeq L'/(L')^n$$

for each n, and hence, an isomorphism

$$\overline{F(\tilde{S})} := \{F(\tilde{S})/F(\tilde{S})^n\}_n \simeq L'$$

of pro-Lie algebras. (See, for example, [11], appendix A again.) As generators for L', we take a lifting $\tilde{B} = \{\tilde{e}_1, \cdots, \tilde{e}_{2g}\}$ of the basis B above. The corresponding isomorphism from $\overline{F(\tilde{B})}$ to L' puts on L' the structure of a graded pro-Lie algebra

$$L' = \oplus_{n=1}^{\infty} L'(n)$$

in such a way that

$$(L')^n = \oplus_{i\geq n}^{\infty} L'(i).$$

We warn the reader that this grading is *not* compatible with the Galois action. Since there appears to be little danger of confusion, we will denote the elements $\tilde{e}_i$ by e_i again and the generating set $\tilde{B}$ by B.

By [19], the natural map

$$\pi' \to \pi$$

induces an isomorphism

$$(Z(\pi') \otimes \mathbb{Q})/\bar{R}_B \simeq Z(\pi) \otimes \mathbb{Q}$$

for a Lie ideal $\bar{R}_B$ generated by the class of a single element $c := \prod_i [a_i, b_i] \in (\pi')^2$, expressed in terms of a set of free generators $\{a_1, \ldots, a_g, b_1, \ldots, b_g\}$ for π'. Consider the natural map

$$p : L' \to L.$$

We have $\omega := \log(c) \in Ker(p)$, and the preceding discussion implies that

$$L'/R \simeq L,$$

where R is the closed ideal generated by ω, since there is induced an isomorphism of associated graded algebras.

For the structure of $N := LieW$, we have therefore

$$N \simeq L'/[I + R],$$

where

$$I = (L')^{(3)} = [[L', L'], [L', L']].$$

According to [24], we can construct a Hall basis for L' as follows. First, we order B so that $e_i < e_j$ if $i < j$. This is, by definition, the set H_0. Now define H_{n+1} recursively as the brackets of the form

$$[\ldots[h_1, h_2], h_3], \ldots], h_k]$$

where $k \geq 2$, $h_i \in H_n$, and

$$h_1 < h_2 \geq h_3 \geq \cdots h_k.$$

Now choose a total order on H_{n+1}. Finally, put $H = \cup_i H_i$ and extend the order by the condition

$$h \in H_i, \quad k \in H_j, \quad i < j \quad \Rightarrow h > k.$$

Symbolically,

$$H_0 > H_1 > H_2 > \cdots.$$

In fact, it is shown that $\cup_{i\geq n}H_i$ is a Hall basis for the subalgebra

$$(L')^{(n+1)}.$$

In particular, it follows that the elements of H_1 are linearly independent from $(L')^{(3)}$, which is generated by $\cup_{i\geq 2}H_i$. Furthermore, the basis consists of monomials, so that $H(i) := H \cap L'(i)$ is a basis for $L'(i)$. Define $H_n(i) := H_n \cap L'(i)$ so that $H(i) = \cup_n H_n(i)$. We thus get a bigrading

$$L' = \oplus L'(i,n),$$

where $L'(i,n)$ is the span of $H_n(i)$.

Denote by N' the Lie algebra

$$(L')_{(2)} = L'/I.$$

Then

Lemma 2.1 *For $n \geq 2$, the set $H_1(n)$, consisting of Lie monomials of the form*

$$[[\ldots[e_{i_1}e_{i_2}]e_{i_3}]\ldots]e_{i_n}],$$

where $i_1 < i_2 \geq i_3 \geq \cdots \geq i_n$, is linearly independent from

$$(L')^{(n+1)} + I.$$

Proof. We have the bigradings

$$I = \oplus_{i=1}^{\infty} \oplus_{j\geq 2} L_(i,j)$$

$$(L')^{(n+1)} = \oplus_{i\geq n+1} \oplus_{j=1}^{\infty} L(i,j),$$

from which it is clear that $(L')^{(n+1)} + I$ is the sum of $L'(i,j)$ where (i,j) runs over the pairs such that $j \geq 2$ or $i \geq n+1$. Thus, $H_1(n)$ is linearly independent from it. □

Corollary 2.2 *The image $[H_1(n)]$ of $H_1(n)$ in N'_n is a basis for $Z_n(N')$.*

The elements of $H_1(n)$ for $n \geq 2$ can be counted by noting that there are $\binom{2g}{2}$ possibilities for the bracket $[e_{i_1}, e_{i_2}]$, while for each such bracket, the cardinality of the non-increasing $(i_3, i_4, \ldots, i_n)$ with $i_3 \leq i_2$ is

$$\binom{(n-2)+(i_2-1)}{i_2-1} = \binom{n-3+i_2}{i_2-1}.$$

So we find the following dimension formula:

Corollary 2.3 *For $n \geq 2$,*

$$dim Z_n(N') = \sum_{i=1}^{2g} (i-1)\binom{n-3+i}{i-1}.$$

Proof. This follows immediately from the previous discussion together with the observation that for any index i, there are $i-1$ possibilities for the bracket $[e_j, e_i]$ at the beginning of an element of $H_1(n)$. □

We would like to understand the dimension of $Z_n(N)$. Although it would be elementary work out a precise formula, we need just a reasonable estimate for our purposes. That is, we need to estimate the dimension of

$$Z_n(N')/[Z_n(N') \cap Im(R)],$$

where $Im(R)$ refers to the ideal in N'_n generated by the image of ω (which we will again denote by ω).

For an ordered collection of elements $v = (x_1, x_2, \dots, x_m) \in B^m$ and an element $y \in L'$, define

$$\mathrm{ad}_v(y) := [[\dots[y, x_1], x_2], \dots, x_m]$$

Note that if $y \in (L')^2$ and v' is a re-ordering of v, then

$$\mathrm{ad}_v(y) - \mathrm{ad}_{v'}(y) \in I$$

Thus, for $y \in (L')^2$, we have

$$\mathrm{ad}_v(y) \equiv \mathrm{ad}_{\mathrm{ord}(v)}(y) \quad \mod \ I$$

where $\mathrm{ord}(v)$ is the unique reordering of v for which the components are non-increasing. Hence, any $x \in R \cap L'(n)$ has an expression as a linear combination

$$x \equiv \sum_i c_i \mathrm{ad}_{v_i}(\omega) \qquad \mod I,$$

where v_i runs through elements of B^{n-2} with non-increasing components. The number of such v_i is

$$\binom{n-2+2g-1}{2g-1} = \binom{n-3+2g}{2g-1},$$

which therefore gives an upper bound on the dimension of $Im(R) \cap Z_n(N')$.

Lemma 2.4 *For $n \geq 2$,*

$$dim Z_n(N) \geq (2g-2)\binom{n-3+2g}{2g-1} + \sum_{i=1}^{2g-1}(i-1)\binom{n-3+i}{i-1}$$

3 Proofs

We refer to [14] and [15], section 2, for general background material on Selmer varieties. Recall that

$$H^1_f(G, W_n) \subset H^1(G_T, W_n)$$

consists of the cohomology classes corresponding to W_n-torsors that are unramified outside T and crystalline at p. So a bound for $H^1(G_T, W_n)$ will be a bound for $H^1_f(G_T, W_n)$ as well.

We will use again the exact sequence

$$0 \to H^1(G_T, Z_n(W)) \to H^1(G_T, W_n) \to H^1(G_T, W_{n-1})$$

as in op. cit. and a bound for the dimension of $H^1(G_T, Z_n(W))$. There is, as usual, the Euler characteristic formula [12] that reduces over $\mathbb{Q}$ to

$$\mathrm{dim} H^0(G_T, Z_n(W)) - \mathrm{dim} H^1(G_T, Z_n(W)) + \mathrm{dim} H^2(G_T, Z_n(W)) = \mathrm{dim}[Z_n(W)]^+ - \mathrm{dim}[Z_n(W)]$$

$$= -\mathrm{dim}[Z_n(W)]^-,$$

where the signs in the superscript refer to the ±1 eigenspaces for the action of complex conjugation. Because $Z_n(W)$ has weight n, we see that the H^0-term is zero for $n \geq 1$, from which we get

$$(EC) \qquad \mathrm{dim} H^1(G_T, Z_n(W)) = \mathrm{dim}[Z_n(W)]^- + \mathrm{dim} H^2(G_T, Z_n(W)).$$

Note that if $T' \supset T$, then

$$\mathrm{dim} H^1(G_{T'}, W_n) \geq \mathrm{dim} H^1(G_T, W_n).$$

The Euler characteristic formula then shows that

$$\dim H^2(G_{T'}, W_n) \geq \dim H^2(G_T, W_n)$$

as well. Therefore, in our discussion of bounds, we may increase the size of T to include the primes that ramify in the field F. In particular, we may assume that $F \subset \mathbb{Q}_T$ so that

$$G_{F,T} \subset G_T,$$

a subgroup of finite index.

Proof of theorem 0.1 Since there is a constant in the formula, we can assume $n \geq 3$. Furthermore, by the surjectivity of the corestriction map

$$H^2(G_{F,T}, Z_n(N)) \rightarrow H^2(G_T, Z_n(N)),$$

we may concentrate on bounding $H^2(G_{F,T}, Z_n(N))$. As in [17], we consider the localization sequence

$$0 \rightarrow Ш^2(Z_n(N)) \rightarrow H^2(G_{F,T}, Z_n(N)) \rightarrow \oplus_{v|T} H^2(G_v, Z_n(N)),$$

where $G_v = \mathrm{Gal}(\bar{F}_v/F_v)$. For the local terms, we have Tate duality

$$H^2(G_v, Z_n(N)) \simeq (H^0(G_v, Z_n(N)^*(1)))^*.$$

For $v \nmid p$, since J has good reduction, the action of G_v on $Z_n^*(N)(1))$ is unramified. But then, for $n \geq 3$, $Z_n(N)^*$ has Frobenius weight ≥ 3, while $\mathbb{Q}_p(1)$ has Frobenius weight -2. Therefore,

$$H^0(G_v, Z_n(N)^*(1)) = 0.$$

For $v|p$, we use instead the fact ([7], theorem 5.2) that

$$H^0(H_v, Z_n(N)^*(1)) = \mathrm{Hom}_{MF(\phi)}(F_v^{nr}, D_{cris}(Z_n(N)^*(1))).$$

Here, F_v^{nr} is the maximal absolutely unramified subextension of F_v and $D_{cris}(\cdot) = ((\cdot) \otimes B_{cris})^{G_v}$ is Fontaine's crystalline Dieudonné functor applied to crystalline G_v-representations, while $MF(\phi)$ is the category of admissible filtered ϕ-modules over F_v^{nr} (op. cit., section 5.1). Since each character ψ_i occurs inside $H^1_{et}(\bar{J}, \mathbb{Q}_p)$, we know that $D_{cr}(\psi_i)$ occurs inside the crystalline cohomology $H^1_{cr}(J, \mathbb{Q}_p)$ ([8]). But then, if the residue field of F_v is of degree d over $\mathbb{F}_p$, ϕ^d again has positive weights on $D_{cris}(Z_n^*(N)(1))$ ([13]). Therefore, $H^0(G_v, Z_n^*(N)(1)) = 0$. It follows that

$$H^2(G_v, Z_n(N)) \simeq Ш^2(Z_n(N)) \simeq [Ш^1(Z_n(N)^*(1))]^*$$

by Poitou-Tate duality ([20], theorem 4.10), where $Ш^1(Z_n(N)^*(1))$ is defined by the exact sequence

$$0 \rightarrow Ш^1(Z_n(N)^*(1)) \rightarrow H^1(G_{F,T}, Z_n(N)^*(1)) \rightarrow \oplus_{v|T} H^1(G_v, Z_n(N)^*(1)).$$

Now, the group $\Gamma = \mathrm{Gal}(F_\infty/F)$ is the image of $G_{F,T}$ inside $\mathrm{Aut}(J[p^\infty])$, and $Z_n(N)^*(1)$, being a sum of tensor products of the characters $\psi_i = \chi_i^*$ and $\mathbb{Q}_p(1)$, is a direct summand of $(V^*)^{\otimes n}(1)$. Hence, by Bogomolov's theorem (as in op. cit. Lemma 6.20, Lemma 6.21),

$$H^1(\Gamma, Z_n(N)^*(1)) = 0.$$

Therefore, using the Hochschild-Serre sequence, we get

$$H^1(G_T, Z_n(N)^*(1)) \subset \mathrm{Hom}_\Lambda(\mathcal{X}_T, Z_n(N)^*(1))$$

for

$$\Lambda := \mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T_1, T_2, \ldots, T_d]]$$

and $\mathcal{X}_T = \mathrm{Gal}(K_T/F_\infty)$, the Galois group of the maximal abelian pro-p extension K_T of F_∞ unramified outside T. Here, $T_i = \gamma_i - 1$ for free generators γ_i of Γ chosen as in section 1 so that $\xi_i(\gamma_j) = 1$ while $\xi_i(\gamma_i)$ is a generator for the image of $\xi_i(G_{F,T})$. The condition of belonging to the kernel of the localization map will, in any case, imply

$$Ш^1(Z_n(N)^*(1)) \subset \mathrm{Hom}_\Lambda(M, Z_n(N)^*(1)) = \mathrm{Hom}_\Lambda(M(-1), Z_n(N)^*),$$

where $M = M'/(\mathbb{Z}_p - \text{torsion})$ for the Galois group $M' = \mathrm{Gal}(H'/F_\infty)$ of the p-Hilbert class field H' of F_∞. (Of course, we could take an even smaller Galois group.) According to [9], M', and hence M, is a torsion Λ-module. (That reference states this in the case where F_∞ is replaced by the compositum of all $\mathbb{Z}_p$-extensions of F, but the proof clearly applies to any $\mathbb{Z}_p^r$-extension.) According to a lemma of Greenberg ([10], Lemma 2), there is a subgroup $P \subset \Gamma$ such that $\Gamma/P \simeq \mathbb{Z}_p$ and M is still finitely generated over $\mathbb{Z}_p[[P]]$. Consequently, as explained in op. cit., page 89, if we choose a basis $\{\epsilon_1, \ldots, \epsilon_{d-1}\}$ for P and complete it to a basis of Γ using an element ϵ_d that maps to a topological generator of $\mathbb{Z}_p$, then in the variables $S_i = \epsilon_i - 1$, we can take the annihilator to have the form

$$f = b_0(S_1, \ldots, S_{d-1}) + b_1(S_1, \ldots, S_{d-1})S_d + \cdots + b_{l-1}(S_1, \ldots, S_{d-1})S_d^{l-1} + S_d^l$$

for some power series b_i. Furthermore, by approximation, we can choose the ϵ_i to be of the form

$$\epsilon_i = \gamma_1^{n_{i1}} \cdots \gamma_d^{n_{i,d}}$$

for integers n_{ij}. That is, if the original P involved p-adic powers n_{ij}, we can approximate them by integral n'_{ij} that are p-adically close, defining another subgroup P'. If the $S \subset M$ is a generating set as a $\mathbb{Z}_p[[N]]$ module, then we see that $\mathbb{Z}_p[[P]]S = \mathbb{Z}_p[[P']]S \bmod pM$, and hence, that $\mathbb{Z}_p[[P']]S = M$ as well.

We know that $Z_n(N)$ is generated by the image of $H_1(n)$. So $Z_n(N)^*$ is a subspace of the $G_{F,T}$-representation given as the direct sum of the one-dimensional representations

$$\psi_{i_1} \otimes \psi_{i_2} \otimes \psi_{i_3} \otimes \cdots \otimes \psi_{i_n},$$

where i_i run over indices from $\{1, 2, \ldots, 2g\}$ such that

$$i_1 < i_2 \geq i_3 \geq \cdots \geq i_n.$$

So this is of the form

$$\oplus_{i<2g}[\psi_i \otimes \psi_{2g} \otimes \mathrm{Sym}^{n-2}(V^*)] \oplus K_n$$

where

$$\mathrm{dim} K_n \leq \binom{2g}{2}\binom{n-2+2g-2}{2g-2} = O(n^{2g-2}).$$

Therefore, the representation

$$\oplus_{i=3}^n Z_i(N)^*$$

is of the form

$$\oplus_{i<2g}[\psi_i \otimes \psi_{2g} \otimes (\oplus_{i=1}^{n-2}\mathrm{Sym}^i(V))] + R_n$$

where R_n has dimension $\leq An^{2g-1}$ for some constant A. Clearly, $\mathrm{dim} H^2(G_T, R_n) \leq A'n^{2g-1}$ for another constant A'. So we need to find a good bound for

$$\mathrm{Hom}_\Lambda(M(-1), \oplus_{i<2g}[\psi_i \otimes \psi_{2g} \otimes (\oplus_{i=1}^{n-2}\mathrm{Sym}^i(V))]).$$

We use the multi-index notation

$$\underline{\psi}^\alpha = \psi_1^{\alpha_1}\psi_2^{\alpha_2} \cdots \psi_{2g}^{\alpha_{2g}}$$

for a multi-index $\alpha = (\alpha_1, \ldots, \alpha_{2g}) \in \mathbb{N}^{2g}$. The weight of the multi-index α is denoted $|\alpha| := \sum_i \alpha_i$ so that

$$\mathrm{Sym}^i(V) = \oplus_{|\alpha|=i}\underline{\psi}^\alpha.$$

If a component

$$\mathrm{Hom}_\Lambda(M(-1), \psi_i \otimes \psi_{2g} \otimes \psi^\alpha) = \mathrm{Hom}_\Lambda(M(-1) \otimes \chi_i \otimes \chi_{2g}, \psi^\alpha)$$

is non-zero, then we must have

$$\psi^\alpha(f_i) = 0.$$

where

$$\begin{aligned} f_i &:= f(c_{i1}S_1 + c_{i1} - 1, \cdots, c_{i,d}S_d + c_{i,d} - 1) \\ &= b_0^i(S_1, \ldots, S_{d-1}) + b_1^i(S_1, \ldots, S_{d-1})S_d + \cdots + b_{l-1}^i(S_1, \ldots, S_{d-1})S_d^{l-1} + c_{id}^l S_d^l, \end{aligned}$$

for some power series b_j^i and units $c_{ij} := \psi_i(S_j+1)\psi_{2g}(S_j+1)$, is in the annihilator of $M(-1)\otimes\chi_i\otimes\chi_{2g}$. We wish to estimate how many zeros each f_i can have on the set $\{\underline{\psi}^\alpha \mid \ |\alpha| \leq n-2\}$.

There are independent elements $\{\phi_i\}$ in the $\mathbb{Z}-$lattice of characters generated by the ξ_i such that $\phi_i(\epsilon_j) = 1$ for $i \neq j$ and

$$\xi_i = \phi_1^{m_{i1}} \cdots \phi_d^{m_{i,d}}$$

for a nonsingular matrix (m_{ij}) with entries $m_{ij} \in (1/M')\mathbb{Z}$ for some fixed denominator $M' \in \mathbb{Z} \cap \mathbb{Z}_p^*$. Therefore, by the discussion in section 1, we have

$$\psi_i = \phi_1^{q_{i1}} \cdots \phi_d^{q_{i,d}}$$

for a $(2g) \times d$ integral matrix $D = (q_{ij})$ of rank d having entries in $(1/M)\mathbb{Z}$ for some fixed integer M. Given a multi-index α, we then have

$$\underline{\psi}^\alpha = \underline{\phi}^{\alpha D},$$

with αD denoting the matrix product. For $|\alpha| \leq n-2$, we find the bound

$$|\alpha D| \leq (n-2)(2g)|D|,$$

where $|D| = \max\{|q_{ij}|\}$. Now, for each multi-index

$$\delta = (\delta_1, \ldots, \delta_d) \in [(1/M)\mathbb{Z}]^d$$

such that

$$|\delta| \leq (n-2)(2g)|D|,$$

we need to count the cardinality of the set

$$L_\delta = \{\alpha \in \mathbb{N}^{2g} \mid \ \delta = \alpha D, |\alpha| \leq n-2\}.$$

If we fix one $\alpha \in L_\delta$, the map $\alpha' \mapsto \alpha' - \alpha$ will inject L_δ into the set of $\mu = (\mu_1, \ldots, \mu_{2g}) \in \mathbb{Z}^{2g}$ such that $\mu D = 0$ and $\sup_i |\mu_i| \leq (n-2)$. The first condition defines a lattice inside a Euclidean space of dimension $2g-d$ while the second condition defines a fixed compact convex body (independent of n) inside this space dilated by a factor of $n-2$. Thus, there is a constant C depending on the convex body such that $|L_\delta| \leq C(n-2)^{2g-d}$. Now we turn to the number of δ for which

$$\underline{\phi}^\delta(f_i) = 0$$

and $|\delta| \leq (n-2)(2g)|D|$. The coefficients power series b_j^i depend only on $(\delta_1, \ldots, \delta_{d-1})$, which runs over a set of cardinality

$$\sum_{i=1}^{2g(n-2)M|D|} \binom{i+d-2}{d-2}.$$

This is the number of lattice points in $d-1$ dimensional space that are contained inside a simplex with vertices at the origin and at the points

$$(0, \ldots, 0, 2g(n-2)M|D|, 0, \ldots, 0).$$

This number is clearly majorized by the number of lattice points inside the cube

$$[0, 2g(n-2)M|D|]^{d-1},$$

that is,

$$(2g(n-2)M|D|+1)^{d-1}.$$

For each such $(\delta_1, \ldots, \delta_{d-1})$, there are at most l d-tuples $\delta = (\delta_1, \ldots, \delta_{d-1}, \delta_d)$ such that $\underline{\phi}^{\delta}(f) = 0$. We conclude that the number of δ such that $|\delta| \leq 2g(n-2)M|D|$ and $\delta(f) = 0$ is bounded by $l(2g(n-2)M|D|+1)^{d-1}$. Therefore, the number of zeros of each f_i on $\{\underline{\psi}^{\alpha} \ | \ |\alpha| \leq n-2\}$ is bounded by

$$C(n-2)^{2g-d} l(2g(n-2)M|D|+1)^{d-1} \leq An^{2g-1}$$

for some constant A. For each such zero α, the dimension of

$$\mathrm{Hom}_{\Lambda}(M \otimes \chi_i \otimes \chi_{2g}, \underline{\psi}^{\alpha})$$

is bounded by the number of generators m of M. From this, we deduce the desired asympototics

$$\mathrm{dimHom}_{\Lambda}(M(-1), \oplus_{i<2g}[\psi_i \otimes \psi_{2g} \otimes (\oplus_{i=1}^{n-2}\mathrm{Sym}^i(V))]) \leq mAn^{2g-1}.$$

□

Proof of corollary 0.2. For the rough estimates relevant to this paper, we will find useful the elementary fact that $(n+a)^b = n^b + O(n^{b-1})$ for any fixed constant a and exponent b.

We need to find lower bounds for the dimension of the local Selmer variety. We have the De Rham realization

$$W^{DR} := U^{DR}/(U^{DR})^{(3)},$$

where U^{DR} is the De Rham fundamental group of $X \otimes \mathbb{Q}_p$ with base point at b. We denote by $(U')^{DR}$ the De Rham fundamental group of X' with basepoint at v ([4], [15]). Since

$$(U')^{DR} \otimes \mathbb{C}_p \simeq U' \otimes \mathbb{C}_p,$$

([21], [22]) we see that

$$(L')^{DR} = Lie(U')^{DR}$$

is also free, and we can estimate dimensions exactly as in section 1. For example, as in Lemma 1.3,

$$\mathrm{dim}Z_n(W^{DR}) \geq (2g-2)\binom{n-3+2g}{2g-1}$$

so that

$$\sum_{i=3}^{n} \mathrm{dim}Z_i(W^{DR}) \geq \frac{2g-2}{(2g)!}(n-2)^{2g}.$$

We need to estimate the contribution of $F^0(Z_n(W^{DR}))$. For this, we let $\{b_1, \ldots, b_g, \ldots, b_{2g}\}$ be a basis of $(L')^{DR}_1$ such that $\{b_1, \ldots, b_g\}$ is a basis for $F^0(L')^{DR}_1$. This determines a basis $H^{DR} = \cup_n H^{DR}_n$ for $(L')^{DR}$ following the recipe of section 1. There are also corresponding bases for L^{DR}, $(N')^{DR} := Lie[(U')^{DR}/[(U')^{DR}]^{(3)}]$, and a generating set for N^{DR}, exactly as in the discussion of section 1. The Hodge filtration on

$$(L')^{DR}_1 = [H^1_{DR}(X' \otimes \mathbb{Q}_p)]^*$$

is of the form

$$(L')^{DR}_1 = F^{-1}(L')^{DR}_1 \supset F^0(L')^{DR}_1 \supset F^1(L')^{DR}_1 = 0.$$

Hence, for an element

$$[[\ldots[b_{i_1}, b_{i_2}], b_{i_3}], \ldots]b_{i_n}]$$

of $H_1^{DR}(n)$ to lie in $F^0[Z_n((L')^{DR})]$, all of the b_i must be in $F^0(L')_1^{DR}$. Thus, the dimension of $F^0[Z_n((N')^{DR})]$, and hence, of $F^0[Z_n(W^{DR})]$ is at most

$$\binom{g}{2}\binom{n+g-3}{g-1}.$$

From this, we get the estimate

$$\dim_{i=3}^{n} F^0(Z_i(W^{DR})) \leq cn^g$$

for some constant c. Therefore, we see that

$$(*) \quad \dim W_n^{DR}/F^0 = \dim W_2^{DR}/F^0 + \sum_{i=3}^{n} Z_i(W^{DR}) \geq \frac{(2g-2)}{(2g)!}n^{2g} + O(n^{2g-1}).$$

Now we examine the dimension of the minus parts $Z_n(W)^-$. For this, it is convenient to carry out the Hall basis construction with yet another generating set. We choose $B' = \{f_1, \ldots, f_g, \ldots, f_{2g}\}$ so that $\{f_1, \ldots, f_g\}$ and $\{f_{g+1}, \ldots, f_{2g}\}$ consist of the plus and minus 1 eigenvectors in V, respectively. Clearly, $\dim Z_n(N')^-$ will majorize $\dim Z_n(W)^-$. Furthermore, as discussed above, $Z_n(N') = S_n + R_n$ where S_n is the span of

$$[\ldots[f_j, f_{2g}], f_{i_3}] \ldots, f_{i_n}]$$

for $j < 2g$ and nondecreasing $(n-2)$-tuples $(i_3, \ldots, i_n)$, while $\dim R_n = O(n^{2g-2})$. Now, $[f_j, f_{2g}]$ is in the minus part for $j \leq g$ and in the plus part for $j \geq g+1$, while the contribution of the $(n-2)$-tuple will be as $\mathrm{Sym}^{n-2}(V)$.

That is,

$$\dim S_n^- = g\dim\mathrm{Sym}^{n-2}(V)^+ + (g-1)\mathrm{Sym}^{n-2}(V)^-.$$

But

$$\mathrm{Sym}^{n-2}(V) = \oplus_i[\mathrm{Sym}^i(V^+) \otimes \mathrm{Sym}^{n-2-i}(V^-)]$$

of which we need to take into account the portions where $n-2-i$ is even and odd respectively, to get the positive and negative eigenspaces.

For n odd, we easily see that the plus and minus parts pair up, giving us

$$\dim\mathrm{Sym}^{n-2}(V)^- = \dim\mathrm{Sym}^{n-2}(V)^+ = (1/2)\dim\mathrm{Sym}^{n-2}(V) = (1/2)\binom{n-3+2g}{2g-1}.$$

From this, we deduce that for n odd,

$$\dim S_n^- = (1/2)(2g-1)\binom{n-3+2g}{2g-1}.$$

On the other hand, if n is even, then there is the embedding

$$\mathrm{Sym}^{n-2}(V) \hookrightarrow \mathrm{Sym}^{n-1}(V)$$

$$v \rightarrow v \cdot f_1$$

that preserves the plus and minus eigenspaces. Hence,

$$\dim\mathrm{Sym}^{n-2}(V)^+ \leq \dim\mathrm{Sym}^{n-1}(V)^+ = (1/2)\binom{n-2+2g}{2g-1} = (1/2)n^{2g-1}/(2g-1)! + O(n^{2g-2})$$

and

$$\dim\mathrm{Sym}^{n-2}(V)^- \leq \dim\mathrm{Sym}^{n-1}(V)^- = (1/2)\binom{n-2+2g}{2g-1} = (1/2)n^{2g-1}/(2g-1)! + O(n^{2g-2}).$$

Therefore, for any n, we have

$$\dim S_n^- \leq (1/2)(2g-1)n^{2g-1}/(2g-1)! + O(n^{2g-2}).$$

and

$$\dim Z_n(N)^- \leq (1/2)(2g-1)\frac{n^{2g-1}}{(2g-1)!} + O(n^{2g-2}).$$

We deduce immediately that

$$\sum_{i=1}^{n} Z_i(N)^- \leq (1/2)(2g-1)\frac{n^{2g}}{(2g)!} + O(n^{2g-1}).$$

Combining this inequality with the lower bound (*), theorem (0.1), and the Euler characteristic formula (EC), we get

$$\dim H^1_f(G, W_n) < \dim H^1_f(G_p, W_n)$$

for n sufficiently large. □

Remark: Note that in the comparison of leading coefficients,

$$(1/2)\frac{2g-1}{(2g)!} < \frac{2g-2}{(2g)!}$$

exactly for $g \geq 2$.

Proof of corollary 0.3

By [15], section 2, and [6], there is an algebraic map

$$D = D_{cr} : H^1_f(G_p, U) \longrightarrow U^{DR}/F^0$$

sending a U-torsor

$$P = \mathrm{Spec}(\mathcal{P})$$

to

$$\mathrm{Spec}(D_{cr}(\mathcal{P})) = \mathrm{Spec}(\mathcal{P} \otimes B_{cr})^{G_p},$$

an admissible U^{DR} torsor, that is, a U^{DR}-torsor with a compatible Frobenius action and a reduction of structure group to F^0U^{DR} ([15], section 1).

We wish to deduce an analogous map for W. But [21] and [22] give an isomorphism

$$L \otimes B_{cr} \simeq L^{DR} \otimes B_{cr}$$

compatible with the Lie algebra structure as well as the usual Galois action, ϕ-action, and Hodge filtration. In particular,

$$L^{(3)} \otimes B_{cr} \simeq (L^{DR})^{(3)} \otimes B_{cr},$$

and hence,

$$N \otimes B_{cr} \simeq N^{DR} \otimes B_{cr}.$$

Therefore,

$$D_{cr}(N) = N^{DR}$$

and

$$D_{cr}(W) = W^{DR}.$$

There is thereby an induced map

$$D : H^1_f(G_p, W) \longrightarrow W^{DR}/F^0$$

following verbatim the construction for U and U^{DR} as in [15], section 2. That is, as in [15], Proposition 1 of section 1, W^{DR}/F^0 classifies admissible torsors for W^{DR}, and the map assigns to a W-torsor a W^{DR}-torsor, exactly following the recipe for U and U^{DR}.

Now corollary (0.3) also follows verbatim the argument in [14], section 2, and [15], section 3, by using the diagram

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d] & X(\mathbb{Q}_p) \arrow[d] \arrow[dr] & . \\
H^1_f(G, W_n) \arrow[r] & H^1_f(G_p, W_n) \arrow[r] & W_n^{DR}/F^0
\end{tikzcd}$$

for n sufficiently large. We need only note that the map

$$]y[\rightarrow W_n^{DR}/F^0$$

from any residue disk $]y[\subset X(\mathbb{Q}_p)$ to W_n^{DR}/F^0 has Zariski dense image, since the same is true of

$$]y[\rightarrow U_n^{DR}/F^0$$

and the map

$$U_n^{DR}/F^0 \rightarrow W_n^{DR}/F^0$$

is surjective. □

Acknowledgements: We are very grateful to Henri Darmon, Ralph Greenberg, Richard Hain, Ramadorai Sujatha, and especially Kazuya Kato for many conversations related to the present subject. This paper was finalized during a stay at the Tata Institute for Fundamental Research in September, 2008. The hospitality of the staff and the organizers of the special semester on arithmetic geometry, E. Ghate, C.S. Rajan, and R. Sujatha, was essential to the completion of the present work.

References

[1] Amorós, Jaume On the Malcev completion of Kähler groups. Comment. Math. Helv. 71 (1996), no. 2, 192–212.

[2] Coates, J.; Wiles, A. On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. 39 (1977), no. 3, 223–251.

[3] Coleman, Robert F. Effective Chabauty. Duke Math. J. 52 (1985), no. 3, 765–770.

[4] Deligne, Pierre Le groupe fondamental de la droite projective moins trois points. Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), 79–297, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.

[5] Deligne, Pierre; Milne, James S.; Tannakian Categories. Hodge cycles, motives, and Shimura varieties. Lecture Notes in Mathematics, 900. Springer-Verlag, Berlin-New York, 1982.

[6] Faltings, Gerd Mathematics around Kim's new proof of Siegel's theorem. Diophantine geometry, 173–188, CRM Series, 4, Ed. Norm., Pisa, 2007.

[7] Fontaine, Jean-Marc Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate. Ann. of Math. (2) 115 (1982), no. 3, 529–577.

[8] Fontaine, Jean-Marc; Messing, William p-adic periods and p-adic étale cohomology. Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), 179–207, Contemp. Math., 67, Amer. Math. Soc., Providence, RI, 1987.

[9] Greenberg, Ralph The Iwasawa invariants of Γ-extensions of a fixed number field. Amer. J. Math. 95 (1973), 204–214.

[10] Greenberg, Ralph On the structure of certain Galois groups. Invent. Math. 47 (1978), no. 1, 85–99.

[11] Hain, Richard; Matsumoto, Makoto Weighted completion of Galois groups and Galois actions on the fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$. Compositio Math. 139 (2003), no. 2, 119–167.

[12] Jannsen, Uwe On the l-adic cohomology of varieties over number fields and its Galois cohomology. Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), 315–360, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.

[13] Katz, Nicholas M.; Messing, William Some consequences of the Riemann hypothesis for varieties over finite fields. Invent. Math. 23 (1974), 73–77.

[14] Kim, Minhyong The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. Invent. Math. 161 (2005), no. 3, 629–656.

[15] Kim, Minhyong The unipotent Albanese map and Selmer varieties for curves. Publ. Res. Inst. Math. Sci. (to be published).

[16] Kim, Minhyong Remark on fundamental groups and effective Diophantine methods for hyperbolic curves. To be published in Serge Lang memorial volume. Available at mathematics archive, arXiv:0708.1115.

[17] Kim, Minhyong p-adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication. Preprint. Available at mathmetics archive: arXiv:0710.5290 (math.AG)

[18] Kim, Minhyong, and Tamagawa, Akio The l-component of the unipotent Albanese map. Math. Ann. 340 (2008), no. 1, 223–235.

[19] Labute, John P. On the descending central series of groups with a single defining relation. J. Algebra 14 1970 16–23.

[20] Milne, J. S. Arithmetic duality theorems. Perspectives in Mathematics, 1. Academic Press, Inc., Boston, MA, 1986.

[21] Olsson, Martin Towards non-abelian p-adic Hodge theory in the good reduction case. Preprint. Available at http://math.berkeley.edu/ molsson/.

[22] Olsson, Martin The bar construction and affine stacks. Preprint. Available at http://math.berkeley.edu/ molsson/.

[23] Quillen, Daniel Rational homotopy theory. Ann. of Math. (2) 90 (1969), 205–295.

[24] Reutenauer, Christophe Free Lie algebras. London Mathematical Society Monographs. New Series, 7. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1993.

[25] Rubin, Karl On the main conjecture of Iwasawa theory for imaginary quadratic fields. Invent. math. 93 (1988), 701–713.

[26] Schmidt, Claus-Günther, Arithmetik abelscher Varietäten mit komplexer Multiplikation. Lecture Notes in Mathematics, 1082. Springer-Verlag, Berlin, 1984.

[27] Serre, Jean-Pierre Lie algebras and Lie groups. 1964 lectures given at Harvard University. Second edition. Lecture Notes in Mathematics, 1500. Springer-Verlag, Berlin, 1992. viii+168 pp.

[28] Serre, Jean-Pierre; Tate, John Good reduction of abelian varieties. Ann. of Math. (2) 88 1968 492–517.

[29] Serre, Jean-Pierre Abelian l-adic representations and elliptic curves. With the collaboration of Willem Kuyk and John Labute. Second edition. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.

[30] Wamelen, Paul van Examples of genus 2 CM curves defined over the rationals. Math. Comp. 68, no. 205 (1999), 307–320.

[31] Wildeshaus, Jörg Realizations of polylogarithms. Lecture Notes in Mathematics, 1650. Springer-Verlag, Berlin, 1997.

[32] Wojtkowiak, Zdzislaw Cosimplicial objects in algebraic geometry. Algebraic K-theory and algebraic topology (Lake Louise, AB, 1991), 287–327, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 407, Kluwer Acad. Publ., Dordrecht, 1993.

J.C.: Department of Pure Mathematics and Mathematical Statistics, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WB

M.K: Department of Mathematics, University College London, Gower Street, London, WC1E 6BT, United Kingdom and The Korea Institute for Advanced Study, Hoegiro 87, Dongdaemun-gu, Seoul 130-722, Korea