Some remarks on the two-variable main conjecture of Iwasawa theory for elliptic curves without complex multiplication

Jeanine Van Order *

Abstract

We establish several results towards the two-variable main conjecture of Iwasawa theory for elliptic curves without complex multiplication over imaginary quadratic fields, namely (i) the existence of an appropriate p-adic L-function, building on works of Hida and Perrin-Riou, (ii) the basic structure theory of the dual Selmer group, following works of Coates, Hachimori-Venjakob, et al., and (iii) the implications of dihedral or anti-cyclotomic main conjectures with basechange. The result of (i) is deduced from the construction of Hida and Perrin-Riou, which in particular is seen to give a bounded distribution. The result of (ii) allows us to deduce a corank formula for the p-primary part of the Tate-Shafarevich group of an elliptic curve in the $\mathbf{Z}_p^2$-extension of an imaginary quadratic field. Finally, (iii) allows us to deduce a criterion for one divisibility of the two-variable main conjecture in terms of specializations to cyclotomic characters, following a suggestion of Greenberg, as well as a refinement via basechange.

1 Introduction

Fix a prime $p \in \mathbf{Z}$. Given a profinite group G, let $\Lambda(G)$ denote the $\mathbf{Z}_p$-Iwasawa algebra of G, which is the completed group ring

$$\Lambda(G) = \mathbf{Z}_p[[G]] = \varprojlim_U \mathbf{Z}_p[G/U].$$

Here, the projective limit runs over all open normal subgroups U of G. Note that the elements of $\Lambda(G)$ can be viewed in a natural way as $\mathbf{Z}_p$-valued measures on G. Let E be an elliptic curve defined over $\mathbf{Q}$ of conductor N. Hence E is modular by fundamental work of Wiles [47], Taylor-Wiles [41], and Breuil-Conrad- Diamond-Taylor [3], with Hasse-Weil L-function $L(E, s)$ given by that of a cuspidal newform $f \in S_2(\Gamma_0(N))$.

Let k be an imaginary quadratic field. The Hasse-Weil L-function $L(E/k, s)$ of E over k is given by the Rankin-Selberg L-function $L(f \times \Theta_k, s)$, where Θ_k is the theta series associated to k by a classical construction (as described for

*The author acknowledges support from the Swiss National Science Foundation (FNS) grant 200021-125291.

instance in [11]). Let k_∞ denote the compositum of all $\mathbf{Z}_p$-extensions of k, which by class field theory is a $\mathbf{Z}_p^2$-extension. Let G denote the Galois group $\mathrm{Gal}(k_\infty/k)$. The complex conjugation automorphism of $\mathrm{Gal}(k/\mathbf{Q})$ acts on G with eigenvalues ± 1. Let k^{cyc} denote the $\mathbf{Z}_p$-extension associated to the $+1$-eigenspace, which is the cyclotomic $\mathbf{Z}_p$-extension of k. Let D_∞ denote the $\mathbf{Z}_p$-extension associated to the -1-eigenspace, which is the dihedral or anticyclotomic $\mathbf{Z}_p$-extension of k. Let Γ denote the cyclotomic Galois group $\mathrm{Gal}(k^{\mathrm{cyc}}/k)$, and let Ω denote the dihedral or anticyclotomic Galois group $\mathrm{Gal}(D_\infty/k)$. Let H denote the Galois group $\mathrm{Gal}(k_\infty/k^{\mathrm{cyc}})$, which is naturally isomorphic to $\Omega \cong \mathbf{Z}_p$. Let $X(E/k_\infty)$ denote the Pontryagin dual of the p^∞-Selmer group of E over k_∞, which has the natural structure of a compact $\Lambda(G)$-module. The subject of this note is the following conjecture, made in the spirit of Iwasawa (but often attributed to Greenberg and Mazur), known as the *two-variable main conjecture of Iwasawa theory for elliptic curves*:

Conjecture 1.1 *Let E be an elliptic curve defined over $\mathbf{Q}$, and p a prime where E has either good ordinary or multiplicative reduction.*

(i) There is a unique element $L_p(E/k_\infty) \in \Lambda(G)$ that interpolates p-adically the central values $L(E/k, \mathcal{W}, 1)/\Omega_f$. Here, $L(E/k, \mathcal{W}, s)$ is the Hasse-Weil L-function of E over k twisted by a finite order character $\mathcal{W}$ of G, and Ω_f is a suitable complex period for which the quotient $L(E/k, \mathcal{W}, 1)/\Omega_f$ lies in $\overline{\mathbf{Q}}$ (and hence in $\overline{\mathbf{Q}}_p$ via any fixed embedding $\overline{\mathbf{Q}} \to \overline{\mathbf{Q}}_p$).

(ii) The dual Selmer group $X(E/k_\infty)$ is $\Lambda(G)$-torsion, hence has a $\Lambda(G)$-characteristic power series $\mathrm{char}_{\Lambda(G)} X(E/k_\infty)$.

(iii) The equality of ideals $(L_p(E/k_\infty)) = \left(\mathrm{char}_{\Lambda(G)} X(E/k_\infty)\right)$ holds in $\Lambda(G)$.

In the setting where E has complex multiplication by k, much is known about this conjecture thanks to work of Rubin [35] (see also [36]), building on previous work of Coates-Wiles [6] and Yager [48]. Here, we consider the somewhat more mysterious setting where E does *not* have complex multiplication, and in particular what can be deduced from known Iwasawa theoretic results for the one-variable cases corresponding to the Galois groups Γ and Ω.

We start with the construction of p-adic L-functions, (i). Given a finite order character $\mathcal{W}$ of G, let $\mathcal{W}(\lambda)$ denote the specialization to $\mathcal{W}$ of an element $\lambda \in \Lambda(G)$. That is, writing $d\lambda$ to denote the measure associated to λ, let

$$\mathcal{W}(\lambda) = \int_G \mathcal{W}(g) \cdot d\lambda(g).$$

Fix a cuspidal Hecke eigenform $f \in S_2(\Gamma_0(N))$ of weight 2, level N, and trivial Nebentypus. Such an eigenform $f \in S_2(\Gamma_0(N))$ is said to be *p-ordinary* if its T_p-eigenvalue is a p-adic unit with respect to any embedding $\overline{\mathbf{Q}} \to \overline{\mathbf{Q}}_p$. Let

$$\langle f, f \rangle_N = \int_{\Gamma_0(N)\backslash \mathfrak{H}} |f|^2 dxdy$$

denote the Petersson inner product of f with itself. Let $L(f \times \Theta(\mathcal{W}), s)$ denote the Rankin-Selberg L-function of f times the theta series $\Theta(\mathcal{W})$ associated to $\mathcal{W}$, normalized to have central value at $s = 1$. The ratio

$$\frac{L(f \times \Theta(\mathcal{W}), 1)}{8\pi^2 \langle f, f \rangle_N}$$

lies in $\overline{\mathbf{Q}}$ by an important theorem of Shimura [39]. Using this fact, along with the constructions of Hida [14] and Perrin-Riou [32], we obtain the following result.

Theorem 1.2 (Theorem 2.9) *Fix an embedding $\overline{\mathbf{Q}} \to \overline{\mathbf{Q}}_p$. Let $f \in S_2(\Gamma_0(N))$ be a p-ordinary eigenform of weight 2, level N, and trivial Nebentypus. Assume that N is prime to the discriminant of k, and that $p \geq 5$. There exists an element $\mu_f \in \Lambda(G)$ whose specialization to any finite order character $\mathcal{W}$ of G satisfies the interpolation formula*

$$\mathcal{W}(\mu_f) = \eta \cdot \frac{L(f \times \Theta(\overline{\mathcal{W}}), 1)}{8\pi^2 \langle f, f \rangle_N} \in \overline{\mathbf{Q}}_p,$$

where $\eta = \eta(f, \mathcal{W})$ is a certain explicit (nonvanishing) algebraic number.

Hence, we obtain a p-adic L-function $L_p(E/k_\infty) = L_p(f/k_\infty) \in \Lambda(G)$ associated to this measure μ_f.

Remark The two-variable p-adic L-function $L_p(f/k_\infty)$ corresponding to $d\mu_f$ also satisfies a functional equation, as described in Corollary 2.10 below.

We now consider the Iwasawa module structure theory of (ii), using standard techniques. Recall that we let H denote the Galois group $\mathrm{Gal}(k_\infty/k^{\mathrm{cyc}})$, which is naturally isomorphic to the dihedral or anticyclotomic Galois group $\Omega \cong \mathbf{Z}_p$. If E has good ordinary reduction at p, then an important theorem of Kato [23] with a nonvanishing theorem of Rohrlich [34] implies that the dual Selmer group $X(E/k^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. To be more precise, the construction of Kato [23] with the nonvanishing theorem of Rohlich [34] show that the dual Selmer group $X(E/\mathbf{Q}^{\mathrm{cyc}})$ is $\Lambda(\mathrm{Gal}(\mathbf{Q}^{\mathrm{cyc}}/\mathbf{Q}))$-torsion, where $\mathbf{Q}^{\mathrm{cyc}}$ denotes the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. It then follows from a simple restriction argument, using Artin formalism for abelian L-functions, that the analogous structure theorem holds for E in the cyclotomic $\mathbf{Z}_p$-extension of any abelian number field. In particular, $X(E/k^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion, and hence has a $\Lambda(\Gamma)$-characteristic power series with associated cyclotomic Iwasawa invariants $\mu_E(k) = \mu_{\Lambda(\Gamma)}(X(E/k^{\mathrm{cyc}}))$ and $\lambda_E(k) = \lambda_{\Lambda(\Gamma)}(X(E/k^{\mathrm{cyc}}))$. Using this result, we then deduce the following structure theorem for the dual Selmer group $X(E/k_\infty)$.

Theorem 1.3 *Let $E/\mathbf{Q}$ be an elliptic curve with good ordinary reduction at each prime above p in k.*

(i) (Theorem 3.8) The dual Selmer group $X(E/k_\infty)$ is $\Lambda(G)$-torsion, hence has a $\Lambda(G)$-characteristic power series $\mathrm{char}_{\Lambda(G)} X(E/k_\infty)$.

(ii) (Theorem 3.13) If the cyclotomic invariant $\mu_E(k)$ vanishes, then the two-variable invariant $\mu_{\Lambda(G)}\left(X(E/k_\infty)\right)$ also vanishes.

(iii) (Theorem 3.11) Let $\mathrm{char}_{\Lambda(G)} X(E/k_\infty)(0)$ denote the image of the characteristic power series $\mathrm{char}_{\Lambda(G)} X(E/k_\infty)$ under the augmentation map $\Lambda(G) \longrightarrow \mathbf{Z}_p$. If $p \geq 5$ and the p^∞-Selmer group $\mathrm{Sel}(E/k)$ is finite, then

$$|\,\mathrm{char}_{\Lambda(G)} X(E/k_\infty)(0)|_p = \frac{|E(k)_{p^\infty}|^2}{|\ Ш(E/k)(p)|} \cdot \frac{\prod_v |c_v|_p}{\prod_{v|p} |\widetilde{E}_v(\kappa_v)(p)|^2}.$$

Here, $Ш(E/k)(p)$ denotes the p-primary part of the Tate-Shafarevich group $Ш(E/k)$ of E over k, $E(k)_{p^\infty}$ the p-primary part of the Mordell-Weil group $E(k)$, κ_v the residue field at v, $\widetilde{E}_v$ the reduction of E over κ_v, and $c_v = [E(k_v) : E_0(k_v)]$ the local Tamagawa factor at a prime $v \subset \mathcal{O}_k$.

(iv) (Theorem 3.12) If $\mu_E(k) = 0$, then there is an isomorphism of $\Lambda(H)$-modules $X(E/k_\infty) \cong \Lambda(H)^{\lambda_E(k)}$.

We also obtain from this the following application to Tate-Shafarevich ranks. Consider the short exact descent sequence of discrete $\Lambda(H)$-modules

$$0 \longrightarrow E(k_\infty) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathrm{Sel}(E/k_\infty) \longrightarrow\ Ш(E/k_\infty)(p) \longrightarrow 0.$$

Here, $E(k_\infty)$ denotes the Mordell-Weil group of E over k_∞, and $Ш(E/k_\infty)(p)$ denotes the p-primary part of the Tate-Shafarevich group of E over k_∞.

Proposition 1.4 (Proposition 3.14) *Assume that p is odd, and moreover that p does not divide the class number of k if the root number $\epsilon(E/k, 1)$ equals -1. If E has good ordinary reduction at p with $\mu_E(k) = 0$, then*

$$\mathrm{corank}_{\Lambda(H)}\ Ш(E/k_\infty)(p) = \begin{cases} \lambda_E(k) & \text{if } \epsilon(E/k,1) = +1 \\ \lambda_E(k) - 1 & \text{if } \epsilon(E/k,1) = -1. \end{cases}$$

Example Consider the elliptic curve $E = 53a : y^2 + xy + y = x^3 - x^2$ at $p = 5$ over $k = \mathbf{Q}(\sqrt{-31})$. The discriminant of k is -31, which is prime to both 5 and the conductor 53 of E. A simple calculation shows that the root number $\epsilon(E/k, 1)$ is $+1$. Moreover, the mod 5 Galois representation associated to E is surjective, as shown by the calculations in Serre [37, § 5.4]. Computations of Pollack [30] show that $\mu_E(k) = 0$ with $\lambda_E(k) = 9$ (and moreover that the Mordell-Weil rank of $E(k)$ is 1), from which we deduce that $Ш(E/k_\infty)(5)$ has $\Lambda(H)$-corank 9. In particular, $Ш(E/k_\infty)(5)$ contains infinitely many copies of $\mathbf{Q}_5/\mathbf{Z}_5$.

Finally, we establish the following criterion for one divisibility of (iii) in terms of specializations to cyclotomic characters, following a suggestion of Ralph Greenberg. To be more precise, let Ψ denote the set of finite order characters of

the Galois group $\Gamma = \mathrm{Gal}(k^{\mathrm{cyc}}/k)$. Given a character $\psi \in \Psi$, let us write $\mathcal{O}_\psi$ to denote the ring obtained from adjoining to $\mathbf{Z}_p$ the values of ψ. Let $L_p(E/k_\infty)|_\Omega$ denote the image of the two-variable p-adic L-function $L_p(E/k_\infty)$ in the Iwasawa algebra $\Lambda(\Omega)$.

Theorem 1.5 (Corollary 4.2) *Assume that p does not divide $L_p(E/k_\infty)|_\Omega$, and that for each character $\psi \in \Psi$, we have the inclusion of ideals*

$$(\psi\,(L_p(E/k_\infty))) \subseteq \left(\psi\left(\mathrm{char}_{\Lambda(G)}\, X(E/k_\infty)\right)\right) \text{ in } \mathcal{O}_\psi[[G]]. \tag{1}$$

Then, we have the inclusion of ideals

$$(L_p(E/k_\infty)) \subseteq \left(\mathrm{char}_{\Lambda(G)}\, X(E/k_\infty)\right) \text{ in } \Lambda(G). \tag{2}$$

We deduce from this the following result. Let K be any finite extension of k contained in the cyclotomic $\mathbf{Z}_p$-extension k^{cyc}. Let Ω_K denote the Galois group $\mathrm{Gal}(KD_\infty/k)$, which is topologically isomorphic to $\mathbf{Z}_p$. Let $L_p(E/k_\infty)|_{\Omega_K}$ denote the image of the two-variable p adic L-function $L_p(E/k_\infty)$ in the Iwasawa algebra $\Lambda(\Omega_K)$. Let Ψ_K denote the set of characters of order $[K:k]$ of the Galois group $\mathrm{Gal}(K/k)$. Let us consider as well the following condition(s), so that we can invoke the recent work of Pollack-Weston [31].

Hypothesis 1.6 *Let $\epsilon(E/k,1) \in \{\pm 1\}$ denote the root number of the complex L-function $L(E/k,s) = L(f \times \theta_k, s)$. We assume that:*

(i) The mod p Galois representation $\overline{\rho}_E$ associated to E is surjective.

(ii) If $\epsilon(E/k,1) = +1$, then $p \geq 5$ and the conductor N is prime to the discriminant of k. This latter condition determines an integer factorization $N = N^+N^-$ of N, where N^+ is divisible only by primes that split in k, and N^- is divisible only by primes that remain inert in k; we then assume that N^- is the squarefree product of an odd number of primes.

We obtain the following main result.

Proposition 1.7 (Proposition 4.3) *Assume that the root number $\epsilon(E/k,1)$ of $L(E/k,1)$ is $+1$. Assume additionally that for a finite extension K of k contained in the cyclotomic $\mathbf{Z}_p$-extension k^{cyc}, we have the inclusion of ideals*

$$(L_p(E/k_\infty)|_{\Omega_K}) \subseteq \left(\mathrm{char}_{\Lambda(\Omega_K)}\, X(E/KD_\infty)\right) \text{ in } \Lambda(\Omega_K), \tag{3}$$

with equality for $K = k$. Then, there exists a nontrivial character $\psi \in \Psi_K$ such that the specialization divisibility (1) *holds. In particular, if Hypothesis 1.6 (i) and (ii) hold, then we obtain the inclusion of ideals*

$$(L_p(E/k_\infty)) \subseteq \left(\mathrm{char}_{\Lambda(G)}\, X(E/k_\infty)\right) \text{ in } \Lambda(G).$$

Though we do not discuss the issue here, the equality condition for $k = K$ would follow from the nonvanishing criterion of Howard [17, Theorem 3.2.3 (c)] for dihedral/anticyclotomic p-adic L-functions, as explained in [43, §5]. Hence, by Proposition 4.3, this criterion would also imply one divisibility of the two-variable main conjecture in the setting where the root number $\epsilon(E/k,1)$ is 1.

Acknowledgements. It is a pleasure to thank John Coates, Ralph Greenberg, David Loeffler, Robert Pollack, Christopher Skinner and Christian Wuthrich for various helpful discussions. In particular, it is a pleasure to thank Christopher Skinner for informing me of the three-variable main conjecture proved in [40], which I had not been aware of before writing this work. It is also a pleasure to thank the anonymous referee for various helpful comments that have done much to improve the exposition, as well as the correctness of some of the writing.

Contents

2 Two-variable p-adic L-functions

We start with the proof of Theorem 2.9, following closely the constructions of Hida [14] and Perrin-Riou [32]. Both of the these constructions depend in an essential way on the bounded linear form defined in [14], which we review below.

Remark The results described below hold more generally for f any p-ordinary eigenform of weight $l \geq 2$ and nontrivial Nebentypus, following the same methods described below with [32, Théorème B]. We have restricted to the setting of eigenforms associated to modular elliptic curves for simplicity of exposition.

Hida's bounded linear form. We follow Hida [14, §4], using the same notations for spaces of modular forms and Hecke algebras used there. Suppose we have a modular form

$$f(z) = \sum_{n \geq 0} a_n(f) e^{2\pi i n z} \in M_l(\Gamma_*(M), \xi; L_0),$$

with l and M positive integers, $* = 0$ or 1, ξ a Dirichlet character mod M, and $L_0 = \mathbf{Q}(a_n(f))_{n \geq 0}$ the extension of $\mathbf{Q}$ generated by the Fourier coefficients of f. We define a norm $|\cdot|_p$ on $f \in M_l(\Gamma_*(M), \xi; L_0)$ by letting

$$|f|_p = \sup_n |a_n(f)|_p .$$

Let L denote the closure of L_0 in $\overline{\mathbf{Q}}_p$ with respect to a fixed embedding $\overline{\mathbf{Q}} \to \overline{\mathbf{Q}}_p$. Let $M_l(\Gamma_*(M), \xi; L)$ denote the completion of the space $M_l(\Gamma_*(M), \xi; L_0)$ with respect to $|\cdot|_p$. Let $\mathcal{O} = \mathcal{O}_L$. Define a subspace of *integral forms*

$$M_l(\Gamma_*(M), \xi; \mathcal{O}) = \{f \in M_l(\Gamma_*(M), \xi; L) : |f|_p \leq 1\}.$$

Let us write $\mathbf{T}(M,\xi;L)$ to denote the algebra of Hecke operators acting on $M_l(\Gamma_*(M),\xi;L)$, as defined in [14, p. 171]. Hence, $\mathbf{T}(M,\xi;L)$ denotes the L-subalgebra of the ring of all L-linear endomorphisms of $M_l(\Gamma_*(M),\xi;L)$ generated by Hecke operators. If given integers $n \geq m \geq 0$, then the restriction $\mathbf{T}(Mp^n,\xi;\mathcal{O})$ of $\mathbf{T}(Mp^n,\xi;L)$ to $M_l(\Gamma_*(Mp^m),\xi;\mathcal{O})$ defines an $\mathcal{O}$-algebra homomorphism

$$M_l(\Gamma_*(Mp^n),\xi;\mathcal{O}) \longrightarrow M_l(\Gamma_*(Mp^m),\xi;\mathcal{O}).$$

We define the *extended Hecke algebra* by passage to the inverse limit with respect to these homomorphisms,

$$\mathbf{T}(M,\xi;\mathcal{O}) = \varprojlim_n \mathbf{T}(Mp^n,\xi,\mathcal{O}).$$

Let us now fix a p-ordinary eigenform

$$f(z) = \sum_{n\geq 1} a_n(f)e^{2\pi inz} \in S_2(\Gamma_0(N))$$

of weight 2, level N, and trivial Nebentypus. Let Ψ denote the principal or trivial character modulo N (hence $\psi(p) = 1$ if p does not divide p, and $\psi(p) = 0$ otherwise). Let $\alpha_p(f)$ denote the p-adic unit root of the polynomial

$$x^2 - a_p(f)x + p\psi(p),$$

and $\beta_p(f)$ the non-unit root. Let f_0 denote p-stabilization of f, which is the unique ordinary form associated to f by Hida [14, Lemma 3.3]. That is, let

$$f_0(z) = \begin{cases} f(z) & \text{if } p \mid N \\ f(z) - \beta_p(f)f(pz) & \text{if } p \nmid N. \end{cases}$$

This eigenform f_0 has level N_0, where

$$N_0 = \begin{cases} Np & \text{if } p \nmid N \\ N & \text{if } p \mid N. \end{cases}$$

Its Fourier coefficients $a_n(f_0)$ satisfy the relations

$$a_n(f_0) = \begin{cases} a_n(f) & \text{if } (n,p) = 1 \\ \alpha_p(f) & \text{if } n = p. \end{cases}$$

We now recall briefly the definition of idempotent operators in extended Hecke algebras, following [14, pp. 171 - 172]. That is, let $\mathbf{T}(Np^m) = \mathbf{T}(\Gamma_0(Np^m);\mathcal{O})$ denote the $\mathcal{O}$-algebra generated by Hecke operators acting on the space of cusp forms $S_2(\Gamma_0(Np^m);\mathcal{O})$, with $T_p = T_p(Np^m)$ denoting the Hecke operator at p. Let $\overline{T}_p$ denote the image of T_p in the quotient $\mathbf{T}(Np^m)/p$. This reduction $\overline{T}_p$ can be decomposed uniquely into semisimple and nilpotent parts. Since $\mathbf{T}(Np^m)/p$ is

a finitely-generated, commutative $\mathbf{F}_p$-algebra, it follows that $\overline{T}_p^{\,p^r}$ is semisimple for r sufficiently large. Hence, $\overline{T}_p^{\,up^r}$ is idempotent for some integer u. Let e_m denote the unique lift to $\mathbf{T}(Np^m)$ of $\overline{T}_p^{\,up^r}$. Note that this lift does not depend on the choice of integer u.

Definition The *idempotent* $\mathbf{e}$ in the extended Hecke algebra $\mathbf{T}(N) = \varprojlim_m \mathbf{T}(Np^m)$ is defined to be the projective limit $\mathbf{e} = \varprojlim_m e_m$.

Proposition 2.1 (Hida) *Let $f \in S_2(\Gamma_0(N))$ be a p-ordinary eigenform, with f_0 its associated ordinary form. There is a decomposition $\mathbf{T}(N;L) \cong A \oplus L$ induced by the split exact sequence*

$$0 \longrightarrow A \oplus L \longrightarrow \mathbf{T}(N;L) \xrightarrow{\phi(f_0)} \mathbf{T}^{(0)}(N;L) \longrightarrow 0. \qquad (4)$$

Here, $\phi(f_0)$ is the map that sends $T_n \longmapsto a_n(f_0)$, with $\mathbf{T}^{(0)}(N;L) \cong L$ the direct summand of $\mathbf{T}(N;L)$ through which this map factors, and A the complementary direct summand.

Proof See [14, Proposition 4.4 and (4.5)]. □

We now use this result to define the following operator.

Definition Let $f \in S_2(\Gamma_0(N))$ be a p-ordinary eigenform with associated ordinary form f_0. We let $\mathbf{1}_{f_0}$ denote the component of the idempotent $\mathbf{e}$ corresponding to the summand $\mathbf{T}^{(0)}(N)$ in the spit exact sequence (4) above.

Definition Let $f \in S_2(\Gamma_0(N))$ be a p-ordinary eigenform with associated ordinary form f_0. Let $m \geq 0$ be an integer. *Hida's bounded linear form* l_{f_0} of level Np^m is then given by the map

$$l_{f_0} : M_2(\Gamma_*(Np^m), \xi; L) \longrightarrow L, \quad g \longmapsto a_1\left(g|_{\mathbf{e}\circ\mathbf{1}_{f_0}}\right),$$

in other words by the map that sends a modular form $g \in M_2(\Gamma_*(Np^m), \xi; L)$ to the the first Fourier coefficient of its image under the operation $\mathbf{e} \circ \mathbf{1}_{f_0}$.

Proposition 2.2 (Hida) *The linear form $l_{f_0} : M_2(\Gamma_*(Np^n), \xi; L) \longrightarrow L$ is given explicitly on any $g \in M_2(\Gamma_*(Np^m), \xi; L)$ by the map*

$$g \longmapsto \alpha_p(f_0)^{-m} \cdot p \cdot \frac{\langle h_m, g\rangle_{Np^m}}{\langle h, f_0\rangle_{N_0}}.$$

Here, $h = \overline{f}_0(z)|_2 \begin{pmatrix} 0 & -1 \\ N_0 & 0 \end{pmatrix}$ with $\overline{f}_0(z) = \overline{f_0(-\overline{z})}$, and $h_m(z) = h(p^m z)$.

Proof See [14, Proposition 4.5]. □

Lemma 2.3 *The linear form l_{f_0} sends $M_2(\Gamma_*(Np^m), \xi; \mathcal{O})$ to $\mathcal{O}$.*

Proof Fix $g \in M_2(\Gamma_*(Np^m), \xi; \mathcal{O})$. We know that $|\alpha_p(f)|_p = |a_p(f_0)|_p = 1$. On the other hand, the operator $\phi(f_0)$ in the split exact sequence (4) sends $T_p(Np^m) \longmapsto a_p(f_0)$ for each $m \geq 0$. It follows that $\phi(f_0)$ sends the idempotent $\mathbf{e} = \varprojlim_m e_m$ to the unit defined by $\lim_r a_p(f_0)^{p^r} = \lim_r \alpha_p(f_0)^{p^r}$. Now, the action of $\mathbf{T}(N)$ maps the space $M_2(\Gamma_*(Np^m); \mathcal{O})$ to itself for any $m \geq 0$, as explained for instance in [14, §4]. Thus if $|g|_p \leq 1$, then $g|_{\mathbf{e}\circ\mathbf{1}_{f_0}} = (g|_{\mathbf{e}})\,|_{\mathbf{1}_{f_0}}$ has the property that $\left|a_1\left(g|_{\mathbf{e}\circ\mathbf{1}_{f_0}}\right)\right|_p \leq 1$. The result follows. □

Some p-adic convolution measures. We now give a sketch of Perrin-Riou's construction of the measure $d\mu_f$, [32], starting with the setup described above. This construction is made up of several constituent measures that a priori take values in the spaces $M_l(\Gamma_*(M), \xi; L)$, but can be seen to take values in the integral subspaces $M_l(\Gamma_*(M), \xi; \mathcal{O})$, as we show in Proposition 2.8.

Let us fix throughout a finite order character $\mathcal{W}$ of G. We commit an abuse of notation in viewing $\mathcal{W}$ as a character on the ideals of k via class field theory. Observe that we can always write such a character $\mathcal{W}$ as the product of characters $\rho\chi \circ \mathbf{N}$, where ρ is a character of G that factors though the dihedral $\mathbf{Z}_p$-extension D_∞ of k, and $\chi \circ \mathbf{N}$ a character of G that factors though the cyclotomic $\mathbf{Z}_p$-extension k^{cyc} of k. Here, the cyclotomic character $\chi \circ \mathbf{N}$ is given by the composition with the norm homomorphism $\mathbf{N}$ on ideals of k with some Dirichlet character χ that factors through the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Hence, we fix a finite order character $\mathcal{W}$ of G with dihedral/cyclotomic factorization

$$\mathcal{W} = \rho\chi \circ \mathbf{N}. \tag{5}$$

Let $c(\mathcal{W})$ denote the conductor of $\mathcal{W}$, with $c(\rho)$ the conductor of the dihedral or anticyclotomic part ρ. Let $D = D_{k/\mathbf{Q}}$ denote the discriminant of k. Let $\omega = \omega_{k/\mathbf{Q}}$ denote the quadratic character associated to k. A classical construction associates to the $\mathcal{W}$ a theta series of weight 1, level $\Delta = \Delta(\mathcal{W}) = |D|\mathbf{N}c(\mathcal{W})^2$, and Nebentypus $\omega\chi^2$. To be more precise, let $\mathcal{O}_{c(\rho)} = \mathbf{Z} + c(\rho)\mathcal{O}_k$ denote the $\mathbf{Z}$-order of conductor $c(\rho)$ in $\mathcal{O}_k$. Fix an element of the class group $A \in \mathrm{Pic}\mathcal{O}_{c(\rho)}$. Fix a representative $\mathfrak{a} \in A$. We then define a χ-twisted theta series associated to A,

$$\Theta_A(\chi)(z) = \frac{1}{u}\sum_{x\in\mathfrak{a}} \chi\left(\frac{N_{k/\mathbf{Q}}(x)}{\mathbf{N}\mathfrak{a}}\right) e^{\frac{2\pi i N_{k/\mathbf{Q}}(x) z}{\mathbf{N}\mathfrak{a}}} = \frac{1}{u} + \sum_{n\geq 1} \chi(n) r_A(n) e^{2\pi i n z}.$$

Here, x runs over points in the lattice defined by $\mathfrak{a}$, $u = 2|\mathcal{O}_k^\times|$ is twice the number of units of k , and $r_A(n)$ is the number of ideals of norm n in A. This series does not depend on choice of representative $\mathfrak{a} \in A$. It is seen to lie in $M_1(\Gamma_0(\Delta), \omega\chi^2)$ by a standard application of Poisson summation. Taking the ρ-twisted sum over classes $A \in \mathrm{Pic}\mathcal{O}_{c(\rho)}$, it gives rise to a modular form

$$\Theta(\mathcal{W})(z) = \sum_A \rho(A)\Theta_A(\chi)(z) \in M_1(\Gamma_0(\Delta), \omega\chi^2)$$

associated to $\mathcal{W}$. We refer the reader to [11], [14] or [15] for proofs of these facts. In what follows, we fix a finite order character $\mathcal{W}$ of G having the decomposition (5) above. We fix a ring class $A \in \mathrm{Pic}\mathcal{O}_{c(\rho)}$. We then construct a measure associated to the underlying Dirichlet character χ in the decomposition (5). In fact, to follow [32], we shall suppose more generally that χ is any finite order character of $\mathbf{Z}_p^{\times}$. Taking the ρ-twisted sum over classes $A \in \mathrm{Pic}\mathcal{O}_{c(\rho)}$ then gives the appropriate measure in $\mathcal{O}[[G]]$ whose specialization to $\mathcal{W}$ interpolates the value

$$\frac{L(f \times \Theta(\overline{\mathcal{W}}), 1)}{8\pi^2 \langle f, f \rangle_N} \in \overline{\mathbf{Q}}_p$$

up to some algebraic factor (which can be made explicit). We give only a sketch of this construction, referring the reader to [32] for proofs and calculations. We start with the following constituent constructions.

Theta series measures. Fix an integer $m \geq 1$. Consider the series defined by

$$\Theta_A(\chi)(a, p^m)(z) = \sum_{\substack{x \in \mathfrak{a} \\ \frac{N_{k/\mathbf{Q}}(x)}{\mathbf{N}(\mathfrak{a})} \equiv a \bmod p^m}} \chi\left(\frac{N_{k/\mathbf{Q}}(x)}{\mathbf{N}\mathfrak{a}}\right) e^{\frac{2\pi i N_{k/\mathbf{Q}}(x) z}{\mathbf{N}\mathfrak{a}}}.$$

Let $d\Theta_A(\chi)$ denote the measure on $\mathbf{Z}_p^{\times}$ given by the rule

$$\int_{a+p^m \mathbf{Z}_p^{\times}} d\Theta_A(\chi) = \Theta_A(\chi)(z).$$

Lemma 2.4 *The measure $d\Theta_A(\chi)$ takes values in the space $M_1(\Gamma_0(\Delta), \omega\chi^2; \mathcal{O})$ if $p \geq 5$.*

Proof The result follows plainly from the q-expansion of $\Theta_A(\chi)(z)$.$\square$

Remark We impose the condition $p \geq 5$ to deal with the $\frac{1}{u}$ term in the q-expansion of $\Theta_A(\chi)(z)$, since we could in exceptional cases have $u = 4$ or $u = 6$.

Eisenstein series measures. Let ξ be an odd Dirichlet character modulo an integer $M > 2$. Let $E_M(\xi)$ denote the Eisenstein series of weight 1 given by

$$E_M(\xi)(z) = \frac{L(\xi, 0)}{2} + \sum_{n \geq 1} \left(\sum_{\substack{d > 0 \\ d | n}} \xi(d) \right) e^{2\pi i n z}.$$

Here,

$$L(\xi, s) = \sum_{n \geq 1} \xi(n) n^{-s}$$

is the standard Dirichlet L-series associated to ξ. The series $E_M(\xi)(z)$ lies in $M_1(\Gamma_0(M), \xi)$, as shown for instance in [16]. Fix an integer $m \geq 1$. Let $M = Np^m$. Consider the series defined by

$$E(\xi)(a, M)(z) = \frac{L(\xi, 0)}{2} + \sum_{n \geq 1} \left(\sum_{\substack{d > 0, d | n \\ d \equiv a \bmod M}} \xi(d) \right) e^{2\pi i n z}.$$

Fix an integer $C > 1$ prime to M. Let C^{-1} denote the inverse class of C modulo M. Consider the difference defined by

$$E^C(\xi)(a, M)(z) = E(\xi)(a, M)(z) - CE(\xi)(C^{-1}a, M)(z).$$

It is well known that $E^C(\xi)(a, M)(z)$ is a bounded distribution on the product $\mathbf{Z}_p^\times \times (\mathbf{Z}/N)^\times$ (see [14], [24] or [25]). Let $dE^C(\xi)(a, M)$ denote the measure on $\mathbf{Z}_p^\times \times (\mathbf{Z}/N)^\times$ given by the rule

$$\int_{a + Np^m \mathbf{Z}_p^\times} dE^C(\xi)(a, M) = E^C(\xi)(a, Np^m)(z).$$

Note that this measure takes values in certain spaces of Eisenstein series. To be more precise, we have the following result.

Lemma 2.5 *The measure $dE^C(\xi)(a, M)$ takes values in the space $M_1(\Gamma_0(M), \xi; \mathcal{O})$.*

Proof The result follows from the Key Lemma of Katz [24, 1.2.1, Key Lemma for $\Gamma(N)$], which shows that the Eisenstein measure takes p-integral values at an elliptic curve with level structure defined over a p-integral ring. Note also that $dE^C(\xi)(a, M)$ arises from a one-dimensional part of the Eisenstein pseudo-distribution $2H^{(a,b)}$ given in [24, §3.4] (i.e. with $a = C$). This pseudo-distribution can be shown to take integral values by [24, Key Lemma 1.2.1], e.g. by the proof given in [24, Theorem 3.3.3] (cf. also [24, §3.5, (3.5.5)]). □

Convolution measures. Fix a class $A \in \mathrm{Pic}\mathcal{O}_{c(\rho)}$. Fix integers $a, m \geq 1$. Fix an integer $C > 1$ prime to pND. Consider the series defined by

$$\Phi_A^C(\chi)(a, p^m)(z) = \sum_{\alpha \in (\mathbf{Z}/N\Delta)^\times} \Theta_A(\chi)(\alpha^2 a, p^m)(Nz) E^C(\omega\chi^2)(\alpha, N\Delta)(z).$$

The function $\Phi_A^C(a, p^m)(z)$ can be seen to define a bounded distribution on $\mathbf{Z}_p^\times$ (see [32, Lemme 4]). Let $d\Phi_A^C(\chi)$ denote the measure on $\mathbf{Z}_p^\times$ given by this function.

Lemma 2.6 *The measure $d\Phi_A^C(\chi) = \Phi_A^C(a, p^m)(z)$ takes values in the space $M_2(\Gamma_0(N\Delta), \omega\chi^2; \mathcal{O})$, at least if $p \geq 5$.*

Proof The function $\Phi_A(a, p^m)(z)$ lies in $M_2(\Gamma_0(N\Delta), \omega\chi^2)$ (see [32, Lemme 5]). We then deduce from Lemmas 2.4 and 2.5 that it lies in $M_2(\Gamma_0(N\Delta), \omega\chi^2; \mathcal{O})$. □

Trace operators. Keep the setup used to define the convolution measure $d\Phi_A^C(\chi)$ above. Fix a set representatives $\mathcal{R}$ for the space $\Gamma_0(N\Delta)\backslash\Gamma_0(N)$. We define the trace operator $\mathrm{Tr}_N^{N\Delta} : M_2(\Gamma_0(N\Delta), \xi) \longrightarrow M_2(\Gamma_0(N), \xi)$ by the rule

$$h(z) \longmapsto \sum_{\gamma \in \mathcal{R}} \xi(a_\gamma) \cdot h|_2\gamma, \quad \gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix}.$$

Lemma 2.7 *The composition function* $\mathrm{Tr}_N^{N\Delta} \circ \Phi_A^C(\chi)(a, p^m)(z)$ *takes values in the space* $M_2(\Gamma_0(N), \omega\chi^2; \mathcal{O})$*, at least if* $p \geq 5$*.*

Proof Given the result of Lemma 2.7, the assertion can be deduced from explicit computations of the Fourier series expansion of the trace form. If N and D are both prime, then the result follows from the computation given in Gross [10, Proposition 9.3, 2)]. In the more general case with $(N, D) = 1$, it follows from the computation of the coefficients given in Gross-Zagier [11, IV§2 Proposition (2.4) and §3, Proposition (3.2)]. □

Mesures fondamentales. Keep the setup from above. Recall that we let f_0 denote the p-stabilization of f, which is the unique ordinary form associated to f by Hida [14, Lemma 3.3]. Let $l_{f_0} : M_2(\Gamma_0(N), \omega\chi^2; L) \longrightarrow L$ denote Hida's bounded linear form, as defined above. Let L denote the closure of the field of values $L_0 = \mathbf{Q}(\omega\chi^2(n))_{n\geq 0}$ in $\overline{\mathbf{Q}}_p$. Let $d\phi_A^C(\chi)$ denote the measure on $\mathbf{Z}_p^\times$ given by the rule

$$\int_{a+p^m\mathbf{Z}_p^\times} d\phi_A^C(\chi) = l_{f_0} \circ \mathrm{Tr}_N^{N\Delta} \circ \Phi_A^C(\chi)(a, p^m)(z).$$

Proposition 2.8 *The measure* $d\phi_A^C(\chi)$ *takes values in the ring* $\mathcal{O} = \mathcal{O}_L$*, at least if* $p \geq 5$*.*

Proof The result follows from Lemmas 2.4, 2.5, 2.6, 2.7 and 2.3. □

We can now at last define the two-variable measures that gives rise to $d\mu_f$.

Definition Keep the notations above, with $C > 1$ an integer prime to pND. Let $L(\rho)$ denote the closure of the field of values $L_0(\rho(A))_{A\in \mathrm{Pic}\mathcal{O}_{c(\rho)}}$ in $\overline{\mathbf{Q}}_p$. Let $\mathcal{O} = \mathcal{O}_{L(\rho)}$. Let $d\mu_f^C$ denote the $\mathcal{O}$-valued function on G defined by the rule

$$\int_G \mathcal{W}\mu_f^C = \sum_{A\in \mathrm{Pic}\mathcal{O}_{c(\rho)}} \rho(A) d\phi_A^C(\chi).$$

This function is seen easily to be a well-defined distribution on G (see [32, § 5]), and hence (by Proposition 2.8) a measure on G. That is, the distribution is seen easily to be bounded for any choice of p, and integral for any choice $p \geq 5$. It is also seen to be integral for any choice of p if $\rho \neq \mathbf{1}$ (in which case the twisted sum of theta series $\sum_A \rho(A)\Theta_A(\chi)(z)$ is cuspidal).

Interpolation properties and functional equation. Let us keep all of the notations above, with $C > 1$ an integer prime to pND. The two-variable measure $d\mu_f^C$ satisfies the following interpolation property. Let $\tau(\mathcal{W})$ denote the Artin root number of $L(\mathcal{W}, s)$. Recall that $\Delta = \Delta(\mathcal{W})$ denotes the level of the theta series $\Theta(\mathcal{W})(z)$. Let ψ denote the principal character modulo N as above (hence, $\psi(p) = 1$ if p does not divide N and zero otherwise). Recall as well that we let α_p denote the unique p-adic unit root of the polynomial $X^2 - a_p(f)X - p\psi(p)$. Given an integer $r \geq 1$, let us write α_{p^r} to denote α_p^r. Let us also write N' to denote the prime-to-p part of N. Let β denote the p-primary component of the level Δ of $\Theta(\mathcal{W})$. Finally, let us commit an abuse of notation in using the same notations used to denote the measures defined on $\mathbf{Z}_p^\times$ above to denote the induced measures defined on $\mathbf{Z}_p$.

Theorem 2.9 *There exists for each integer $C > 1$ prime to pND an $\mathcal{O}$-valued measure $d\mu_f^C$ on G such that for any finite order character $\mathcal{W}$ of G,*

$$\begin{aligned}\int_G \mathcal{W} d\mu_f^C = &\left(1 - \frac{\psi(p)}{\alpha_{p^2}}\right)^{-1} \left(1 + \frac{p\psi(p)}{\alpha_{p^2}}\right)^{-1} \prod_{\mathfrak{p}|p} \left(1 - \frac{\mathcal{W}(\mathfrak{p})}{\alpha_{\mathbf{N}\mathfrak{p}}}\right)\left(1 - \frac{\overline{\mathcal{W}}\psi(\mathbf{N}\mathfrak{p})(\mathfrak{p})}{\alpha_{\mathbf{N}\mathfrak{p}}}\right) \\ &\times \omega(-N')\mathcal{W}(N')\left(1 - C\omega(C)\overline{\mathcal{W}}(C)\right)\frac{\Delta^{\frac{1}{2}}}{\alpha_{p^\beta}}\tau(\mathcal{W}) \\ &\times \frac{L(f \times \Theta(\overline{\mathcal{W}}), 1)}{8\pi^2\langle f, f\rangle_N}.\end{aligned}$$

Here, the product runs over all primes $\mathfrak{p}$ of $\mathcal{O}_k$ that divide p.

Proof See Perrin-Riou [32, Théorème A], along with Proposition 2.8 above. That is, fix a finite order character $\mathcal{W}$ of G having the decomposition (5). Fix an integer $C > 1$ prime to pND. A simple argument shows that $d\mu_f^C$ is a well-defined distribution on G (see [32, § 5]). On the other hand, we know that $d\mu_f^C$ takes values in $\mathcal{O} = \mathcal{O}_{L(\rho)}$ (by Proposition 2.8). Hence, $d\mu_f^C$ is an $\mathcal{O}$-valued measure on G, corresponding to an element of the completed group ring $\mathcal{O}[[G]]$. The calculation of the interpolation value is given in [32, § 4]. □

We may now define the two-variable p-adic L-function associated to a p-ordinary eigenform $f \in S_2(\Gamma_0(N))$ in the tower k_∞/k, following Perrin-Riou [32]. Observe that this definition does not depend on the choice of auxiliary integer $C > 1$ prime to pND thanks to Theorem 2.9.

Definition Let $\eta : G \to \mathbf{Z}_p^\times$ be a continuous character. Let $\mathfrak{D}$ denote the different of k. Let $C > 1$ be any integer prime to pND. The *two-variable p-adic L-function* $L_p(f, k)(\eta)$ of f in k_∞/k is then defined to be

$$\begin{aligned}L_p(f, k)(\eta) = &\left(1 - \frac{\psi(p)}{\alpha_{p^2}}\right)\left(1 + \frac{p\psi(p)}{\alpha_{p^2}}\right) \\ &\times \eta^{-1}(\mathfrak{D}'N')\left(1 - C\omega(C)\eta^{-1}(C)\right)^{-1} \\ &\times \int_G \eta(g) d\mu_f^C(g).\end{aligned}$$

Here, $\mathfrak{D}'$ and N' denote the prime to p parts of $\mathfrak{D}$ and N respectively.

Corollary 2.10 *The function $L_p(f,k)$ is an Iwasawa function on G with coefficients in $\mathbf{Z}_p$. Moreover, the Iwasawa function defined by*

$$\Lambda_p(f,k)(\eta) = \eta^{\frac{1}{2}}(N')\eta(\mathfrak{D}')L_p(f,k)(\eta)$$

satisfies the functional equation

$$\Lambda_p(f,k)(\eta^{-1}) = -\omega(N')\Lambda_p(f,k)(\eta).$$

Proof See [32, Corollaire, Théorème A] or [32, Corollaire, Théorème B]. □

3 Iwasawa module structure theory

We now describe the Iwasawa module structure theory of the dual Selmer group of E over k_∞, along with that of the p-primary component of the associated Tate-Shafarevich group. We follow closely many of the arguments of Coates-Sujatha-Schneider [7], as well as the refinements of those given by Hachimori-Venjakob [13] for the somewhat analogous setting of the false Tate curve extension.

Some definitions. Fix S a finite set of primes of k containing both the primes above p and the primes where E has bad reduction. Let k^S denote the maximal Galois extension of k that is unramified outside of S and the archimedean primes of k. Note that since k_∞ is unramified outside of primes above p, we have the inclusion $k_\infty \subset k^S$. Given L any finite extension of k contained in k_∞, let $G_S(L)$ denote the Galois group $\mathrm{Gal}(k^S/L)$. The p^∞-Selmer group $\mathrm{Sel}(E/L)$ of E over L is defined classically as the kernel of the localization map,

$$\mathrm{Sel}(E/L) = \ker\left(\lambda_E(L) : H^1(G_S(L), E_{p^\infty}) \longrightarrow \bigoplus_{v\in S} J_v(L)\right).$$

Here, $E_{p^\infty} = E(k^S)_{p^\infty}$ denotes the p-power torsion: $E_{p^\infty} = \bigcup_{n\geq 0} E_{p^n}$ where $E_{p^n} = \ker([p^n] : E \to E)$. We also write

$$J_v(L) = \bigoplus_{w|v} H^1(L_w, E(\overline{L}_w))(p),$$

where the sum runs over all primes w above v in L. Note that this group fits into the classical short exact descent sequence

$$0 \longrightarrow E(L)\otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathrm{Sel}(E/L) \longrightarrow \text{Ш}(E/L)(p) \longrightarrow 0,$$

where $\text{Ш}(E/L)(p)$ denotes the p-primary component of the Tata-Shafarevich group $\text{Ш}(E/L)$ of E over L. Let L_∞ be any infinite extension of k contained in k_∞. We then define the Selmer group of E over L_∞ to be the inductive limit

$$\mathrm{Sel}(E/L_\infty) = \varinjlim_{L} \mathrm{Sel}(E/L).$$

Here, the limit is taken over all finite extensions L of k contained in L_∞ with respect to the natural restriction maps on cohomology. We write

$$X(E/L_\infty) = \mathrm{Hom}(\mathrm{Sel}(E/L_\infty), \mathbf{Q}_p/\mathbf{Z}_p)$$

to denote the Pontryagin dual of $\mathrm{Sel}(E/L_\infty)$.

$\Lambda(\Gamma)$-module structure. Let us first review the cyclotomic structure theory implied by work of Kato and Rohrlich.

Theorem 3.1 (Kato-Rohrlich) *If $E/\mathbf{Q}$ has good ordinary reduction at each prime above p in k, then the dual Selmer group $X(E/k^{cyc})$ is $\Lambda(\Gamma)$-torsion.*

Proof The result follows from the Euler system method of Kato [23, Theorems 14.2 and 17.4], which requires for nontriviality the nonvanishing theorem of Rohrlich [34]. □

We may then invoke the structure theory of finitely generated torsion $\Lambda(\Gamma)$-modules ([2, Chapter VII, §4.5]) to obtain a $\Lambda(\Gamma)$-module pseudoisomorphism

$$X(E/k^{\mathrm{cyc}}) \longrightarrow \bigoplus_{i=1}^{r} \Lambda(\Gamma)/p^{m_i} \oplus \bigoplus_{j=1}^{s} \Lambda(\Gamma)/\gamma_j^{n_j}. \tag{6}$$

Here, the indices r, s, m_i and n_j are all positive integers, and each γ_j can be viewed as an irreducible monic distinguished polynomial $\gamma_j(T)$ (with respect to a fixed isomorphism $\Lambda(\Gamma) \cong \mathbf{Z}_p[[T]]$). The $\Lambda(\Gamma)$-characteristic power series

$$\mathrm{char}_{\Lambda(\Gamma)} X(E/k^{\mathrm{cyc}}) = \prod_{i=1}^{r} p^{m_i} \cdot \prod_{j=1}^{s} \gamma_j^{n_j}$$

is defined uniquely up to unit in $\Lambda(\Gamma)$. One defines from it the $\Lambda(\Gamma)$-module invariants

$$\mu_{\Lambda(\Gamma)}\left(X(E/k^{\mathrm{cyc}})\right) = \sum_{i=1}^{r} m_i \quad \text{and} \quad \lambda_{\Lambda(\Gamma)}\left(X(E/k^{\mathrm{cyc}})\right) = \sum_{j=1} n_j \cdot \deg(\gamma_j).$$

We shall often for simplicity denote these by

$$\mu_E(k) = \mu_{\Lambda(\Gamma)}\left(X(E/k^{\mathrm{cyc}})\right) \quad \text{and} \quad \lambda_E(k) = \lambda_{\Lambda(\Gamma)}\left(X(E/k^{\mathrm{cyc}})\right).$$

respectively. We refer the reader to the monograph of Coates-Sujatha [8] for further discussion, for instance on how to compute the (finite) G-Euler characteristic of $\mathrm{Sel}(E/k^{\mathrm{cyc}})$, or equivalently how to compute $|\mathrm{char}_{\Lambda(\Gamma)} X(E/k^{\mathrm{cyc}})(0)|_p^{-1}$, where $\mathrm{char}_{\Lambda(\Gamma)} X(E/k^{\mathrm{cyc}})(0)$ denotes the image of the characteristic power series $\mathrm{char}_{\Lambda(\Gamma)} X(E/k^{\mathrm{cyc}})$ under the natural augmentation map $\Lambda(\Gamma) \longrightarrow \mathbf{Z}_p$.

$\Lambda(G)$-module structure. We now use the $\Lambda(\Gamma)$-module structure of $X(E/k^{\mathrm{cyc}})$ to study the $\Lambda(G)$-module structure of $X(E/k_\infty)$, following the main ideas of [7] and [13]. Let us first consider the following standard result. Let $\mathfrak{S}(E/L)$ denote the compactified Selmer group of E over any finite extension L of k contained in k_∞, which is defined as the projective limit

$$\mathfrak{S}(E/L) = \varprojlim_n \ker\left(H^1(G_S(L), E_{p^n}) \longrightarrow \bigoplus J_v(L)\right)$$

taken with respect to the natural maps $E_{p^{n+1}} \to E_{p^n}$ induced by multiplication by p. Given any infinite extension L_∞ of k contained in k_∞, we then define

$$\mathfrak{S}(E/L_\infty) = \varprojlim_L \mathfrak{S}(E/L)$$

to be the projective limit over all finite extensions L of k contained in L_∞, taken with respect to the natural corestriction maps.

Proposition 3.2 *Let $\Omega = Gal(L_\infty/k)$ be any infinite pro-p group. If $E(L_\infty)_{p^\infty}$ is finite, then there is a $\Lambda(\Omega)$-module injection*

$$\mathfrak{S}(E/L_\infty) \longrightarrow Hom_{\Lambda(\Omega)}(X(E/L_\infty), \Lambda(\Omega)).$$

Proof See for instance [13, Theorem 7.1]. □

We use this to deduce the following result.

Theorem 3.3 *If E has good ordinary reduction at each prime above p in k, then the cohomology group $H^2(G_S(k^{cyc}), E_{p^\infty})$ vanishes. In particular, the localization map*

$$\lambda_S(k^{cyc}) : H^1(G_S(k^{cyc}), E_{p^\infty}) \longrightarrow \bigoplus_{v\in S} J_v(k^{cyc})$$

is surjective, and hence we have a short exact sequence of $\Lambda(\Gamma)$-modules

$$0 \longrightarrow \mathrm{Sel}(E/k^{cyc}) \longrightarrow H^1(G_S(k^{cyc}), E_{p^\infty}) \longrightarrow \bigoplus_{v\in S} J_v(k^{cyc}) \longrightarrow 0. \qquad (7)$$

Proof Consider the Cassels-Poitou-Tate exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{Sel}(E/k^{\mathrm{cyc}}) \longrightarrow H^1(G_S(k^{\mathrm{cyc}}), E_{p^\infty}) &\longrightarrow \bigoplus_{v\in S} J_v(k^{\mathrm{cyc}}) \\ &\longrightarrow \mathfrak{S}(E/k^{\mathrm{cyc}})^\vee \longrightarrow H^2(G_S(k^{\mathrm{cyc}}), E_{p^\infty}) \longrightarrow 0. \end{aligned}$$

Here, $\mathfrak{S}(E/k^{\mathrm{cyc}})^\vee$ is the Pontryagin dual of $\mathfrak{S}(E/k^{\mathrm{cyc}})$. Now, the p-power torsion subgroup $E(k^{\mathrm{cyc}})_{p^\infty}$ is finite by Imai's theorem [21]. Hence, we can invoke Proposition 3.2 to obtain an injection $\mathfrak{S}(E/k^{\mathrm{cyc}}) \to \mathrm{Hom}_{\Lambda(\Gamma)}(X(E/k^{\mathrm{cyc}}), \Lambda(\Gamma))$.

Now, by the main result of Kato [23], the dual Selmer group $X(E/k^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. Hence, we have a $\Lambda(\Gamma)$-module injection

$$\mathfrak{S}(E/k^{\mathrm{cyc}}) \hookrightarrow \mathrm{Hom}_{\Lambda(\Gamma)}(X(E/k^{\mathrm{cyc}}), \Lambda(\Gamma)) = 0.$$

It follows that $\mathfrak{S}(E/k^{\mathrm{cyc}})^{\vee} = 0$, and hence that $H^2(G_S(k^{\mathrm{cyc}}), E_{p^\infty}) = 0$. See also the argument of Kato [23, §§13, 14] for this latter vanishing. □

Let us now consider invariants under the Galois group $H = \mathrm{Gal}(k_\infty/k^{\mathrm{cyc}})$. Note that by Serre's refinement [38] of Lazard's theorem [26], a p-adic Lie group with no element of order p has p-cohomological dimension cd_p equal to its dimension as a p-adic Lie group. Since G has no element of order p, we can and will invoke this characterization throughout. Hence (for instance), $\mathrm{cd}_p(G) = 2$ with $\mathrm{cd}_p(H) = \mathrm{cd}_p(\Gamma) = 1$. To show the main result of this paragraph, we first establish the following standard lemmas.

Lemma 3.4 *If E has good ordinary reduction at each prime above p in k, then there is a short exact sequence*

$$\begin{aligned} 0 \longrightarrow \mathrm{Sel}(E/k_\infty)^H &\longrightarrow H^1(G_S(k_\infty), E_{p^\infty})^H \\ &\xrightarrow{\eta_S(k_\infty)} \bigoplus_{v\in S} J_v(k_\infty)^H \longrightarrow 0. \end{aligned}$$

Here, $\eta_S(k_\infty)$ is the map induced by localization map

$$\lambda_S(k_\infty) : H^1(G_S(k_\infty), E_{p^\infty}) \longrightarrow \bigoplus_S J_v(k_\infty).$$

Proof See [7, Lemma 2.3]. That is, consider the fundamental diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}(E/k_\infty)^H & \longrightarrow & H^1(G_S(k_\infty), E_{p^\infty})^H & \xrightarrow{\eta_S(k_\infty)} & \bigoplus_{v\in S} J_v(k_\infty)^H \\ & & \uparrow & & \uparrow & & \uparrow{\scriptstyle \gamma_S(k^{\mathrm{cyc}})} \\ 0 & \longrightarrow & \mathrm{Sel}(E/k^{\mathrm{cyc}}) & \longrightarrow & H^1(G_S(k^{\mathrm{cyc}}), E_{p^\infty}) & \xrightarrow{\lambda_S(k^{\mathrm{cyc}})} & \bigoplus_{v\in S} J_v(k^{\mathrm{cyc}}). \end{array}$$

Here, the horizontal rows are exact, and the vertical arrows are induced by restriction on cohomology. We have that

$$\mathrm{coker}(\gamma_S(k^{\mathrm{cyc}})) = \bigoplus_{w|v\in S} \mathrm{coker}(\gamma_w(k^{\mathrm{cyc}})),$$

with w ranging over places in k^{cyc} above $v \in S$. Note that only finitely many such primes exist, as no finite prime splits completely in k^{cyc} (see for instance [46, Theorem 2.13]). Given a prime w above v in k_∞, let Ω_w denote the decomposition subgroup of H at w. Note that $\mathrm{cd}_p(\Omega_w) \leq 1$, and so $H^2(\Omega_w, E_{p^\infty}) = 0$. If $w \nmid p$, then standard arguments (see for instance [4, Lemma 3.7]) show that

$$\mathrm{coker}(\gamma_w(k^{\mathrm{cyc}})) = H^2(\Omega_w, E_{p^\infty}) = 0.$$

If $w|p$, then the main result of Coates-Greenberg [5] shows that

$$\mathrm{coker}(\gamma_w(k^{\mathrm{cyc}})) = H^2(\Omega_w, \widetilde{E}_{w,p^\infty}) = 0.$$

Here, $\widetilde{E}_{w,p^\infty}$ denotes the image under reduction modulo w of E_{p^∞}. Hence, we find that $\mathrm{coker}(\gamma_w(k^{\mathrm{cyc}})) = 0$ for each prime w above v in k_∞. It follows that $\gamma_S(k^{\mathrm{cyc}})$ is surjective. Since the map $\lambda_S(k^{\mathrm{cyc}})$ is also surjective by (7), it follows that $\eta_S(k_\infty)$ is surjective as required. □

Lemma 3.5 *If E has good ordinary reduction at each prime above p in k, then for all $i \geq 1$, $H^i(H, H^1(G_S(k_\infty), E_{p^\infty})) = 0$.*

Proof See [7, Lemma 2.4]. The same proof works here, using Theorem 3.3 with the fact that $\mathrm{cd}_p(H) = 1$. □

Lemma 3.6 *If E has good ordinary reduction at each prime above p in k, then $H^1(H, \mathrm{Sel}(E/k_\infty)) = 0$.*

Proof See [7, Lemma 2.5]. Let $A_\infty = \mathrm{Im}(\lambda_S(k_\infty))$. Lemma 3.5 with $i = 1$ gives the exact sequence

$$0 \longrightarrow \mathrm{Sel}(E/k_\infty)^H \longrightarrow H^1(G_S(k_\infty), E_{p^\infty})^H \longrightarrow A_\infty^H \longrightarrow H^1(H, \mathrm{Sel}(E/k_\infty)) \longrightarrow 0. \tag{8}$$

Recall that the map $\eta_S(k_\infty) : H^1(G_S(k_\infty), E_{p^\infty})^H \longrightarrow A_\infty^H$ is surjective by Lemma 3.4. Now,

$$A_\infty^H = \bigoplus_{v \in S} J_v(k_\infty)^H,$$

and so it follows that $H^1(H, S(E/k_\infty)) = 0$. □

Lemma 3.7 *If E has good ordinary reduction at each prime above p in k, then $H^1(H, \bigoplus_{v\in S} J_v(k_\infty)) = 0$.*

Proof See [7, Lemma 2.8]. The same proof works here, using the fact that $\mathrm{cd}_p(H) = 1$. □

We may now deduce the following result.

Theorem 3.8 *If E has good ordinary reduction at each prime above p in k, then $X(E/k_\infty)$ is $\Lambda(G)$-torsion.*

Proof See the arguments of [13, Theorem 2.8, and Corollary 2.9], following [7, Proposition 2.9]. A standard deduction, as given for instance in [13, §2, Remark 2.5], reduces the claim to showing the surjectivity of the localization map

$$\lambda_S(k_\infty) : H^1(G_S(k_\infty), E_{p^\infty}) \longrightarrow \bigoplus J_v(k_\infty).$$

So, let $A_\infty = \mathrm{im}(\lambda_S(k_\infty))$. Taking the H-cohomology of the exact sequence

$$0 \longrightarrow \mathrm{Sel}(E/k_\infty) \longrightarrow H^1(G_S(k_\infty), E_{p^\infty}) \longrightarrow A_\infty \longrightarrow 0,$$

we obtain from Lemma 3.5 the identification

$$H^1(H, A_\infty) = H^2(H, \mathrm{Sel}(E/k_\infty)).$$

Note that since $\mathrm{cd}_p(H) = 1$, we have that $H^2(H, \mathrm{Sel}(E/k_\infty)) = 0$, and hence that $H^1(H, A_\infty) = 0$. Let $B_\infty = \mathrm{coker}(\lambda_S(k_\infty))$. By Lemma (3.7),

$$H^1(H, \bigoplus_{v \in S} J_v(k_\infty)) = 0.$$

Taking H-cohomology of the exact sequence

$$0 \longrightarrow A_\infty \longrightarrow \bigoplus_{v \in S} J_v(k_\infty) \longrightarrow B_\infty \longrightarrow 0,$$

we deduce from Lemma 3.4 that

$$B_\infty^H = H^1(H, A_\infty) = 0.$$

Since H is pro-p, and B_∞ a discrete p-primary H-module, it follows that B_∞ itself must vanish. Hence $\lambda_S(k_\infty)$ is surjective. $\square$

When $X(E/k_\infty)$ is $\Lambda(G)$-torsion, the structure theory of torsion $\Lambda(G)$-modules ([2, Chapter VII, §4.5]) gives a pseudoisomorphism

$$X(E/k_\infty) \longrightarrow \bigoplus_{i=1}^{t} \Lambda(G)/p^{a_i} \oplus \bigoplus_{j=1}^{u} \Lambda(G)/g_j^{b_j}. \tag{9}$$

Here, the indices s, t, a_i and b_j are all positive integers, and each g_j can be viewed as an irreducible monic distinguished polynomial $g_j(T_1, T_2)$ (with respect to a fixed isomorphism $\Lambda(G) \cong \mathbf{Z}_p[[T_1, T_2]]$). The characteristic power series

$$\mathrm{char}_{\Lambda(G)} X(E/k_\infty) = \prod_{i=1}^{t} p^{a_i} \cdot \prod_{j=1}^{u} g_j^{b_j}$$

is again well defined up to unit in $\Lambda(G)$. As in the cyclotomic setting, one uses it to define the $\Lambda(G)$-module invariants

$$\mu_{\Lambda(G)}(X(E/k_\infty)) = \sum_{i=1}^{t} a_i \quad \text{and} \quad \lambda_{\Lambda(G)}(X(E/k_\infty)) = \sum_{j=1}^{u} b_j \cdot \deg(g_j).$$

The invariant $\mu_{\Lambda(G)}(X(E/k_\infty))$. Let us now review what is known about the invariant $\mu_{\Lambda(G)}(X(E/k_\infty))$. Suppose more generally that G is any pro-p group, and Y any finitely-generated torsion $\Lambda(G)$-module. The structure theory of $\Lambda(G)$

modules shown in [2, Chapter VII, §4.5]) again gives a pseudoisomorphism analogous to (9), and so we may define the associated invariant $\mu_{\Lambda(G)}(Y)$. Let $Y(p)$ denote the submodule of elements of Y annihilated by some power of p. It is well known (see for instance [20]) that the cohomology groups $H^i(G, Y)$ are finitely-generated $\mathbf{Z}_p$-modules for all $i \geq 0$, and hence that the cohomology groups $H^i(G, Y(p))$ are finite for all $i \geq 0$. The invariant $\mu_{\Lambda(G)}(Y)$ is then seen to be given by the formula

$$p^{\mu_{\Lambda(G)}(Y)} = \prod_{i \geq 0} |H_i(G, Y(p))|^{(-1)^i} = \chi(G, Y(p)), \tag{10}$$

where $\chi(G, Y(p))$ is by definition the finite G-Euler characteristic of $Y(p)$. Given L any extension of k contained in k_∞, let us write

$$\mathfrak{X}(E/L) = X(E/L)/X(E/L)(p).$$

Proposition 3.9 *If E has good ordinary reduction at p, and $\mathfrak{X}(E/k_\infty)$ is finitely-generated over $\Lambda(H)$, then $\mu_{\Lambda(G)}(X(E/k_\infty)) = \mu_E(k)$.*

Proof See [7, Propostion 2.9], we give a sketch of the proof. Note that we have $X(E/k_\infty)_H = H_0(H, X(E/k_\infty))$. Note as well that $H_1(H, X(E/k_\infty)) = 0$ by Lemma 3.6. Taking H-homology of the short exact sequence

$$0 \longrightarrow X(E/k_\infty)(p) \longrightarrow X(E/k_\infty) \longrightarrow \mathfrak{X}(E/k_\infty) \longrightarrow 0,$$

we obtain a short exact sequence of $\Lambda(\Gamma)$-modules

$$\begin{aligned} 0 \longrightarrow H_1(H, \mathfrak{X}(E/k_\infty)) &\longrightarrow H_0(H, X(E/k_\infty)(p)) \\ &\longrightarrow H_0(H, X(E/k_\infty)) \longrightarrow H_0(H, \mathfrak{X}(E/k_\infty)) \longrightarrow 0. \end{aligned}$$

Following [20, Proposition 1.9], we then show that the alternating sum of $\mu_{\Lambda(\Gamma)}$-invariants along this sequence vanishes. Moreover, the $\mu_{\Lambda(\Gamma)}$-invariants of the two central terms can be computed as follows. For $H_0(H, X(E/k_\infty)) = X(E/k_\infty)_H$, it is well known (see the proof of Theorem 3.12 below for instance) that restriction on cohomology induces a $\Lambda(\Gamma)$-homomorphism

$$\alpha : X(E/k_\infty)_H \longrightarrow X(E/k^{\mathrm{cyc}})$$

with $\ker(\alpha)$ finitely-generated over $\mathbf{Z}_p$ and $\mathrm{coker}(\alpha)$ finite. We deduce that

$$\mu_{\Lambda(\Gamma)}((X(E/k_\infty)_H) = \mu_{\Lambda(\Gamma)}((X(E/k^{\mathrm{cyc}})) = \mu_E(k).$$

For $H_0(H, X(E/k_\infty)(p))$, consider the Hochschild-Serre spectral sequence

$$\begin{aligned} 0 \longrightarrow H_0(\Gamma, H_i(H, X(E/k_\infty)(p)) &\longrightarrow H_i(G, X(E/k_\infty)(p)) \\ &\longrightarrow H_1(\Gamma, H_{i-1}(H, X(E/k_\infty)(p)) \longrightarrow 0. \end{aligned}$$

We deduce that

$$\chi(G, X(E/k_\infty)(p)) = \prod_{i=0}^{1} \chi(\Gamma, H_i(H, X(E/k_\infty)(p)))^{(-1)^i},$$

and so

$$\mu_{\Lambda(G)}(X(E/k_\infty)) = \sum_{i=0}^{1}(-1)^i \mu_{\Lambda(\Gamma)}(H_i(H, X(E/k_\infty)(p))).$$

Putting terms together from the first (alternating sum) sequence above, we find that $\mu_{\Lambda(G)}(X(E/k_\infty)) =$

$$\mu_E(k)+\sum_{i=0}^{1}(-1)^{i+1}\mu_{\Lambda(\Gamma)}(H_i(H, \mathfrak{X}(E/k_\infty)))+\sum_{i=0}^{1}(-1)^i \mu_{\Lambda(\Gamma)}(H_i(H, X(E/k_\infty)(p))).$$

Recall that $H_i(H, X(E/k_\infty)) = 0$ for all $i \geq 0$ by Lemma 3.6. Taking H-cohomology of the short exact sequence

$$0 \longrightarrow X(E/k_\infty)(p) \longrightarrow X(E/k_\infty) \longrightarrow \mathfrak{X}(E/k_\infty) \longrightarrow 0,$$

obtain that $H_1(H, X(E/k_\infty)(p))) = H_2(H, \mathfrak{X}(E/k_\infty)) = 0$. Deduce that

$$\mu_{\Lambda(G)}(X(E/k_\infty)) = \mu_E(k) + \sum_{i=0}^{1}(-1)^{i+1}\mu_{\Lambda(\Gamma)}(H_i(H, \mathfrak{X}(E/k_\infty))).$$

Since we assume that $\mathfrak{X}(E/k_\infty)$ is finitely-generated over $\Lambda(H)$, it follows that $\mathfrak{X}(E/k_\infty)_H$ is finitely-generated over $\mathbf{Z}_p$. Thus,

$$\mu_{\Lambda(\Gamma)}(H_i(H, \mathfrak{X}(E/k_\infty))) = 0.$$

In particular, $\mu_{\Lambda(G)}(X(E/k_\infty)) = \mu_E(k)$ as claimed. □

The G-Euler characteristic of $\mathrm{Sel}(E/k_\infty)$**.** We now give a formula for the G-Euler characteristic of $\mathrm{Sel}(E/k_\infty)$,

$$\chi(G, \mathrm{Sel}(E/k_\infty)) = \prod_{i\geq 0} |H^i(G, \mathrm{Sel}(E/k_\infty))|^{(-1)^i},$$

which in the setup described above is well defined (i.e. finite). Note that this invariant is related to the characteristic power series $\mathrm{char}_{\Lambda(G)} X(E/k_\infty)$ by the formula

$$\chi(G, \mathrm{Sel}(E/k_\infty)) = |\,\mathrm{char}_{\Lambda(G)} X(E/k_\infty)(0)|_p^{-1},$$

where $\mathrm{char}_{\Lambda(G)} X(E/k_\infty)(0)$ denotes the image of $\mathrm{char}_{\Lambda(G)} X(E/k_\infty)$ under the natural augmentation map $\Lambda(G) \longrightarrow \mathbf{Z}_p$. We must first establish the following result.

Lemma 3.10 *If E has good ordinary reduction at each prime above p in k, then the p-primary torsion subgroup $E(k_\infty)_{p^\infty}$ is finite.*

Proof See the argument of [13][Lemma 3.12]. We present the following alternative proof. Fix a rational prime v that remains inert in k and does not equal p. Write k_v to denote the localization of k at the prime above v. Write k_v^{cyc} to denote the cyclotomic $\mathbf{Z}_p$-extension of k_v. By Imai's theorem [21] (cf. [8][A.2.7]), the p-primary subgroup of $E(k_v^{\mathrm{cyc}})$ is finite. On the other hand, the prime above v in k splits completely in D_∞ by class field theory. Hence, writing $D_{\infty,w}$ to denote the union of all completions of D_∞ at primes above v, we have an isomorphism of local fields $D_{\infty,w} \cong k_v$. This induces an isomorphism of Mordell-Weil groups $E(D_{\infty,w}) \cong E(k_v)$. Hence, writing $k_{\infty,\mathfrak{w}}$ to denote the union of all completions of k_∞ at primes above v, we have the identifications

$$E(k_{\infty,\mathfrak{w}}) \cong E(D_{\infty.w} \cdot k_v^{\mathrm{cyc}}) \cong E(k_v^{\mathrm{cyc}}).$$

Hence, the p-primary part of $E(k_{\infty,\mathfrak{w}})$ is seen to be finite by Imai's theorem. Since $E(k_\infty)_{p^\infty}$ injects into the p-primary part of $E(k_{\infty,\mathfrak{w}})$, the result follows. □

Theorem 3.11 *Assume that E has good ordinary reduction at all primes above p in k, that $p \geq 5$, and that $\mathrm{Sel}(E/k)$ is finite. Then, the G-Euler characteristic of $\mathrm{Sel}(E/k_\infty)$ is well defined, and given by the formula*

$$\chi(G, \mathrm{Sel}(E/k_\infty)) = \frac{|\ Ш(E/k)(p)|}{|E(k)_{p^\infty}|^2} \cdot \prod_{v|p} |\widetilde{E}_v(\kappa_v)(p)|^2 \cdot \prod_v |c_v|_p^{-1}.$$

Here, $Ш(E/k)(p)$ denotes the p-primary part of $Ш(E/K)$, $E(k)_{p^\infty}$ the p-primary part of $E(k)$, κ_v the residue field at v, $\widetilde{E}_v$ the reduction of E over κ_v, and $c_v = [E(k_v) : E_0(k_v)]$ the local Tamagawa factor at a prime $v \subset \mathcal{O}_k$.

Proof See for instance [13][Theorem 4.1] The proof is a standard computation, using the facts that (i) $X(E/k_\infty)$ is $\Lambda(G)$-torsion (by Theorem 3.8 above), (ii) $E(k_\infty)_{p^\infty}$ is finite (by Lemma 3.10 above), and (iii) p is totally ramified in k_∞. □

$\Lambda(H)$-module structure. Let us assume now that $\mu_E(k) = 0$. We obtain the following $\Lambda(H)$-module structure theory for $X(E/k_\infty)$.

Theorem 3.12 *Suppose that E has good ordinary reduction at p, with $\mu_E(k) = 0$. Then, there is a $\Lambda(H)$-module isomorphism $X(E/k_\infty) \cong \Lambda(H)^{\lambda_E(k)}$.*

Proof By Nakayama's lemma, $X(E/k_\infty)$ is finitely generated over $\Lambda(H)$ if and only if $X(E/k_\infty)_H$ is finitely generated over $\mathbf{Z}_p$, hence by duality if and only if $S(E/k_\infty)^H$ is co-finitely generated over $\mathbf{Z}_p$. Given $n \geq 0$ an integer, let D_n denote the degree-p^n extension of k contained in D_∞, with D_n^{cyc} its cyclotomic $\mathbf{Z}_p$-extension. Let $H_n = \mathrm{Gal}(k_\infty/D_n^{\mathrm{cyc}})$. Note that $\mathrm{cd}_p(H_n) \leq 1$. Consider the diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & S(E/k_\infty)^{H_n} & \longrightarrow & H^1(G_S(k_\infty), E_{p^\infty})^{H_n} & \longrightarrow & \bigoplus_{v\in S} J_v(k_\infty)^{H_n} \\
 & & \uparrow{\scriptstyle \alpha_n} & & \uparrow{\scriptstyle \beta_n} & & \uparrow{\scriptstyle \gamma_n} \\
0 & \longrightarrow & S(E/D_n^{\mathrm{cyc}}) & \longrightarrow & H^1(G_S(D_n^{\mathrm{cyc}}), E_{p^\infty}) & \longrightarrow & \bigoplus_{v\in S} J_v(D_n^{\mathrm{cyc}}).
\end{array}$$

Here, the horizontal rows are exact sequences, and the vertical maps are induced by restriction on cohomology. We have by inflation-restriction that $\mathrm{coker}(\beta_n) \cong H^2(H_n, E_{p^\infty}) = 0$ and that $\ker(\beta_n) \cong H^1(H_n, E_{p^\infty})$. Note that $H^1(H_n, E_{p^\infty})$ has cardinality equal to that of $E(D_n^{\mathrm{cyc}})_{p^\infty}$, which is finite by Imai's theorem [21]. Given $v \in S$, fix a place w above v in k_∞. We can then write the local restriction map as

$$\gamma_n = \bigoplus_w \gamma_{n,w},$$

where the direct sum ranges over the primes above each $v \in S$ in D_n. Let $\Omega_{n,w}$ denote the decomposition group of H_n at w. We argue as in the proof of Lemma 3.3 that $\mathrm{coker}(\gamma_n) = 0$. Following [4, Lemma 3.7] also find that

$$\mathrm{coker}(\gamma_{n,w}) \cong H^2(\Omega_{n,w}, E_{p^\infty}) = 0 \ \text{ and } \ \ker(\gamma_{n,w}) \cong H^1(\Omega_{n,w}, E_{p^\infty}).$$

In particular, since the latter group is known to be finite, it follows that $\ker(\gamma_n) = \bigoplus_w \ker(\gamma_{n,w})$ is finite. It then follows from the snake lemma that $\ker(\alpha_n)$ and $\mathrm{coker}(\alpha_n)$ must be finite. Now, recall that $X(E/k^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion by Theorem 3.1. Matsuno's theorem [28] then implies that $X(E/k^{\mathrm{cyc}})$ has no nontrivial finite $\Lambda(\Gamma)$-submodule. On the other hand, since $\mu_E(k) = 0$, Hachimori and Matsuno's analogue of Kida's formula [12] implies that $X(E/D_n^{\mathrm{cyc}})$ is $\Lambda(\Gamma_n)$-torsion with $\Gamma_n = \mathrm{Gal}(D_n^{\mathrm{cyc}}/D_n)$ and cyclotomic Iwasawa invariants

$$\lambda_E(D_n) = [D_n : k] \cdot \lambda_E(k) \ \text{ and } \ \mu_E(D_n) = \mu_E(k) = 0.$$

Since D_n is not totally real, it follows from Proposition 7.5 of Matsuno [28] that $X(E/D_n^{\mathrm{cyc}})$ has no nontrivial finite $\Lambda(\Gamma_n)$-submodule. In particular, since $\mu_E(D_n) = 0$ for each $n \geq 0$, Matsuno's theorem implies that $X(E/D_n^{\mathrm{cyc}})$ has no nontrivial finite $\mathbf{Z}_p$-submodule for any $n \geq 0$. This makes the inverse limit $X(E/k_\infty) = \varprojlim_n X(E/D_n^{\mathrm{cyc}})$ $\mathbf{Z}_p$-torsionfree, from which it follows that $\ker(\alpha_n) = \mathrm{coker}(\alpha_n) = 0$ for any $n \geq 0$. Thus, we find an isomorphism of $\mathbf{Z}_p$-modules $\alpha_0 : X(E/k_\infty)_{H_0} \cong X(E/k^{\mathrm{cyc}})$. Let us now put $r = \lambda_E(k)$. Let $x_1, \ldots, x_r$ denote a lift to $X(E/k_\infty)$ of a fixed $\mathbf{Z}_p$-basis of $X(E/k_\infty)_H$. Let $I(H)$ denote the augmentation ideal of H in $\Lambda(H)$. Note that $X(E/k_\infty)_H = X(E/k_\infty)/I(H)$. Let Y denote the $\Lambda(H)$-submodule of $X(E/k_\infty)$ generated by $x_1, \ldots x_r$. Observe that

$$I(H)(X(E/k_\infty)/Y) = (I(H)X(E/k_\infty) + Y)/Y = X(E/k_\infty)/Y,$$

and so $X(E/k_\infty) = Y$ by Nakayama's lemma. In particular, this gives an isomorphism of $\Lambda(H)$-modules

$$X(E/k_\infty) \cong \Lambda(H)^r, \qquad \sum_i a_i x_i \longmapsto \sum_i a_i e_i,$$

where $e_1, \ldots, e_r$ is a standard $\Lambda(H)$-basis of $\Lambda(H)^r$. Observe now that $X(E/k_\infty)$ has no nontrivial finite $\Lambda(H)$-submodule, thus making it $\Lambda(H)$-torsionfree. $\square$

Corollary 3.13 *Suppose that E has good ordinary reduction at each prime above p in k, with $\mu_E(k) = 0$. Then, $\mu_{\Lambda(G)}\left(X(E/k_\infty)\right) = \mu_E(k) = 0$.*

Proof The result follows from argument of Theorem 3.12 above, namely by using Matsuno's theorem [28] and the main result of Hachimori-Matsuno [12] to deduce that $X(E/k_\infty)$ is $\Lambda(H)$-torsionfree. □

We also deduce from Theorem 3.12 the following consequence for the $\Lambda(H)$-corank of the p-primary parts of the Tate-Shafarevich group $Ш(E/k_\infty)$. That is, recall that we consider the short exact descent sequence of $\Lambda(H)$-modules

$$0 \longrightarrow E(k_\infty) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathrm{Sel}(E/k_\infty) \longrightarrow Ш(E/k_\infty)(p) \longrightarrow 0,$$

as well as the dual exact sequence

$$0 \longrightarrow \mathfrak{X}(E/k_\infty) \longrightarrow X(E/k_\infty) \longrightarrow \mathcal{E}(E/k_\infty) \longrightarrow 0. \tag{11}$$

Here, $\mathfrak{X}(E/k_\infty)$ is the Pontryagin dual of $Ш(E/k_\infty)(p)$, and $\mathcal{E}(E/k_\infty)$ is that of $E(k_\infty) \otimes \mathbf{Q}_p/\mathbf{Z}_p$. Recall that we let $\epsilon(E/k, 1) = \epsilon(f/k, 1)$ denote the root number of the complex L-function $L(E/k, s) = L(f \times \Theta_k, s)$.

Proposition 3.14 *Assume that p is odd, and moreover that p does not divide the class number of k if the root number $\epsilon(E/k, 1)$ equals -1. If E has good ordinary reduction at each prime above p in k with $\mu_E(k) = 0$, then*

$$\mathrm{rk}_{\Lambda(H)}\ \mathfrak{X}(E/k_\infty) = \begin{cases} \lambda_E(k) & \text{if } \epsilon(E/k, 1) = +1 \\ \lambda_E(k) - 1 & \text{if } \epsilon(E/k, 1) = -1. \end{cases}$$

Proof Observe that (11) is a short exact sequence of finitely generated $\Lambda(H)$-modules. We know by Theorem 3.12 that the $\Lambda(H)$-rank of $X(E/k_\infty)$ is $\lambda_E(k)$. On the other hand, we claim that

$$\mathrm{rk}_{\Lambda(H)}\mathcal{E}(E/k_\infty) = \begin{cases} 0 & \text{if } \epsilon(E/k, 1) = +1 \\ 1 & \text{if } \epsilon(E/k, 1) = -1. \end{cases} \tag{12}$$

To see why this is so, let K be any finite extension of k contained in k^{cyc}. A simple exercise shows that K is a totally imaginary quadratic extension of its maximal totally real subfield F. Let D_∞^K denote the compositum extension KD_∞, with Galois group $\Omega_K = \mathrm{Gal}(D_\infty^K/K)$. We claim that for any such K, we have the rank formula

$$\mathrm{rk}_{\Lambda(\Omega_K)}\mathcal{E}(E/D_\infty^K) = \begin{cases} 0 & \text{if } \epsilon(E/k, 1) = +1 \\ 1 & \text{if } \epsilon(E/k, 1) = -1. \end{cases}$$

Indeed, in the first case with $\epsilon(E/k, 1) = +1$, the formula follows from the relevant nonvanishing theorem of Cornut-Vatsal [9, Theorem 1.4] over F plus the relevant rank theorem(s) of Nekovar [29, Theorem B, Theorem B', and

Corollary]. In the second case with $\epsilon(E/k,1) = -1$, the formula follows form the relevant nonvanishing theorem of Cornut-Vatsal [9, Theorem 1.5] over F plus the relevent rank theorem of Howard [19, Theorem B (a)]. Note that to invoke the result of Howard [19] in the latter setting, we have used the classical result due to Iwasawa [22] that if p does not divide the class number of k, then p does not divide the class number of any finite extension K. Taking the inductive limit over all finite extensions K of k contained in k^{cyc}, we obtain the stated formula (12). The result then follows immediately from the exactness of (11). □

4 Divisibility criteria

We now discuss various divisibility criteria for the two-variable main conjecture (Conjecture 1.1 (iii) above). In particular, granted suitable hypotheses, we prove one divisibility of the two-variable main conjecture.

Greenberg's criterion. The following criterion was suggested to the author by Ralph Greenberg. It reduces one divisibility of the two-variable main conjecture (Conjecture 1.1 (iii)) to a certain specialization criterion for finite order characters of the Galois group $\Gamma = \mathrm{Gal}(k^{cyc}/k)$. Let us first fix an isomorphism

$$\Lambda(G) \cong \mathbf{Z}_p[[T_1, T_2]], \;\; (\gamma_1, \gamma_2) \longmapsto (T_1 + 1, T_2 + 1)\,. \tag{13}$$

Here, we have fixed a topological generator γ_1 of Γ, as well as a topological generator γ_2 of Ω. Fix $f \in S_2(\Gamma_0(N))$ a p-ordinary eigenform, as required for the construction of the p-adic L-function of Theorem 2.9. Recall that we write $X(f/k_\infty)$ to denote the Pontryagin dual of the p^∞-Selmer group associated to f in k_∞/k. If f is the eigenform associated to an elliptic curve E defined over $\mathbf{Q}$, then a standard argument allows us to make the identification $X(f/k_\infty) = X(E/k_\infty)$. In what follows, we shall fix an elliptic curve E over $\mathbf{Q}$ of conductor N as described in the introduction, with f the eigenform associated to E by modularity. We shall then make the identification $X(f/k_\infty) = X(E/k_\infty)$ implicitly in what follows.

Let $g(T_1, T_2)$ denote the $\Lambda(G)$-characteristic power series of $X(f/k_\infty)$, or rather its image under the fixed isomorphism (13). (We take this to be zero if $X(f/k_\infty)$ is not $\Lambda(G)$-torsion). Let $L(T_1, T_2) = L_p(f,k)(T_1, T_2)$ denote the image under (13) of the two-variable p-adic L-function $L_p(f,k) \in \Lambda(G)$ associated to f by Theorem 2.9. Recall that we write Ψ to denote the set of finite order characters of $\Gamma = \mathrm{Gal}(k^{cyc}/k)$. Given an element element $\lambda \in \Lambda(G)$ with associated power series $\lambda(T_1, T_2) \in \mathbf{Z}_p[[T_1, T_2]]$, we can and will invoke the usual Weierstrass preparation theorem for $\lambda(T_1, T_2)$ as an element of the one-variable power series ring $R[[T_1]]$ with $R = \mathbf{Z}_p[[T_2]]$. We refer the reader to the discussion in Venjakob [45, Example 2.4, Theorem 3.1, and Corollary 3.2] for a more general account of the situation.

Theorem 4.1 *Suppose that p does not divide the specialization $g(T_1, 0)$. Assume that for each character $\psi \in \Psi$, we have the inclusion of ideals*

$$(L(T_1, \psi(T_2))) \subseteq (g(T_1, \psi(T_2))) \;\; \textit{in } \mathcal{O}_\psi[[T_1, T_2]]. \tag{14}$$

Then, we have the inclusion of ideals

$$(L(T_1, T_2)) \subseteq (g(T_1, T_2)) \text{ in } \mathbf{Z}_p[[T_1, T_2]].$$

Proof Observe that we may write

$$g(T_1, T_2) = \sum_{i=0}^{\infty} a_i(T_2) \cdot T_1^i,$$

with $a_i(T_2) \in \mathbf{Z}_p[[T_2]]$. Since we assume that $p \nmid g(T_1, 0)$, it follows that for some minimal positive integer m,

$$g(T_1, 0) = \sum_{i=0}^{m} a_i(0) \cdot T_1^i,$$

with $a_i(0) \in \mathbf{Z}_p^{\times}$. We claim it then follows that

$$L(T_1, T_2) = h(T_1, T_2) \cdot g(T_1, T_2) + r(T_1, T_2),$$

with $h(T_1, T_2)$ a polynomial in $\mathbf{Z}_p[[T_1, T_2]]$, and $r(T_1, T_2)$ a remainder polynomial in $\mathbf{Z}_p[[T_2]]$ of degree less than m. Now, the remainder term is given by

$$r(T_1, T_2) = \sum_{j=0}^{m-1} c_j(T_2) \cdot T_1^j,$$

with $c_j(T_2) \in \mathbf{Z}_p[[T_2]]$. Granted the inclusion (22) for each $\psi \in \Psi$, we have that

$$r(T_1, \psi(T_2)) = 0$$

for each $\psi \in \Psi$. It then follows from the Weierstrass preparation theorem that

$$c_j(\psi(T_2)) = 0$$

for each $\psi \in \Psi$ and $j \in \{0, \ldots, m-1\}$. Hence, we conclude that $r(T_1, T_2) = 0$. $\square$

We obtain the following immediate consequence.

Corollary 4.2 *Assume Hypothesis 1.6 (i) and (ii). Suppose that for each character $\psi \in \Psi$, we have the inclusion of ideals*

$$(L(T_1, \psi(T_2))) \subseteq (g(T_1, \psi(T_2))) \text{ in } \mathcal{O}_{\psi}[[T_1, T_2]]. \tag{15}$$

Then, we have the inclusion of ideals

$$(L(T_1, T_2)) \subseteq (g(T_1, T_2)) \text{ in } \mathbf{Z}_p[[T_1, T_2]].$$

Proof Theorem 4.1 requires that p does not divide the specialization of the characteristic power series $g(T_1, 0)$, equivalently that the dihedral or anticyclotomic μ-invariant associated to f in the tower D_∞/k vanishes. Assuming Hypothesis 1.6 (i) and (ii), the main result of Pollack-Weston [31] shows that this is always the case if the underlying eigenform f is p-ordinary. $\square$

A basechange criterion Let K be any finite extension of k contained in the cyclotomic extension k^{cyc}. Let D_∞^K denote the compositum extension KD_∞, with $\Omega_K = \mathrm{Gal}(D_\infty^K/K)$ the corresponding Galois group. Note that Ω_K is topologically isomorphic to $\mathbf{Z}_p$. Let Ψ_K denote the set of (primitive) characters of order $[K : k]$ of the Galois group $\mathrm{Gal}(K/k)$. Hence, we have the decomposition

$$\Psi = \bigcup_{k \subset K \subset k^{\mathrm{cyc}}} \Psi_K.$$

Recall that given a character $\psi \in \Psi$, we write $\mathcal{O}_\psi$ to denote the ring of integers obtained from $\mathbf{Z}_p$ by adding the values of ψ. Let us also write $\mathcal{O}_{\Psi_K}$ to denote the ring of integers obtained by adding to $\mathbf{Z}_p$ the values of each of the characters in the set Ψ_K. Given a polynomial $f(T_1, T_2) \in \mathbf{Z}_p[[T_1, T_2]]$, let us write

$$f(T_1, T_2^K) = \prod_{\psi \in \Psi_K} f(T_1, \psi(T_2)) \tag{16}$$

to denote the product of specializations of $f(T_1, T_2)$ to the characters of the set Ψ_K. Note that this specialization product $f(T_1, T_2^K)$ lies in the polynomial ring $\mathbf{Z}_p[[T_1, T_2^K]] = \mathcal{O}_{\Psi_K}[[T_1]]$. Note as well that we have the identifications

$$f(T_1, T_2^k) = f(T_1, \mathbf{1}(T_2)) = f(T_1, 0) \in \mathbf{Z}_p[[T_1]].$$

Proposition 4.3 *Assume that for any finite extension K of k contained in k^{cyc}, we have the inclusion of ideals*

$$\big(L(T_1, T_2^K)\big) \subseteq \big(g(T_1, T_2^K)\big) \ \textit{in } \mathcal{O}_{\Psi_K}[[T_1]]. \tag{17}$$

Assume additionally that the root number of the central value $L(f/k, 1)$ is $+1$, and moreover that we have a nontrivial equality of ideals for $K = k$,

$$(L(T_1, 0)) = (g(T_1, 0)) \ \textit{in } \mathbf{Z}_p[[T_1]]. \tag{18}$$

Then, for each character $\psi \in \Psi$, we have the inclusion of ideals

$$(L(T_1, \psi(T_2))) \subseteq (g(T_1, \psi(T_2))) \ \textit{in } \mathcal{O}_\psi[[T_1]].$$

Proof Since we assume that the root number $\epsilon(f/k, 1)$ is equal to $+1$, we know for instance by the nonvanishing theorems of Vatsal [44] and more generally Cornut-Vatsal [9] that the p-adic L-function $L(T_1, 0)$ does not vanish identically. Let K be any finite extension of k contained in k^{cyc}. Using the equality (18), we

may then divide each side of (17) by the corresponding ideals in (18) to obtain for each extension K the inclusion of ideals

$$\left(\frac{L(T_1, T_2^K)}{L(T_1, 0)}\right) \subseteq \left(\frac{g(T_1, T_2^K)}{g(T_1, 0)}\right) \text{ in } \mathcal{O}_{\Psi_K}[[T_1]]. \tag{19}$$

Now, the divisibility (17) implies that we have for each extension K the relation

$$g(T_1, T_2^K) = f(T_1, T_2^K) \cdot L(T_1, T_2^K) + r(T_1, T_2^K).$$

Here, $f(T_1, T_2^K)$ denotes some polynomial in $\mathbf{Z}_p[[T_1, T_2^K]] = \mathcal{O}_{\Psi_K}[[T_1]]$, and $r(T_1, T_2^K)$ the corresponding remainder term. It then follows from (19) that

$$\prod_{\substack{\psi \in \Psi_K \\ \psi \neq 1}} r(T_1, \chi(T_2)) = 0.$$

Hence, we deduce that for each finite extension K of k contained in k^{cyc}, there exists a nontrivial character $\psi \in \Psi_K$ such that

$$(L(T_1, \psi(T_2))) \subseteq (g(T_1, \psi(T_2))) \text{ in } \mathcal{O}_\psi[[T_1]]. \tag{20}$$

We now argue that if the divisibility (20) holds for one (nontrivial) character in Ψ_K, then it holds for all (nontrivial) characters in Ψ_K. To see why this is, let $\mathcal{L}(E/k, \mathcal{W}, 1) = \mathcal{L}(f \times \Theta(\mathcal{W}), 1)$ denote the value

$$\frac{L(f \times \Theta(\mathcal{W}), 1)}{8\pi\langle f, f\rangle}, \tag{21}$$

where $\mathcal{W}$ is any finite order character of the Galois group G. Recall that the value (21) is algebraic by Shimura's theorem [39]. In particular, for any finite order character ρ of Ω, the values $\mathcal{L}(f \times \Theta(\rho\psi), 1)$ with $\psi \in \Psi_K$ are Galois conjugate by Shimura's theorem. Hence, by uniqueness of interpolation series, we deduce that the specializations $L(T_1, \psi(T_2))$ with $\psi \in \Psi_K$ are Galois conjugate. We can then deduce that if the divisibility (20) holds for one character $\psi \in \Psi_K$, then it holds for all characters $\psi \in \Psi_K$. Taking the union of all finite extensions K of k contained in k^{cyc}, the result follows. □

Corollary 4.4 *Keep the hypotheses of Proposition 4.3 above. If p does not divide the specialization $g(T_1, 0)$, then there is an inclusion of ideals*

$$(L(T_1, \psi(T_2))) \subseteq (g(T_1, \psi(T_2))) \text{ in } \mathcal{O}_\psi[[T_1, T_2]]. \tag{22}$$

Proof Apply Theorem 4.1 to Proposition 4.3 above. □

Some remarks on further reductions. A simple argument shows that each finite extension K of k contained in k^{cyc} is a totally imaginary quadratic extension of its maximal totally real subfield F. Each such totally real field F is abelian. Hence, we can associate to f a Hilbert modular eigenform $\mathbf{f}$ over

F via the theory of cyclic basechange. It is then simple to see (via Artin formalism for instance) that the root number of the complex Rankin-Selberg L-function $L(\mathbf{f} \times \Theta_K, s)$ is equal to that of $L(E/k, s) = L(f \times \Theta_k, s)$. In particular, the divisibilities (17) of Proposition 4.3 would follow from the dihedral/anticyclotomic main conjectures for $\mathbf{f}$ in the dihedral/anticyclotomic $\mathbf{Z}_p^d$-extension of K, where $d = [F : \mathbf{Q}]$. For results in this direction, see for instance the generalizations to totally real fields of work of Bertolini-Darmon [1] (as well as Pollack-Weston [31]) by Longo [27] and the author [42]. For the equality condition (18) of Proposition 4.3, see the result of Howard [17, Theorem 3.2.3] with the main result of Pollack-Weston [31]. These works combined show that the inclusion $(L(T_1, 0)) \subseteq (g(T_1, 0))$ often holds, in which case the reverse inclusion $(g(T_1, 0)) \subseteq (L(T_1, 0))$ can be reduced by Howard [17, Theorem 3.2.3(c)] to a certain nonvanishing criterion for the associated p-adic L-functions $L(T_1, 0) \in \Lambda(\Omega)$.

Some remarks on the setting of root number minus one. In the setting where the root number $\epsilon(f/k, 1)$ of $L(f/k, 1)$ is equal to -1, then we know that $L(T_1, T_2) = 0$ by the functional equation for $L(T_1, T_2)$ given in Corollary 2.10 (derived from the fact that the complex central value $L(f/k, 1)$ vanishes). It follows that $L(T_1, T_2^K) = 0$ for all finite extensions K of k contained in k^{cyc}. Hence in this setting, the hypotheses of Proposition 4.3 do not hold. Indeed, consider the basechange setup described in the remark above, where $\mathbf{f}$ is the basechange Hilbert modular eigenform defined over the maximal totally real subfield F of K. The formulation of the analogous dihedral/anticyclotomic main conjecture in this setting asserts that each dual Selmer group $X(\mathbf{f}/D_\infty^K)$ has $\Lambda(\Omega_K)$-rank one, and moreover that there is an equality of ideals

$$\big(\mathrm{char}_{\Lambda(\Omega_K)}(X(\mathbf{f}/D_\infty^K)_{\mathrm{tors}})\big) = \big(\mathrm{char}_{\Lambda(\Omega_K)}(\mathfrak{X}(\mathbf{f}/D_\infty^K))\big) \text{ in } \Lambda(\Omega_K)$$

Here, $X(\mathbf{f}/D_\infty^K)_{\mathrm{tors}}$ denotes the $\Lambda(\Omega_K)$-torsion submodule of $X(\mathbf{f}/D_\infty^K)$, and $\mathfrak{X}(\mathbf{f}/D_\infty^K)$ is the $\Lambda(\Omega_K)$-torsion submodule defined by $\mathfrak{S}(\mathbf{f}/D_\infty^K)/H(\mathbf{f}/D_\infty^K)$, where $\mathfrak{S}(\mathbf{f}/D_\infty^K)$ is the compactified Selmer group of $\mathbf{f}$ over D_∞^K, and $H(\mathbf{f}/D_\infty^K)$ is the so-called Heegner submodule generated by CM points (defined on an associated quaternionic Shimura curve). We refer the reader to Howard [19, Theorem B] or Perrin-Riou [33] for more details on this formulation. Anyhow, the dual Selmer group $X(\mathbf{f}/D_\infty^K)$ does not have a $\Lambda(\Omega_K)$ characteristic power series in this setting. If we adopt the standard convention of taking the characteristic power series to be 0 in this case, then we obtain for each extension K the trivial equality of ideals $\big(L(T_1, T_2^K)\big) = \big(g(T_1, T_2^K)\big)$ in $\mathcal{O}_{\Psi_K}[[T_1]]$. It therefore seems unlikely that we can do any better than Theorem 4.2 for determining a two-variable divisibility criterion by considering main conjecture divisibilities via basechange. This is especially apparent after noting of the shape of the two-variable main conjecture in this case, as described for instance in Howard [18]. To be somewhat more precise, recall that we fixed a topological generator γ_2 of Γ for our fixed isomorphism (13). The two-variable p-adic L-function $L_p(f, k_\infty)$

can then be written as a power series

$$\mathcal{L}_f = \mathcal{L}_{f,0} + \mathcal{L}_{f,1} \cdot (\gamma_2 - 1) + \ldots \in \Lambda(G),$$

with coefficients $\mathcal{L}_{f,n} \in \mathbf{Z}_p[[\Omega]]$. In the case where the root number $\epsilon(f/k, 1)$ is -1, we know by the associated functional equation(s) that $\mathcal{L}_{f,0} = 0$. Another result of Howard (proving one divisibility of a conjecture made by Perrin-Riou in [33]) shows that the second term $\mathcal{L}_{f,1}$ can be expressed as a certain twisted sum of images under any appropriate p-adic height pairing of some associated regularized Heegner points (see [18, Theorem A]). If p does not divide the level N of f, then we know by Theorem 3.8 that $\mathrm{char}_{\Lambda(G)} X(f/k_\infty)$ exists, equivalently that $g(T_1, T_2) \neq 0$. Now, two-variable characteristic power series $\mathrm{char}_{\Lambda(G)} X(f/k_\infty)$ can be written as a power series

$$\mathcal{G}_f = \mathcal{G}_{f,0} + \mathcal{G}_{f,1} \cdot (\gamma_2 - 1) + \ldots \in \Lambda(G),$$

with coefficients $\mathcal{G}_{f,n} \in \mathbf{Z}_p[[\Omega]]$. Hence, if we know that $g(T_1, 0) = 0$, then we find that $\mathcal{G}_{f,0} = 0$. This would reduce our task to showing $\mathcal{G}_f \mid \mathcal{L}_f$ in $\Lambda(G)$, where both $\mathcal{G}_f$ and $\mathcal{L}_f$ correspond under the fixed isomorphism (13) to power series that vanish at $T_2 = 0$. It is then apparent from this fact that comparing the products of specializations to characters $\psi \in \Psi_K$ of these power series alone will not give much more information, as Ψ_K contains the trivial character.

References

[1] M. Bertolini and H. Darmon, *Iwasawa's Main Conjecture for elliptic curves over anticyclotomic $\mathbf{Z}_p$-extensions*, Annals of Math. **162** (2005), 1 - 64.

[2] N. Bourbaki, *Élements de mathématique, Fasc. XXXI, Algèbre commutative, Chapitre 7: Diviseurs*, Actualiés Scientifiques et Industrielles, **1314**, Paris, Hermann, (1965).

[3] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises*, Jour. Amer. Math. Soc. **14** (2001), 843-939.

[4] J. Coates, *Fragments of GL_2 Iwasawa Theory of Elliptic Curves without Complex Multiplication*, in Arithmetic Theory of Elliptic Curves, ed. C. Viola, Lecture Notes in Math., 1716 (1997), 1-50.

[5] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Inventiones math. 124 (1996), 124-178.

[6] J. Coates and A. Wiles, *On the Conjecture of Birch and Swinnerton-Dyer*, Inventiones math. **39** (1977), 223 - 251.

[7] J. Coates, P. Schneider, and R. Sujatha, *Links between cyclotomic and GL_2 Iwasawa theory*, Doc. Math. Extra Volume: Kazuya Kato's 50th birthday (2003), 187-215.

[8] J. Coates, and R. Sujatha, *Galois Cohomology of Elliptic Curves*, Tata Institute of Fundamental Research Lectures on Mathematics **88**, Narosa Publishing House (2000).

[9] C. Cornut and V. Vatsal, *Nontriviality of Rankin-Selberg L-functions and CM points*, L-functions and Galois Representations, Ed. Burns, Buzzard and Nekovář, Cambridge University Press (2007), 121 - 186

[10] B. Gross, *Heights and the Special Values of L-series*, Can. Math. Soc. Conference Proceedings, **7** (1987).

[11] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Inventiones math. **84** No. 2 (1986), 225-320.

[12] Y. Hachimori and K. Matsuno, *An analogue of Kida's formula for Selmer groups of elliptic curves*, Jour. Alg. Geom. 8 (1999), 581-601.

[13] Y. Hachimori and O. Venjakob, *Completely faithful Selmer groups over Kummer extensions*, Doc. Math. Extra Volume: Kazuya Kato's 50th birthday (2003), 2-36.

[14] H. Hida, *A p-adic measure attached to the zeta functions associated to two elliptic modular forms I*, Inventiones math. **79**, 159-195 (1985).

[15] E. Hecke, *Arithmetik der positiven quadratischen Formen*, in Mathematische Werke, Göttingen: Vandenhoeck und Ruprecht (1959), 789 - 918.

[16] E. Hecke, *Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik*, Ab. aus dem Math. Seminar der Hamburgischen Universität Bd. 5 (1927), 199-224.

[17] B. Howard, *Bipartite Euler systems*, J. reine angew. Math. **597** (2006).

[18] B. Howard, *The Iwasawa theoretic Gross-Zagier theorem,* Compositio Math. **141** No. 4 (2005), 811 - 846.

[19] B. Howard, *Iwasawa theory of Heegner points on abelian varieties of GL_2-type,* Duke Math. Jour. **124** No. 1 (2004), 1-45.

[20] S. Howson, *Euler characteristics as invariants of Iwasawa modules*, Proc. London Math. Soc. **(3)** 85 (2002) 634-658.

[21] H. Imai, *A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_l$-extensions*, Proc. Japan. Acad. Math. Sci. **51** (1975), 12-16.

[22] K. Iwasawa, *On the $\mathbf{Z}_l$-extensions of algebraic number fields*, Annals of Math. **98** (1973), 246 - 326.

[23] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adique et applications arithmetiques III, Astérisque 295 (2004), 117-290.

[24] N. Katz, *The Eisenstein measure and p-adic interpolation*, American Journal of Mathematics **99** (1977), 238-311.

[25] N. Katz, *p-adic interpolation of real analytic Eisenstein series*, Annals of Math. **104** (1976), 459-571.

[26] M. Lazard, *Groupes analytiques p-adiques*, Inst. Hautes Études Sci. Publ. Math. (1965), 389 - 603.

[27] M. Longo, *Anticyclotomic Iwasawa's Main Conjecture for Hilbert Modular Forms*, to appear in Commentarii Math. Helv.

[28] K. Matsuno, *Finite Λ-submodules of Selmer groups of abelian varieties over cyclotomic $\mathbf{Z}_p$-extensions*, Journal of Number Theory 99 (2003), 415-443.

[29] J. Nekovar, *Level raising and anticyclotomic Selmer groups for Hilbert modular forms of weight* 2, to appear in Canadian J. Math.

[30] R. Pollack, *Tables of Iwasawa invariants of elliptic curves*, available at `http://math.bu.edu/people/rpollack/Data/data.html`.

[31] R. Pollack and T. Weston, *On anticyclotomic μ-invariants of modular forms,* to appear in Compositio Math.

[32] B. Perrin-Riou, *Fonctions L p-adiques attachées á une courbe elliptique modulaire et á un corps quadratique imaginaire*, Jour. London Math Soc. **(2)** 38 (1988), 1-32.

[33] B. Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115**(4) (1987) 399-456.

[34] D. Rohrlich, *On L-funtions of elliptic curves and cyclotomic towers*, Inventiones math. **75** (1984), 409-423.

[35] K. Rubin, *On the main conjectures of Iwasawa theory for imaginary quadratic fields*, Inventiones math. **93** (1988), 701 - 713.

[36] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Inventiones math. **103** (1991), 25 - 68.

[37] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones math. **115** (1972), 259 - 331.

[38] J.-P. Serre, *Sur la dimension cohomologique des groupes profinis*, Topology **3** (1965) 413 - 420.

[39] G. Shimura, *On the Periods of Modular Forms*, Math. Ann. **229** (1977), 211-221.

[40] C. Skinner and E. Urban, *The Main Conjecture for $GL(2)$*, preprint (2010), available at `http://www.math.columbia.edu/~urban/EURP.html`

[41] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math., **141** (1995), 553-572.

[42] J. Van Order, *On the dihedral main conjectures of Iwasawa theory for Hilbert modular eigenforms*, submitted (2011), available at `http://arxiv.org/abs/1112.3823`

[43] J. Van Order, *On the quaternionic p-adic L-functions associated to Hilbert modular eigenforms*, submitted (2011), available at `http://arxiv.org/abs/1112.3821`

[44] V. Vatsal, *Uniform distribution of Heegner points*, Inventiones math. **148** 1-46 (2002).

[45] O. Venjakob, *A noncommutative Weierstrass preparation theorem and applications to Iwasawa theory*, J. reine angew. Math. **559** (2003), 153-191.

[46] L. Washington, *Introduction to Cyclotomic Fields, Second Edition*, Springer GTM **83** (1991).

[47] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math. **141** (1995), 443-551.

[48] R.I. Yager, *On the two-variable p-adic L-functions*, Annals of Math. **115** (1982), 411-449.