

ANTICYCLOTOMIC IWASAWA THEORY OF CM ELLIPTIC CURVES II

ADEBISI AGBOOLA AND BENJAMIN HOWARD

ABSTRACT. We study the Iwasawa theory of a CM elliptic curve E in the anticyclotomic \mathbf{Z}_p -extension D_∞ of the CM field K , where p is a prime of good, supersingular reduction for E . Our main result yields an asymptotic formula for the corank of the p -primary Selmer group of E along the extension D_∞/K .

1. INTRODUCTION

Let E be an elliptic curve over \mathbf{Q} . Whilst much is known about the Iwasawa theory of E for primes of ordinary reduction, the same is unfortunately not true of Iwasawa theory at supersingular primes, for in this case the Iwasawa modules that one naturally considers are not torsion, and the obvious candidates for p -adic L -functions do not lie in the Iwasawa algebra. Nevertheless, there has recently been a great deal of progress in the study of the Iwasawa theory of elliptic curves at supersingular primes. In particular, S. Kobayashi has recently formulated a cyclotomic main conjecture for E within this framework (see [5]). His conjecture relates certain restricted ‘plus/minus’ Selmer groups of E to certain modified p -adic L -functions defined by R. Pollack (see [9]), and it is equivalent to a cyclotomic main conjecture that was proposed earlier by K. Kato and B. Perrin-Riou (see [4], [7] [6]). Kobayashi’s conjecture has recently been proved by Rubin and Pollack (see [15]) when E has complex multiplication, and Kobayashi himself, using methods of Kato, proves one divisibility of the main conjecture in the non-CM case. In both cases, the plus/minus Selmer groups are cotorsion modules over the cyclotomic Iwasawa algebra, and so the corank of the p -Selmer group remains bounded as one ascends the cyclotomic \mathbf{Z}_p -extension.

Suppose now that E has complex multiplication by the maximal order \mathcal{O} of an imaginary quadratic field K . Let ψ denote the K -valued grossencharacter associated to E , and write \mathfrak{f} for the conductor of ψ . Fix once and for all a rational prime $p > 3$ at which E has good reduction, and which is inert in K . Then E has supersingular reduction at p . We write \mathfrak{p} for the unique prime of K above p . Let D_∞ be the anticyclotomic \mathbf{Z}_p extension of K , and let $D_n \subset D_\infty$ be the subfield such that $[D_n : K] = p^n$. The prime \mathfrak{p} is totally ramified in D_∞ , and we let \mathfrak{p} also denote the unique place of D_∞ above \mathfrak{p} .

In this paper, we study the Iwasawa theory of E over D_∞ . We define anticyclotomic versions of Kobayashi’s restricted plus/minus Selmer groups, and we analyse their structure using the Euler system of twisted elliptic units (cf. [1]). In contrast to what happens in the cyclotomic case, it turns

Date: Final version, March 23, 2005.

2000 *Mathematics Subject Classification.* 11G05, 11R23, 11G16.

The first author was partially supported by NSF grant DMS-0070449.

The second author was supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship.

out that one of the restricted Selmer groups is a cotorsion Iwasawa module, while the other is not, and which module is cotorsion is determined by the sign in the functional equation of $L(E/\mathbf{Q}, s)$. Our main result, predicted by R. Greenberg [3, p. 247], is as follows (somewhat more information is contained in Theorem 5.4).

Theorem A. *Let ϕ be Euler's function and let $\varepsilon = \pm 1$ be the sign in the functional equation of $L(E/\mathbf{Q}, s)$. Write $\text{Sel}_{\mathfrak{p}^\infty}(E/D_n)$ for the \mathfrak{p} -primary Selmer group of E/D_n , and $\mathcal{O}_{\mathfrak{p}}$ for the local completion of \mathcal{O} at \mathfrak{p} . Then there is an integer e , independent of n , such that*

$$\text{corank}_{\mathcal{O}_{\mathfrak{p}}} \text{Sel}_{\mathfrak{p}^\infty}(E/D_n) = e + \sum_{1 \leq k \leq n, (-1)^k = \varepsilon} \phi(p^k)$$

for all $n \gg 0$.

The results in this paper may be viewed as a first step towards a supersingular main conjecture of the same type as that considered in [1]. However, in the present setting, we do not know how to define suitable anticyclotomic analogues of Pollack's plus/minus p -adic L -functions. The essential missing ingredient is a construction of local elements along the lines of [5, §8.4].

2. SELMER GROUPS

We write

$$T = T_p(E), \quad W = E[p^\infty]$$

for the p -adic Tate module and the group of p -power torsion points in $E(\overline{K})$ respectively. Let F/K be any finite extension. For any place v of F , we define $H_f^1(F_v, W)$ to be the image of $E(F_v) \otimes (\mathbf{Q}_p/\mathbf{Z}_p)$ under the Kummer map

$$E(F_v) \otimes (\mathbf{Q}_p/\mathbf{Z}_p) \rightarrow H^1(F_v, W),$$

and we write $H_f^1(F_v, T)$ for the orthogonal complement of $H_f^1(F_v, W)$ with respect to the local Tate pairing. Note that $H_f^1(F_v, W) = 0$ if $v \nmid p$. If $c \in H^1(F, W)$, then we write $\text{loc}_v(c)$ for the image of c in $H^1(F_v, W)$.

We define

- the *relaxed Selmer group* $\text{Sel}_{\text{rel}}(F, W)$ by

$$\text{Sel}_{\text{rel}}(F, W) = \{c \in H^1(F, W) \mid \text{loc}_v(c) \in H_f^1(F_v, W) \text{ for all } v \text{ not dividing } p\};$$

- the *true Selmer group* $\text{Sel}(F, W)$ by

$$\text{Sel}(F, W) = \{c \in H^1(F, W) \mid \text{loc}_v(c) \in H_f^1(F_v, W) \text{ for all } v\};$$

- the *strict Selmer group* $\text{Sel}_{\text{str}}(F, W)$ by

$$\text{Sel}_{\text{str}}(F, W) = \{c \in \text{Sel}(F, W) \mid \text{loc}_v(c) = 0 \text{ for all } v \text{ dividing } p\}.$$

We also define $\text{Sel}_{\text{rel}}(F, T)$, $\text{Sel}(F, T)$ and $\text{Sel}_{\text{str}}(F, T)$ in a similar way. It follows from the definitions that there are inclusions

$$\text{Sel}_{\text{str}}(F, W) \subset \text{Sel}(F, W) \subset \text{Sel}_{\text{rel}}(F, W),$$

and similarly with W replaced by T . If F/K is an infinite extension, we define

$$\mathrm{Sel}_*(F, W) = \varinjlim \mathrm{Sel}_*(F', W) \quad \mathcal{S}_*(F, T) = \varprojlim \mathrm{Sel}_*(F', T),$$

where the limits are taken with respect to restriction and corestriction, respectively, over all subfields $F' \subset F$ finite over K .

We now give the definition of a slightly modified (see Remark 3.2 below) form of Kobayashi's restricted plus/minus Selmer groups. Let \mathbf{E} denote the formal group of E over $K_{\mathfrak{p}}$. Since E has supersingular reduction at $p > 3$, it is a standard fact that \mathbf{E} is isomorphic to the unique (up to isomorphism) Lubin-Tate formal group over $K_{\mathfrak{p}}$ with parameter $-p$. For $n \geq 0$, let Ξ_n^- be the set of characters of Γ_n of exact order p^k with k odd, together with the trivial character. Let Ξ_n^+ be the set of characters of Γ_n of exact order p^k with k even, excluding the trivial character. Define subspaces of $E(D_{n,\mathfrak{p}}) \otimes_{\mathcal{O}_{\mathfrak{p}}} K_{\mathfrak{p}}$ by

$$E_{\pm}(D_{n,\mathfrak{p}}) = \left\{ x \in \mathbf{E}(D_{n,\mathfrak{p}}) \otimes K_{\mathfrak{p}} \mid \sum_{\sigma \in \Gamma_n} \chi(\sigma) x^{\sigma} = 0, \forall \chi \in \Xi_n^{\mp} \right\}.$$

Let $H_{\pm}^1(D_{n,\mathfrak{p}}, W)$ be the image of $E_{\pm}(D_{n,\mathfrak{p}})$ under the Kummer map

$$E(D_{n,\mathfrak{p}}) \otimes K_{\mathfrak{p}} \rightarrow E(D_{n,\mathfrak{p}}) \otimes (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \rightarrow H^1(D_{n,\mathfrak{p}}, W)$$

and let $H_{\pm}^1(D_{n,\mathfrak{p}}, T)$ be the orthogonal complement of $H_{\pm}^1(D_{n,\mathfrak{p}}, W)$ with respect to the local Tate pairing. We define

$$\mathrm{Sel}_{\pm}(D_n, W) = \{c \in \mathrm{Sel}_{\mathrm{rel}}(D_n, W) \mid \mathrm{loc}_{\mathfrak{p}}(c) \in H_{\pm}^1(D_{n,\mathfrak{p}}, W)\};$$

$$\mathrm{Sel}_{\pm}(D_n, T) = \{c \in \mathrm{Sel}_{\mathrm{rel}}(D_n, T) \mid \mathrm{loc}_{\mathfrak{p}}(c) \in H_{\pm}^1(D_{n,\mathfrak{p}}, T)\}.$$

It follows from the definitions that we have inclusions

$$\mathrm{Sel}_{\mathrm{str}}(D_n, W) \subset \mathrm{Sel}_{\pm}(D_n, W) \subset \mathrm{Sel}(D_n, W),$$

$$\mathrm{Sel}(D_n, T) \subset \mathrm{Sel}_{\pm}(D_n, T) \subset \mathrm{Sel}_{\mathrm{rel}}(D_n, T).$$

In the limit, we define

$$\mathrm{Sel}_{\pm}(D_{\infty}, W) = \varinjlim \mathrm{Sel}_{\pm}(D_n, W) \quad \mathcal{S}_{\pm}(D_{\infty}, T) = \varprojlim \mathrm{Sel}_{\pm}(D_n, T),$$

where the inverse limits are taken with respect to restriction and corestriction, respectively.

In order to ease notation, we shall sometimes write

$$\mathrm{Sel}_*^{\infty} = \mathrm{Sel}_*(D_{\infty}, W) \quad \mathcal{S}_* = \mathcal{S}_*(D_{\infty}, T).$$

3. RANKS

Let \mathfrak{a} be an integral ideal of \mathcal{O} coprime to $6p\mathfrak{f}$, and write $\mathcal{K}_{\mathfrak{a}}$ for the union of all ray class fields of K of conductor prime to \mathfrak{a} . Let $c_{\mathrm{ell},\mathfrak{a}}$ denote the Euler system of elliptic units for $(\mathbf{Z}_p(1), \mathfrak{f}p, \mathcal{K}_{\mathfrak{a}})$ in the sense of [14]. Twisting $c_{\mathrm{ell},\mathfrak{a}}$ by the character $\omega_{\mathrm{cyc}}^{-1}\psi_{\mathfrak{p}}$, where

$$\psi_{\mathfrak{p}} : \mathrm{Gal}(\overline{K}/K) \rightarrow \mathrm{Aut}_{\mathcal{O}_K}(T) \cong \mathcal{O}_{\mathfrak{p}}^{\times},$$

and ω_{cyc} is the cyclotomic character, yields an Euler system $c_{\mathfrak{a}}$ for $(T, fp, \mathcal{K}_{\mathfrak{a}})$ (see [14, Chapter 6]). Then $c_{\mathfrak{a}}(F) \in \text{Sel}_{\text{rel}}(F, T)$ for every $F \subset \mathcal{K}_{\mathfrak{a}}$ finite over K . For any $L \subset K_{\infty}$, let

$$c_{\mathfrak{a}}(L) = \varprojlim c_{\mathfrak{a}}(F') \in \mathcal{S}_{\text{rel}}(L, T),$$

where the inverse limit is taken over all subfields F' of L that are finite over K . Let $\mathcal{C}_{\mathfrak{a}}(F)$ be the $\mathcal{O}_{\mathfrak{p}}[[\text{Gal}(F/K)]]$ -submodule of $\mathcal{S}_{\text{rel}}(F, T)$ generated by $c_{\mathfrak{a}}(F)$, and write $\mathcal{C}(F)$ for the submodule generated by $\mathcal{C}_{\mathfrak{a}}(F)$ as \mathfrak{a} varies over all ideals that are coprime to $6p\mathfrak{f}$. We set $\mathcal{C} = \mathcal{C}(D_{\infty})$.

Define

$$\mathcal{H}_{\pm}^1 = \varprojlim H_{\pm}^1(D_{n,p}, T) \quad \mathcal{H}^1 = \varprojlim H^1(D_{n,p}, T)$$

and

$$H_{\pm}^1(D_{\infty,p}, W) = \varprojlim H_{\pm}^1(D_{n,p}, W).$$

Let $W(\psi)$ denote the root number of ψ . In particular $W(\psi) = \pm 1$ and is equal to the sign in the functional equation of $L(E/\mathbf{Q}, s)$.

Proposition 3.1. *The image of \mathcal{C} in \mathcal{H}^1 is nontrivial, and lies in $\mathcal{H}_{\varepsilon}^1$ if and only if ε is equal to the sign of $W(\psi)$. In particular \mathcal{C} is nontrivial, and is contained in $\mathcal{S}_{\varepsilon}$ if and only if ε is the sign of $W(\psi)$.*

Proof. Let χ be any primitive character of $\text{Gal}(D_n/K)$ for $n > 0$, and write $W(\chi\psi)$ for the root number of $\chi\psi$. The following formula is proved by Greenberg in [3, page 247]:

$$W(\chi\psi) = (-1)^{n+1}W(\psi). \quad (3.1)$$

If $(-1)^n = W(\psi)$, the functional equation of $L(E/\mathbf{Q}, s)$ forces $L(\chi\psi, 1) = 0$. On the other hand, the main result of [10] shows that if $(-1)^n = -W(\psi)$, then $L(\chi\psi, 1) \neq 0$ for all but finitely many χ . The claim now follows from the reciprocity law of Coates-Wiles, which relates the localization of the elliptic units to the special value of twists of $L(\psi, s)$ (see [15, Theorem 5.1] for example). \square

Remark 3.2. The equality (3.1) (which is visibly incorrect when $n = 0$) is the reason for placing the trivial character in Ξ_n^- . In particular, our definitions differ from those of [15, Definition 3.1].

The reader should also note that in [12], the characters of Γ_n are indexed according to the parity of their conductors, while we have indexed them according to the parity of their orders. Hence our Ξ^+ (respectively Ξ^-) is denoted by Ξ^- (respectively Ξ^+) in [12]. \square

Set $\Lambda = \mathcal{O}_{\mathfrak{p}}[[\text{Gal}(D_{\infty}/K)]]$. For any finitely generated Λ -module M , we write $\text{Char}_{\Lambda}(M)$ for the characteristic ideal of M in Λ , and $\text{rk}_{\Lambda}(M)$ for the Λ -rank of M . Define a Λ -module

$$X_* = \text{Hom}_{\mathbf{Z}_p}(\text{Sel}_*^{\infty}, \mathbf{Q}_p/\mathbf{Z}_p).$$

Let $\iota : \Lambda \rightarrow \Lambda$ denote the canonical involution on Λ which is induced by inversion on group-like elements. We adopt the convention that Λ acts on X_* via the rule $(\lambda \cdot f)(x) = f(\lambda^{\iota}x)$ (cf. [1, Remark 1.18]).

The following two propositions are consequences of the work of Rubin.

Proposition 3.3. (i) The Λ -modules \mathcal{S}_{rel} and X_{str} are torsion-free of rank one, and torsion, respectively. The Λ -module X_{rel} has rank one.

(ii) There is an equality of characteristic ideals

$$\text{Char}_\Lambda(X_{\text{str}}) = \text{Char}_\Lambda(\mathcal{S}_{\text{rel}}/\mathcal{C}).$$

Proof. The fact that \mathcal{S}_{rel} is torsion-free of the same rank as X_{rel} may be proved exactly as in [1, Lemma 1.1.9] (the proof of which is essentially the same as that of [8, Proposition 4.2.3]). The remaining claims of (i) follow from the nontriviality of \mathcal{C} using the theory of Euler systems as in [14]. Using (i), (ii) may be deduced from Rubin's two variable main conjecture [13, Theorem 4.1(ii)] exactly as in [1, Proposition 2.4.16]. \square

Proposition 3.4. The Λ -module \mathcal{H}^1 is torsion free of rank 2. The modules \mathcal{H}_\pm^1 have Λ -rank 1 and satisfy $\mathcal{H}_+^1 \cap \mathcal{H}_-^1 = 0$. The modules $H_\pm^1(D_\infty, W)$ have Λ -corank one.

Proof. Write $H_f^1(D_{\infty, \mathfrak{p}}, W) = \varinjlim H_f^1(D_{n, \mathfrak{p}}, W)$, where the inductive limit is taken with respect to restriction maps. Let $\mathbf{E}[\mathfrak{p}^\infty]$ and $E[\mathfrak{p}^\infty]$ denote the \mathfrak{p} -primary torsion subgroups of \mathbf{E} and E respectively, and write $K(E[\mathfrak{p}^\infty])$ for the field obtained by adjoining the elements of $E[\mathfrak{p}^\infty]$ to K . Set

$$V_\infty = \text{Hom}_{\mathcal{O}_\mathfrak{p}}(H_f^1(D_{\infty, \mathfrak{p}}, W), \mathbf{E}[\mathfrak{p}^\infty]), \quad V^\pm = \text{Hom}_{\mathcal{O}_\mathfrak{p}}\left(\frac{H_f^1(D_{\infty, \mathfrak{p}}, W)}{H_\pm^1(D_{\infty, \mathfrak{p}}, W)}, \mathbf{E}[\mathfrak{p}^\infty]\right).$$

We may view V_∞ and V^\pm as being Λ -modules by identifying $\text{Gal}(D_\infty/K)$ with a subgroup of $\text{Gal}(K(E[\mathfrak{p}^\infty])/K)$ in the obvious way. It is shown in [12, Propositions 1.1 and 8.1] that the Λ -module V_∞ is torsion-free of rank 2, while the Λ -modules V^\pm are of rank one and satisfy $V_+ \cap V_- = 0$. The proposition now follows from the fact that fixing an identification of $K_\mathfrak{p}/\mathcal{O}_\mathfrak{p}$ with $\mathbf{E}[\mathfrak{p}^\infty]$ induces Λ -module isomorphisms

$$V \simeq \mathcal{H} \otimes \text{Hom}_{\mathcal{O}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p}, T), \quad V_\pm \simeq \mathcal{H}_\pm \otimes \text{Hom}_{\mathcal{O}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p}, T). \quad (3.2)$$

\square

Conjecture 3.5. (Rubin [12, Conjecture 2.2]) $\mathcal{H}^1 = \mathcal{H}_+^1 \oplus \mathcal{H}_-^1$.

Theorem 3.6. We have $\text{rk}_\Lambda(\mathcal{S}_\pm) = \text{rk}_\Lambda(X_\pm)$. If the sign of $W(\psi)$ is ε , then X_ε has Λ -rank one, and $X_{-\varepsilon}$ is Λ -torsion. In particular $\mathcal{S}_{\text{str}} = \mathcal{S}_{-\varepsilon} = 0$, as \mathcal{S}_{rel} is torsion-free.

Proof. Global duality (see [14, Theorem 1.7.3]) gives the exact sequence

$$0 \rightarrow \mathcal{S}_\pm \rightarrow \mathcal{S}_{\text{rel}} \rightarrow \mathcal{H}^1/\mathcal{H}_\pm^1 \rightarrow X_\pm \rightarrow X_{\text{str}} \rightarrow 0. \quad (3.3)$$

The first claim now follows from Propositions 3.3 and 3.4.

Since $\mathcal{S}_\pm \subset \mathcal{S}_{\text{rel}}$, the Λ -rank of \mathcal{S}_\pm is at most one, and as $\mathcal{C} \subset \mathcal{S}_\varepsilon$ is non-trivial, we see that the Λ -rank of \mathcal{S}_ε is in fact equal to one. Next, we observe that if $\text{rk}_\Lambda(\mathcal{S}_{-\varepsilon}) = 1$, then $\text{rk}_\Lambda(\mathcal{S}_+ \cap \mathcal{S}_-) = 1$, since both \mathcal{S}_+ and \mathcal{S}_- are submodules of the rank one Λ -module \mathcal{S}_{rel} . By Proposition 3.4, $\mathcal{S}_+ \cap \mathcal{S}_- \subset \mathcal{S}_{\text{str}}$, and so also $\text{rk}_\Lambda(\mathcal{S}_{\text{str}}) = 1$. But then $\mathcal{S}_{\text{rel}}/\mathcal{S}_{\text{str}}$ is a Λ -torsion module. This quotient injects into \mathcal{H}^1 which is torsion-free by Proposition 3.4. We conclude that $\mathcal{S}_{\text{str}} = \mathcal{S}_{\text{rel}}$ and that the localization map $\mathcal{S}_{\text{rel}} \rightarrow \mathcal{H}^1$ is trivial, contradicting Proposition 3.1.

It now follows that $\mathrm{rk}_\Lambda(\mathcal{S}_{-\varepsilon}) = \mathrm{rk}_\Lambda(\mathcal{S}_{\mathrm{str}}) = 0$, and since $\mathcal{S}_{\mathrm{rel}}$ is torsion-free, this implies that both $\mathcal{S}_{-\varepsilon}$ and $\mathcal{S}_{\mathrm{str}}$ are equal to zero. \square

4. CHARACTERISTIC IDEALS

Theorem 4.1. *We have the equality of characteristic ideals*

$$\mathrm{Char}_\Lambda(X_{\mathrm{rel}, \Lambda\text{-tor}}) = \mathrm{Char}_\Lambda(X_{\mathrm{str}}).$$

Proof. Let K_∞/K denote the unique \mathbf{Z}_p^2 -extension of K , and set $\Lambda(K_\infty) := \mathcal{O}_p[[\mathrm{Gal}(K_\infty/K)]]$. Write $X(K_\infty) := \mathrm{Hom}(\mathrm{Sel}(K_\infty), \mathbf{Q}_p/\mathbf{Z}_p)$. It follows from Rubin's proof of the main conjecture that $\mathrm{rk}_{\Lambda(K_\infty)}(X(K_\infty)) = 1$ (see e.g. [15, Remark 2.2] and [13, Theorem 5.3(iii)]). As $X_{\mathrm{rel}} = X$ (see [2, Remark 3.3], for instance), Proposition 3.3(i) implies that $\mathrm{rk}_\Lambda(X) = 1$ also. Hence, if γ_1 is any topological generator of $\mathrm{Gal}(K_\infty/D_\infty)$, then, since

$$\frac{X(K_\infty)}{(\gamma_1 - 1)X(K_\infty)} \simeq X$$

(see [11, Proposition 1.2 and Theorem 2.1] or [2, p. 364–365]), we deduce that $\gamma_1 - 1$ is coprime to $\mathrm{Char}_{\Lambda(K_\infty)}(X(K_\infty)_{\mathrm{tor}})$. The theorem now follows directly from [2, Theorem 3.24] and [1, Lemma 2.1.2] (see also [16, Corollary 6.5] for a more general result along these lines). \square

Theorem 4.2. *Suppose that the sign of $W(\psi)$ is equal to ε . Then*

$$\mathrm{Char}_\Lambda(X_{\varepsilon, \Lambda\text{-tor}}) \mathrm{Char}_\Lambda\left(\frac{\mathcal{H}_\varepsilon^1}{\mathcal{S}_\varepsilon}\right) = \mathrm{Char}_\Lambda\left(\frac{\mathcal{S}_{\mathrm{rel}}}{\mathcal{C}}\right). \quad (4.1)$$

If we assume that Conjecture 3.5 is true then $\mathcal{S}_\varepsilon = \mathcal{S}_{\mathrm{rel}}$ and

$$\mathrm{Char}_\Lambda(X_{-\varepsilon}) = \mathrm{Char}_\Lambda\left(\frac{\mathcal{H}_\varepsilon^1}{\mathcal{C}}\right). \quad (4.2)$$

Proof. From Proposition 3.1, we see that $\mathcal{C} \subset \mathcal{S}_\varepsilon$, and so $\mathrm{rk}_\Lambda(\mathcal{C}) = \mathrm{rk}_\Lambda(\mathcal{S}_\varepsilon) = 1$. Via global duality (see [14, Theorem 1.7.3]), together with the fact that $\mathcal{S}_{\mathrm{str}} = 0$, we have the exact sequence

$$0 \rightarrow \mathcal{S}_\varepsilon \rightarrow \mathcal{H}_\varepsilon^1 \rightarrow X_{\mathrm{rel}} \rightarrow X_\varepsilon \rightarrow 0. \quad (4.3)$$

As $\mathcal{H}^1/\mathcal{S}_\varepsilon$ is Λ -torsion, it is not hard to check that this in turn yields the exact sequence

$$0 \rightarrow \mathcal{H}_\varepsilon^1/\mathcal{S}_\varepsilon \rightarrow X_{\mathrm{rel}, \Lambda\text{-tor}} \rightarrow X_{\varepsilon, \Lambda\text{-tor}} \rightarrow 0. \quad (4.4)$$

The equality (4.1) now follows from (4.4) together with Theorem 4.1 and Proposition 3.3(ii).

Now assume Conjecture 3.5. Then (3.3) gives an injection $\mathcal{S}_{\mathrm{rel}}/\mathcal{S}_\varepsilon \hookrightarrow \mathcal{H}^1/\mathcal{H}_\varepsilon^1$ of a torsion module into a torsion-free module. Hence $\mathcal{S}_\varepsilon = \mathcal{S}_{\mathrm{rel}}$. In order to show (4.2), we observe that, as $\mathcal{S}_{-\varepsilon} = 0$, (3.3) yields

$$0 \rightarrow \mathcal{H}_\varepsilon^1/\mathcal{S}_\varepsilon \rightarrow X_{-\varepsilon} \rightarrow X_{\mathrm{str}} \rightarrow 0.$$

Combining this with the exactness of

$$0 \rightarrow \mathcal{S}_\varepsilon/\mathcal{C} \rightarrow \mathcal{H}_\varepsilon^1/\mathcal{C} \rightarrow \mathcal{H}_\varepsilon^1/\mathcal{S}_\varepsilon \rightarrow 0$$

and with Proposition 3.3 proves the equality (4.2). \square

Let ε be the sign of $W(\psi)$, and write $\bar{\psi}$ denote the complex conjugate of the grossencharacter ψ . Fix a generator c_ε of \mathcal{H}_ε .

Theorem 4.3. *Assume that Conjecture 3.5 holds. Then there exists a generator $\mathcal{L}_{-\varepsilon}$ of $\text{Char}_\Lambda(\mathcal{H}_\varepsilon^1/\mathcal{C})$ such that the following statement is true:*

Let χ be any character of Γ of order p^n , where $n > 0$ and satisfies $(-1)^{n+1} = W(\psi)$. Then

$$\delta_\chi(v_\varepsilon) \cdot \chi(\mathcal{L}_{-\varepsilon}) = \frac{L(\bar{\psi}\chi, 1)}{\Omega_E}.$$

Here $\Omega_E \in \mathbf{R}^+$ is the real period of a minimal model of E , $v_\varepsilon \in V_\varepsilon$ is the image of c_ε under a fixed choice of the isomorphism (3.2), and δ_χ is the Coates-Wiles homomorphism defined in [12, §2]. Furthermore, $\delta_\chi(v_\varepsilon)$ is always non-zero.

Proof. This is a direct consequence of [12, §10], once we fix a choice of isomorphism (3.2) above. (One must also bear in mind the last part of Remark 3.2.) \square

Now Theorems 4.2 and 4.3 imply that if Conjecture 3.5 holds, then

$$\mathcal{L}_{-\varepsilon}\Lambda = \text{Char}_\Lambda(\mathcal{H}_\varepsilon^1/\mathcal{C}) = \text{Char}_\Lambda(X_{-\varepsilon}).$$

Hence we see that Conjecture 3.5 implies that $\text{Char}_\Lambda(X_{-\varepsilon})$ is generated by an element which p -adically interpolates suitably normalised special values of twists of $L(\bar{\psi}, s)$, and which may therefore be viewed as being a p -adic L -function attached to E .

5. CONTROL THEOREMS

Define

$$X_{n,*} = \text{Hom}_{\mathcal{O}_p}(\text{Sel}_*(D_n, W), K_p/\mathcal{O}_p).$$

Our goal in this section is to explain how to recover the \mathcal{O}_p -rank of X_n from the Λ -modules X_\pm .

Fix a topological generator $\gamma \in \text{Gal}(D_\infty/K)$ and define

$$\omega_n^+ = \prod_{1 \leq k \leq n, k \text{ even}} \Phi_{p^k}(\gamma) \quad \omega_n^- = (\gamma - 1) \prod_{1 \leq k \leq n, k \text{ odd}} \Phi_{p^k}(\gamma)$$

where Φ_{p^k} is the p^k -th cyclotomic polynomial. Since $\chi(\omega_n^\pm) = 0$ for every $\chi \in \Xi_n^\pm$, we have

$$\begin{aligned} \omega_n^\mp \cdot \mathbf{E}(D_{n,p}) &\subset E_\pm(D_{n,p}) \\ \omega_n^\mp \cdot \text{Sel}(D_n, W) &\subset \text{Sel}_\pm(D_n, W) \end{aligned} \tag{5.1}$$

and similarly $\omega_n^\pm \cdot E_\pm(D_{n,p}) = 0$.

Lemma 5.1. *The natural map*

$$f_n : H_\pm^1(D_{n,p}, W) \rightarrow H_\pm^1(D_{\infty,p}, W)[\omega_n^\pm]$$

is injective, and the \mathcal{O}_p -corank of the cokernel of f_n is a bounded, non-decreasing function of n . If Conjecture 3.5 holds then the cokernel of f_n is finite for all n .

Proof. Let L denote the extension of $K_{\mathfrak{p}}$ obtained by adjoining $E[\mathfrak{p}]$ to $K_{\mathfrak{p}}$. Then it follows from Lubin-Tate theory that $L/K_{\mathfrak{p}}$ is a totally ramified extension of degree $p^2 - 1$. Hence $L \cap D_{\infty, \mathfrak{p}} = K_{\mathfrak{p}}$, and we deduce that $H^0(D_{\infty, \mathfrak{p}}, W) = 0$. From the inflation-restriction sequence we deduce that

$$H^1(D_{n, \mathfrak{p}}, W) \rightarrow H^1(D_{\infty, \mathfrak{p}}, W),$$

and therefore also f_n , is injective. To prove the rest of the lemma, we compare the $\mathcal{O}_{\mathfrak{p}}$ -coranks of $H_{\pm}^1(D_{n, \mathfrak{p}}, W)$ and $H_{\pm}^1(D_{\infty, \mathfrak{p}}, W)[\omega_n^{\pm}]$.

From Proposition 3.4 and the general structure theory of Λ -modules, we see that the $\mathcal{O}_{\mathfrak{p}}$ -corank of $H_{\pm}^1(D_{\infty, \mathfrak{p}}, W)[\omega_n^{\pm}]$ is equal to $\text{rk}_{\mathcal{O}_{\mathfrak{p}}}(\Lambda/\omega_n^{\pm}\Lambda) + e(n)$, where $e(n)$ is a non-decreasing, bounded function of n . If Conjecture 3.5 holds, then the Λ -module $H_{\pm}^1(D_{\infty}, W)$ is cotorsion-free, and so $e(n) = 0$ for all n . On the other hand, there is an isomorphism of $K_{\mathfrak{p}}[\text{Gal}(D_{n, \mathfrak{p}}/K_{\mathfrak{p}})]$ -modules

$$\mathbf{E}(D_{n, \mathfrak{p}}) \otimes_{\mathcal{O}_{\mathfrak{p}}} K_{\mathfrak{p}} \simeq D_{n, \mathfrak{p}} \simeq K_{\mathfrak{p}}[\text{Gal}(D_{n, \mathfrak{p}}/K_{\mathfrak{p}})], \quad (5.2)$$

in which the first isomorphism is induced by the logarithm of the formal group \mathbf{E} , and the second follows from the normal basis theorem of Galois theory. This implies that the $\mathcal{O}_{\mathfrak{p}}$ -corank of $H_{\pm}^1(D_{n, \mathfrak{p}}, W)$ is equal to the $\mathcal{O}_{\mathfrak{p}}$ -rank of Λ/ω_n^{\pm} . The result now follows immediately. \square

The following result is an anticyclotomic analogue of Kobayashi's control theorem (see [5, Theorem 9.3]).

Theorem 5.2. *The natural map*

$$X_{\pm}/\omega_n^{\pm}X_{\pm} \rightarrow X_{n, \pm}/\omega_n^{\pm}X_{n, \pm} \quad (5.3)$$

is surjective. The $\mathcal{O}_{\mathfrak{p}}$ -rank of the kernel is a bounded, nondecreasing function of n . If Conjecture 3.5 holds, then the kernel is finite for all n .

Proof. Write

$$\begin{aligned} L_{n, \pm} &= H^1(D_{n, \mathfrak{p}}, W)[\omega_n^{\pm}]/H_{\pm}^1(D_{n, \mathfrak{p}}, W), \\ L_{\infty, \pm} &= H^1(D_{\infty, \mathfrak{p}}, W)[\omega_n^{\pm}]/H_{\pm}^1(D_{\infty, \mathfrak{p}}, W)[\omega_n^{\pm}]. \end{aligned}$$

Let \mathbf{K} denote the maximal extension of K unramified outside \mathfrak{fp} and set

$$H^1(D_{n, \mathfrak{f}}, W) = \bigoplus_{v|\mathfrak{f}} H^1(D_{n, v}, W), \quad H^1(D_{\infty, \mathfrak{f}}, W) = \bigoplus_{v|\mathfrak{f}} H^1(D_{\infty, v}, W).$$

Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Sel}_{\pm}(D_n, W)[\omega_n^{\pm}] & \longrightarrow & H^1(\mathbf{K}/D_n, W)[\omega_n^{\pm}] & \longrightarrow & H^1(D_{n, \mathfrak{f}}, W) \oplus L_{n, \pm} \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{Sel}_{\pm}(D_{\infty}, W)[\omega_n^{\pm}] & \longrightarrow & H^1(\mathbf{K}/D_{\infty}, W)[\omega_n^{\pm}] & \longrightarrow & H^1(D_{\infty, \mathfrak{f}}, W) \oplus L_{\infty, \pm} \end{array}$$

The left-hand vertical arrow of this diagram is the dual of the map (5.3). Since $H^1(\mathbf{K}/D_n, W) \cong H^1(\mathbf{K}/D_{\infty}, W)[\gamma^{p^n} - 1]$, the middle vertical arrow is an isomorphism. To prove the theorem, it therefore suffices (by the Snake Lemma) to show that the $\mathcal{O}_{\mathfrak{p}}$ -corank of the kernel of the right-hand arrow is a bounded, non-decreasing function of n , and is finite for all n if Conjecture 3.5 holds.

For any place v of D_∞ dividing \mathfrak{f} , the extension $D_{\infty,v}/D_{n,v}$ is either trivial (in which case there is nothing to check) or is the unique unramified \mathbf{Z}_p -extension of $D_{n,v}$. Assume we are in the latter case. The kernel of

$$H^1(D_{n,v}, W) \rightarrow H^1(D_{\infty,v}, W)$$

is isomorphic to $H^1(D_{\infty,v}/D_{n,v}, E(D_{\infty,v})[p^\infty])$, which is isomorphic to a quotient of $E(D_{\infty,v})[p^\infty]$. Since the Galois module W is ramified at all primes dividing \mathfrak{f} , it follows that $E(D_{\infty,v})[p^\infty]$ is a proper $\mathcal{O}_{\mathfrak{p}}$ submodule of W . This implies that $E(D_{\infty,v})[p^\infty]$ is finite, because W is cofree of corank one over $\mathcal{O}_{\mathfrak{p}}$, and so any proper submodule of W is finite.

In order to control the kernel of $L_{n,\pm} \rightarrow L_{\infty,\pm}$, we apply the Snake Lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_{\pm}^1(D_{n,p}, W) & \longrightarrow & H^1(D_{n,p}, W)[\omega_n^{\pm}] & \longrightarrow & L_{n,\pm} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H_{\pm}^1(D_{\infty,p}, W)[\omega_n^{\pm}] & \longrightarrow & H^1(D_{\infty,p}, W)[\omega_n^{\pm}] & \longrightarrow & L_{\infty,\pm} & \longrightarrow & 0. \end{array}$$

Just as in the proof of Lemma 5.1, we deduce from the inflation-restriction sequence that the middle vertical arrow of this diagram is injective; the same inflation-restriction sequence also shows that that this arrow is surjective. We therefore deduce from Lemma 5.1 that the $\mathcal{O}_{\mathfrak{p}}$ -corank of the kernel of the right-hand vertical arrow of this diagram is a bounded, non-decreasing function of n , and is finite for all n if Conjecture 3.5 holds. This completes the proof. \square

Proposition 5.3. *For any n , the natural map*

$$X_n \rightarrow (X_{n,+}/\omega_n^+ X_{n,+}) \oplus (X_{n,-}/\omega_n^- X_{n,-})$$

has finite kernel and cokernel.

Proof. Consider the dual map

$$\mathrm{Sel}_+(D_n, W)[\omega_n^+] \oplus \mathrm{Sel}_-(D_n, W)[\omega_n^-] \rightarrow \mathrm{Sel}(D_n, W). \quad (5.4)$$

By (5.1) and the equality $\omega_n^{\pm} \omega_n^{\mp} = \gamma^{p^k} - 1$, there is an inclusion

$$\omega_n^- \cdot \mathrm{Sel}(D_n, W) + \omega_n^+ \cdot \mathrm{Sel}(D_n, W) \subset \mathrm{Sel}_+(D_n, W)[\omega_n^+] + \mathrm{Sel}_-(D_n, W)[\omega_n^-].$$

Since

$$\mathrm{Sel}(D_n, W) / (\omega_n^- \cdot \mathrm{Sel}(D_n, W) + \omega_n^+ \cdot \mathrm{Sel}(D_n, W))$$

is a module of cofinite type over the finite ring $\Lambda/(\omega_n^+, \omega_n^-)$, it is finite, and therefore the same is true of the cokernel of (5.4). The kernel of (5.4) is isomorphic to

$$\mathrm{Sel}_+(D_n, W)[\omega_n^+] \cap \mathrm{Sel}_-(D_n, W)[\omega_n^-]$$

which is again a cofinite type module over $\Lambda/(\omega_n^+, \omega_n^-)$, and is therefore also finite. \square

Combining Theorem 3.6, Theorem 5.2, and Proposition 5.3 we obtain the following result.

Theorem 5.4. *Let ε be the sign of $W(\psi)$. There is an integer e , independent of n , such that*

$$\text{corank}_{\mathcal{O}_p}(\text{Sel}(D_n, W)) = \text{rank}_{\mathcal{O}_p}(\Lambda/\omega_n^\varepsilon) + e$$

for $n \gg 0$. If Conjecture 3.5 holds then the \mathcal{O}_p -corank of $\text{Sel}(D_n, W)$ is equal to

$$\text{rank}_{\mathcal{O}_p}(\Lambda/\omega_n^\varepsilon) + \text{rank}_{\mathcal{O}_p}(Y_+/\omega_n^+ Y_+) + \text{rank}_{\mathcal{O}_p}(Y_-/\omega_n^- Y_-)$$

for all n , where Y_\pm is the Λ -torsion submodule of X_\pm . □

Theorem A of the Introduction now follows from the first part of Theorem 5.4.

REFERENCES

- [1] A. Agboola, B. Howard. Anticyclotomic Iwasawa theory for CM elliptic curves. Preprint (2003).
- [2] P. Billot. Quelques aspects de la descente sur une courbe elliptique dans le cas de réduction supersingulière. *Comp. Math.* 58 (1986) 341–369.
- [3] R. Greenberg. On the Birch and Swinnerton-Dyer conjecture. *Invent. Math.* 72 (1983) 241–265.
- [4] K. Kato. p -adic Hodge theory and values of zeta functions of modular forms. In: Cohomologies p -adiques et applications arithmétiques III. *Asterisque* 295 (2004), ix, 117–290.
- [5] S. Kobayashi. Iwasawa theory for elliptic curves at supersingular primes. *Invent. Math.* 152 (2003) 1–36.
- [6] B. Perrin-Riou. Arithmétique des courbes elliptiques à réduction supersingulière en p . *Experiment. Math.* 12 (2003), no. 2, 155–186.
- [7] B. Perrin-Riou. Fonctions L p -adiques d’une courbe elliptique et points rationnelles. *Ann. Inst. Fourier* 43 (1993) 945–995.
- [8] B. Perrin-Riou. Théorie d’Iwasawa et hauteurs p -adiques. *Invent. Math.* 109 (1992) 137–185.
- [9] R. Pollack, On the p -adic L -function of a modular form at a supersingular prime. *Duke Math. J.* 118 (2003) 523–558.
- [10] D. Rohrlich. On L -functions of elliptic curves and anticyclotomic towers. *Invent. Math.*, 75 (1984) 383–408.
- [11] K. Rubin. Elliptic curves and \mathbf{Z}_p -extensions. *Comp. Math.* 56 (1985) 237–250.
- [12] K. Rubin. Local units, elliptic units, Heegner points and elliptic curves. *Invent. Math.* 88 (1987) 405–422.
- [13] K. Rubin. The “main conjectures” of Iwasawa theory for imaginary quadratic fields. *Invent. Math.* 103 (1991) 25–68.
- [14] K. Rubin. *Euler Systems*. Princeton University Press, (2000).
- [15] K. Rubin, R. Pollack. The main conjecture for elliptic curves at supersingular primes. *Ann. Math.* 159 (2004) no. 1, 447–464.
- [16] K. Wingberg. Duality theorems for abelian varieties over \mathbf{Z}_p -extensions. *Advanced Studies in Pure Mathematics* 17 (1989) 471–492.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SANTA BARBARA, CA, 93106

E-mail address: `agboola@math.ucsb.edu`

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MA, 02138

Current address: Department of Mathematics, University of Chicago, 5734 S. University Ave., Chicago, IL, 60637

E-mail address: `howard@math.uchicago.edu`