The anticyclotomic Main Conjecture for elliptic curves at supersingular primes

Henri Darmon
Adrian Iovita

September 29, 2007

Abstract

The Main Conjecture of Iwasawa theory for an elliptic curve E over $\mathbb{Q}$ and the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field K was studied in [BD2], in the case where p is a prime of ordinary reduction for E. Analogous results are formulated, and proved, in the case where p is a prime of supersingular reduction. The foundational study of supersingular main conjectures carried out by Perrin-Riou [PR2], [PR4], Pollack [Po1], Kurihara [Ku], Kobayashi [Kob], and Iovita-Pollack [IP] are required to handle this case in which many of the simplifying features of the ordinary setting break down.

Contents

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N_0, and let K be an imaginary quadratic field of discriminant prime to N_0. Choose a rational prime p and let K_∞ denote the anticyclotomic $\mathbb{Z}_p$-extension of K.

To the datum (E, K, p) are associated two kinds of invariants:

1. The twisted special values $L(E/K, \chi, 1)$ of the Hasse-Weil L-series of E over K, as χ ranges over the finite-order characters of $G_\infty := \mathrm{Gal}(K_\infty/K)$. These special values satisfy certain algebraicity and integrality properties. When p is a prime of *ordinary* reduction for E, they can be conveniently packaged into a p-adic L-function $L_p(E, K)$ which belongs to the Iwasawa algebra $\Lambda := \mathbb{Z}_p[\![G_\infty]\!]$.

2. The Selmer group $\mathrm{Sel}(K_\infty, E_{p^\infty})$ consisting of classes in $H^1(K_\infty, E_{p^\infty})$ which are in the images of the local Kummer maps at all places of K_∞. This group is a co-finitely generated Λ-module. One of the interesting features of the anticyclotomic setting is that it need not be Λ-cotorsion in general. Let $\mathcal{C}$ denote the characteristic power series of the Pontryagin dual of the Selmer group, setting $\mathcal{C} = 0$ if this Pontryagin dual is not torsion over Λ. The invariant $\mathcal{C}$ is well-defined up to multiplication by units of Λ.

It is assumed that the discriminant of K is prime to $N := pN_0$ so that K determines a factorization

$$N = pN^+N^-,$$

where N^+ is divisible only by primes which are split in K and N^- by primes which are inert in K.

Under certain technical assumptions stated in the introduction of [BD2] which will be recalled below, the article [BD2] proves the following result in the direction of the anticyclotomic main conjecture of Iwasawa theory in the *ordinary case.* (Cf. Theorem 1 of [BD2].)

Theorem 1.1. *Assume that N^- is the square-free product of an odd number of primes. Assume also that the prime p is* ordinary*, and that (E, K, p) satisfies the technical hypotheses stated in 1.6 below. Then $\mathcal{C}$ divides the p-adic L-function $L_p(E, K)$.*

Remark 1.2. It follows from results of Vatsal [Va] that $L_p(E, K)$ is non-zero under the hypotheses on N made in Theorem 1.1. In particular, this theorem implies that the Selmer group of E over K_∞ is Λ-co-torsion. By contrast, when N^- is the square-free product of an *even* number of primes, then $L_p(E, K)$ vanishes identically. Vatsal's theorem on the non-triviality of Heegner points and arguments of Kolyvagin can be used to show that the Selmer group of E over K_∞ has Λ-corank one in this case.

The main goal of the present note is to formulate and prove an analogous result in the case where p is a prime satisfying

$$a_p := p + 1 - \#E(\mathbb{Z}/p\mathbb{Z}) = 0.$$

This implies that E is supersingular at p, and is in fact equivalent to this statement when $p \geq 5$, in light of the Hasse bound $|a_p| \leq 2\sqrt{p}$. The foundational study of supersingular main conjectures carried out by Perrin-Riou [PR2], [PR4], Pollack [Po1], Kurihara [Ku], Kobayashi [Kob], and Iovita-Pollack [IP] are required to handle this case in which many of the simplifying features of the ordinary setting break down.

1. The special values $L(E/K, \chi, 1)$ cannot be interpolated in an obvious way by an element of Λ. Section 2 explains how the construction of the p-adic L-function $L_p(E, K)$ presented in Section 1 of [BD2] can be modified, following the ideas of [PR2] and [Po1], by removing the infinitely many "trivial zeroes" that occur at p-power roots of unity. This process yields *two* p-adic L-functions $L_p^+(E, K)$ and $L_p^-(E, K)$ which both belong to Λ and emerge as the appropriate substitutes for the p-adic L-function in the supersingular setting.

2. In tandem with this analytic complication, the Selmer group $\mathrm{Sel}(K_\infty, E_{p^\infty})$ is *never* a co-torsion Λ-module when p is supersingular. Following an idea of Kobayashi [Kob], Section 3 introduces two restricted Selmer groups

$$\mathrm{Sel}_+(K_\infty, E_{p^\infty}) \quad \text{and} \quad \mathrm{Sel}_-(K_\infty, E_{p^\infty})$$

defined by imposing more stringent local conditions at the prime p. Let $\mathcal{C}^+$ and $\mathcal{C}^-$ denote the characteristic power series of the Pontryagin duals of $\mathrm{Sel}_+(K_\infty, E_{p^\infty})$ and $\mathrm{Sel}_-(K_\infty, E_{p^\infty})$ respectively. (Here we follow the same conventions as before, whereby the characteristic power series of a non-torsion Λ-module is taken to be 0.)

The main conjecture that we are interested in is formulated in terms of the plus/minus p-adic L-functions and the restricted Selmer groups, as follows:

Conjecture 1.3. *Assume that $a_p = 0$. Then the characteristic power series $\mathcal{C}^+$ and $\mathcal{C}^-$ generate the same ideal of Λ as the p-adic L-functions $L_p^+(E, K)$ and $L_p^-(E, K)$ respectively.*

Fix an integer $n \geq 1$. A key ingredient in the proof of Theorem 1.1 given in [BD2] is the construction of certain global cohomology classes

$$\kappa(\ell) \in \lim_{\leftarrow m} H^1(K_m, E[p^n]),$$

indexed by rational primes ℓ satisfying suitable properties (the *n-admissible primes* in the sense of [BD2]). These classes form a kind of Euler system, as spelled out in Sections 4 and 7 of [BD2]. Section 4 of this paper explains how the construction of [BD2] can be modified in the supersingular case to yield classes $\kappa^+(\ell)$ and $\kappa^-(\ell)$ satisfying properties analogous to the classes $\kappa(\ell)$ of [BD2]. The strategy of the proof of Theorem 1.1 carries over to establish one of the divisibilities predicted by Conjecture 1.3, which is the main result of this paper.

Theorem 1.4. *Assume that $a_p = 0$ and that N^- is the square-free product of an odd number of primes. Assume also that (E, K, p) satisfies the hypotheses stated in 1.6 and 1.7 below. Then the characteristic power series $\mathcal{C}^+$ and $\mathcal{C}^-$ divide the p-adic L-functions $L_p^+(E, K)$ and $L_p^-(E, K)$ respectively.*

Remark 1.5. When N^- is the square-free product of an even number of primes, the p-adic L-functions $L_p^+(E, K)$ and $L_p^-(E, K)$ vanish identically, much as in the ordinary case, and the corresponding Selmer groups are not Λ-co-torsion.

Throughout this article, the following assumptions are made on (E, K, p):

Assumptions 1.6.

1. *The prime p is greater or equal to* 5.
2. *The Galois representation attached to E_p has image isomorphic to $\mathbf{GL}_2(\mathbb{F}_p)$.*
3. *There is a modular parameterization $X_0(N_0) \longrightarrow E$ whose degree is not divisible by p.*
4. *For all primes ℓ such that ℓ^2 divides N, and p divides $\ell + 1$, the module E_p is an irreducible I_ℓ-module, where I_ℓ denotes the inertia group at ℓ.*

These assumptions are made mainly to simplify the arguments and could probably be relaxed at the cost of complicating the proofs. (See Remark 1 after the statement of Assumption 6 in the introduction of [BD2].) The next set of assumptions, which does not appear in [BD2], is imposed on us by our lack of understanding of the local condition to impose at p in defining the appropriate Selmer group when p is a supersingular prime and p is inert in K.

Assumptions 1.7.

1. *The prime p is split in K, so that it can be written $p = \mathfrak{p}\bar{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime of K.*
2. *The prime $\mathfrak{p}$ is totally ramified in the anticyclotomic $\mathbb{Z}_p$-extension attached to K.*

Assumption 2 is automatically satisfied if p does not divide the class number of K. It would be desirable to be able to dispense with assumption 1 and treat the inert primes on the same footing as the split primes, as is done in [BD2] when p is ordinary.

Acknowledgements: The authors are grateful to the anonymous referee for a careful proofreading which led to corrections of some inaccuracies and to significant improvements in the presentation. Both authors were supported by grants from NSERC. The first author was supported by a James McGill Chair, and the second by a Canada Research Chair, while this research was conducted.

2 The plus/minus p-adic L-functions

2.1 Modular forms on quaternion algebras

Let N^+ and N^- be positive integers such that N^+ is divisible only by primes which are split in K and N^- by primes which are inert in K. Assume that N^- is square-free, and has an odd number of prime factors. Let p be a prime which does not divide $N_0 := N^+N^-$.

Let B be the definite quaternion algebra of discriminant $N^-\infty$, and let R be an Eichler $\mathbb{Z}[\frac{1}{p}]$-order of conductor N^+ in B. Since p does not divide N^-, we may fix an isomorphism

$$\iota : B_p := B \otimes \mathbb{Q}_p \longrightarrow M_2(\mathbb{Q}_p).$$

Let $R_1^\times$ denote the group of elements of reduced norm one in R, and define

$$\Gamma = \iota(R^\times) \subset \mathbf{GL}_2(\mathbb{Q}_p).$$

Let $\mathcal{T}$ denote the Bruhat-Tits tree attached to $\mathbf{PGL}_2(\mathbb{Q}_p)$, whose set $\mathcal{V}(\mathcal{T})$ of vertices is in bijection with the similarity classes of $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^2$, two vertices being joined by an edge if the corresponding classes of lattices admit representatives in which one contains the other with index p. The group $\mathbf{GL}_2(\mathbb{Q}_p)$ (and hence, in particular, Γ) acts naturally on $\mathcal{T}$ and the quotient of $\mathcal{T}$ by the action of Γ is a finite graph.

Definition 2.1. A modular form of weight 2 on $\mathcal{V}(\mathcal{T})$ for Γ is a Γ-invariant $\mathbb{Z}_p$-valued function on $\mathcal{V}(\mathcal{T})$.

Denote by $S_2(\mathcal{V}/\Gamma)$ the space of all such forms; it is a finitely generated $\mathbb{Z}_p$-module equipped with a natural action of the Hecke operators T_ℓ (with $\ell \not| N$) described as in [BD2], Section 1.1. Furthermore, it admits a natural $\mathbb{Z}$-structure $S_2(\mathcal{V}/\Gamma)^{\mathbb{Z}}$ consisting of the $\mathbb{Z}$-valued functions in $S_2(\mathcal{V}/\Gamma)$, which is preserved by the action of the Hecke operators.

Let $f_E \in S_2(\Gamma_0(N_0))^{\mathrm{new}}$ be the eigenform of weight two corresponding to E. For each prime ℓ not dividing N we have

$$T_\ell(f_E) = a_\ell(E) f_E,$$

where T_ℓ denotes the Hecke operator acting on the space of classical cusp forms on $\Gamma_0(N_0)$.

Theorem 2.2 (Jacquet-Langlands). *There is an eigenform $f \in S_2(\mathcal{V}/\Gamma)^{\mathbb{Z}}$ with the same Hecke eigenvalues as those attached to f_E, i.e., such that*

$$T_\ell(f) = a_\ell(E) f, \quad \text{for all } \ell \not| N.$$

This form is unique up to multiplication by a non-zero scalar.

In addition, the function f satisfies the following property:

Proposition 2.3. *For all $v \in \mathcal{V}(\mathcal{T})$,*

$$\sum_{v' \leftrightarrow v} f(v') = a_p(E) f(v),$$

where the sum is taken over the $p+1$ vertices v' adjacent to v.

Proof. This follows directly from the description of the action of the Hecke operator T_p on $S_2(\mathcal{V}/\Gamma)$:

$$(T_p f)(v) = \sum_{v' \leftrightarrow v} f(v'),$$

and the fact that f is an eigenvector for T_p with associated eigenvalue $a_p(E)$. □

We normalize the form f so that it is not divisible by any integer in $S_2(\mathcal{V}/\Gamma)^{\mathbb{Z}}$. This makes f well-defined up to a sign. As shall be seen in the next section, the p-adic L-function attached to E and K is defined directly in terms of f rather than in terms of the classical cusp form f_E.

2.2 Rankin L-functions

The goal of this section is to define a p-adic L-function attached to a modular form $f \in S_2(\mathcal{V}/\Gamma)$ satisfying $a_p(f) = 0$ and to a quadratic subfield $K \subset B$, by combining the construction described in Section 1.2. of [BD2] with the ideas of Pollack [Po1].

Suppose for simplicity that the discriminant of K is prime to N. Let $\mathcal{O}_K$ denote the ring of integers of K and let $\mathcal{O} := \mathcal{O}_K[1/p]$ denote its ring of $\{p\}$-integers. For the sake of concreteness, we present the construction under the further assumption that the class number of $\mathcal{O}_K[1/p]$ is equal to 1. The reader may, if she wishes, adapt the construction to general class number by following the approach described in Section 1.2 of [BD2]. The advantage of the class number one assumption is that it allows for a different, more concrete and geometric—purely p-adic, instead of adelic—presentation of Section 1.2 of [BD2], enabling the authors to avoid what would otherwise be a somewhat tedious repetition of the constructions in that section.

Let n be fixed integer, and let f be an eigenform in $S_2(\mathcal{V}/\Gamma)$ satisfying $a_p(f) \equiv 0 \pmod{p^n}$. Let

$$\Psi : K \longrightarrow B$$

be an embedding of algebras, satisfying

$$\Psi(K) \cap R := \Psi(\mathcal{O}).$$

Such an embedding exists if and only if all the primes dividing N^+ are split in K, while those dividing N^- are inert in K. It is then unique, up to conjugation by the action of $R^\times$, thanks to the class number one assumption. Let $K_p := K \otimes \mathbb{Q}_p$ be the p-adic completion of K. The embedding Ψ induces an action of the p-adic group $\Pi_\infty := K_p^\times/\mathbb{Q}_p^\times$ on $\mathcal{T}$ by isometries by setting

$$g \star x := \iota\Psi(g)(x), \tag{1}$$

for any $g \in K_p^\times$ and x any vertex or edge of $\mathcal{T}$. We begin by defining certain partial p-adic L-functions attached to Ψ, by studying this action. It is somewhat clearer to separate the study into two cases:

Case 1: Suppose p is split in K. The choice of a prime $\mathfrak{p}$ of K above p induces a homomorphism

$$| \ |_p : K_p^\times/\mathbb{Q}_p^\times \longrightarrow \mathbb{Z}$$

defined by

$$|\alpha|_p := \mathrm{ord}_{\mathfrak{p}}(\alpha/\bar{\alpha}).$$

Note that replacing $\mathfrak{p}$ by $\bar{\mathfrak{p}}$ only changes the resulting homomorphism $| \ |_p$ by a sign, so that the abuse of notation inherent in the notation $| \ |_p$ is not serious. The kernel of $| \ \ |_p$ is the maximal compact subgroup of Π_∞, denoted U_0. This group is identified with $\mathbb{Z}_p^\times$ under the map which sends α to $\alpha/\bar{\alpha}$. Let

$$\ldots \subset U_n \subset \ldots \subset U_1 \subset U_0 \tag{2}$$

be the the natural decreasing filtration of the group U_0 by subgroups in which the index of U_n is $(p-1)p^{n-1}$. In the action of Π_∞ on $\mathcal{T}$ of (1), the maximal compact subgroup U_0 fixes a sequence (infinite in both directions) of consecutive vertices, i.e., a geodesic $J = J_\Psi$ of $\mathcal{T}$. The quotient $\Pi_\infty/U_0 \cong \mathbb{Z}$ acts by translation on this geodesic.

The distance between a vertex v of $\mathcal{T}$ and the geodesic J_Ψ is defined to be the shortest distance between v and a vertex of J_Ψ. If the distance from v to J_Ψ is equal to n, then the stabilizer of v in Π_∞ is exactly U_n, and the quotient Π_∞/U_n acts simply transitively on the set of vertices at distance n from J_Ψ.

Now let us fix a sequence of consecutive vertices $v_0, v_1, v_2, \ldots$ such that v_n is at distance n from $J = J_\Psi$. (See Figure 1 for an illustration in the case where $p = 2$.)

We define a sequence of functions

$$f_{K,n} : \Pi_\infty/U_n \longrightarrow \mathbb{Z}_p, \quad \text{by the rule } f_{K,n}(\alpha) = f(\alpha \star v_n).$$

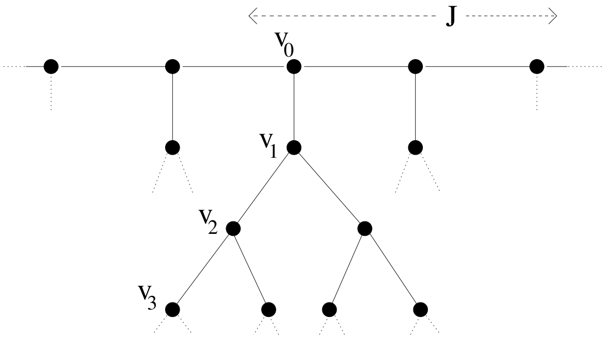

Figure 1: Action of $K_p^\times$ on $\mathcal{T}$ when p is split.

Let u_p be a fundamental p-unit of K, i.e., a generator of the group of elements in $\mathcal{O}_K[1/p]^\times$ of norm one, modulo torsion. The quotient

$$\tilde{G}_\infty = \Pi_\infty / u_p^{\mathbb{Z}}$$

is a compact p-adic group. By abuse of notation, the groups U_j occurring in the filtration (2) and their natural images in $\tilde{G}_\infty$ will be denoted by the same symbol.

Lemma 2.4. *The functions $f_{K,n}$ are invariant under translation by u_p, and hence descend to functions on $\tilde{G}_\infty/U_n$.*

Proof. Note that

$$f_{K,n}(u_p\alpha) = f((u_p\alpha)\star v_n) = f(\iota\Psi(u_p)(\alpha\star v_n)),$$

and that $\iota\Psi(u_p)$ belongs to Γ. The result therefore follows from the invariance of f under translation by elements of Γ. □

Thanks to Lemma 2.4, the functions $f_{K,n}$ defined above can be viewed as functions on the finite quotients $\tilde{G}_\infty/U_n$.

Case 2: Suppose now that p is inert in K. This case is somewhat simpler, because $\Pi_\infty = K_p^\times/\mathbb{Q}_p^\times$ is already compact, and is equal, therefore, to its maximal compact subgroup U_0. This group is identified with the group of elements in $\mathcal{O}_K \otimes \mathbb{Z}_p$ of norm one under the map which sends α to $\alpha/\bar{\alpha}$. Let

$$\ldots \subset U_n \subset \ldots \subset U_1 \subset U_0 = \Pi_\infty \qquad (3)$$

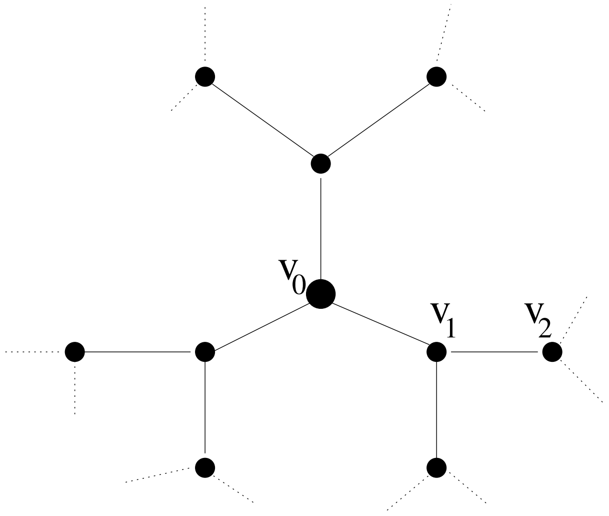

Figure 2: Action of $K_p^\times$ on $\mathcal{T}$ when p is inert.

be the the natural decreasing filtration of the group U_0 by subgroups of index $(p+1)p^{n-1}$. The group $\tilde{G}_\infty$ fixes a distinguished vertex v_0. If the distance from a vertex v to v_0 is equal to n, then the stabilizer of v in $\tilde{G}_\infty$ is exactly U_n, and the quotient $\tilde{G}_\infty/U_n$ acts simply transitively on the set of vertices at distance n from v_0.

Fix a sequence of consecutive vertices $v_0, v_1, v_2, \ldots$ such that v_n is at distance n from v_0. (See Figure 2).

We then define a sequence of functions

$$f_{K,n} : \tilde{G}_\infty/U_n \longrightarrow \mathbb{Z}_p, \quad \text{by the rule } f_{K,n}(\alpha) = f(\alpha \star v_n).$$

In conclusion, in both the cases where p is split or inert in K, we have associated to f and Ψ a sequence of functions

$$f_{K,n} : \tilde{G}_n \longrightarrow \mathbb{Z}_p, \qquad \text{where} \qquad \tilde{G}_n := \tilde{G}_\infty/U_n.$$

We associate to these functions a sequence of elements $\tilde{\mathcal{L}}_n \in \mathbb{Z}_p[\tilde{G}_n]$ by setting:

$$\tilde{\mathcal{L}}_n := \sum_{\sigma \in \tilde{G}_n} f_{K,n}(\sigma)\sigma^{-1} \in \mathbb{Z}_p[\tilde{G}_n].$$

Remark 2.5. The assumption that the class number of $\mathcal{O}$ is equal to 1 can readily be disposed of following the treatment given in Section 1.2 of [BD2].

The definitions given there would yield a sequence $\tilde{\mathcal{L}}_n$ as above, belonging to the finite group rings $\mathbb{Z}_p[\tilde{G}_n]$, where now $\tilde{G}_\infty$ denotes the group

$$\tilde{G}_\infty := (K \otimes \hat{Z})^\times / \left((\mathbb{Q} \otimes \hat{Z})^\times \prod_{\ell \neq p} (\mathcal{O} \otimes \mathbb{Z}_\ell)^\times K^\times \right),$$

which is identified with the Galois group over K of the union of all ring class fields of K of p-power conductor, an extension which contains the Hilbert class field of K.

Denote by

$$\pi_{n+1,n} : \mathbb{Z}_p[\tilde{G}_{n+1}] \longrightarrow \mathbb{Z}_p[\tilde{G}_n]$$

the ring homomorphism induced by the natural projection $\tilde{G}_{n+1} \longrightarrow \tilde{G}_n$. Occasionally we will abuse notation and view $\tilde{\mathcal{L}}_n$ as an element of $\mathbb{Z}_p[\tilde{G}_{n+1}]$ by replacing it by an arbitrary lift to this ring under the homomorphism $\pi_{n+1,n}$. Of course this element is not well-defined, but the product

$$\tilde{\xi}_n \tilde{\mathcal{L}}_n \in \mathbb{Z}_p[\tilde{G}_{n+1}]$$

is well-defined, where

$$\tilde{\xi}_n = \sum_{s \in U_n/U_{n+1}} s.$$

Lemma 2.6. *The elements $\tilde{\mathcal{L}}_n$ satisfy the following compatibility relations under the projections $\pi_{n+1,n}$:*

$$\pi_{n+1,n}(\tilde{\mathcal{L}}_{n+1}) = a_p(E)\tilde{\mathcal{L}}_n - \xi_{n-1}\tilde{\mathcal{L}}_{n-1}.$$

In particular, if p is supersingular for E so that $a_p(E) = 0$,

$$\pi_{n+1,n}(\tilde{\mathcal{L}}_{n+1}) = -\tilde{\xi}_{n-1}\tilde{\mathcal{L}}_{n-1}, \text{ for all } n \geq 1.$$

Proof. If g_n is any element of $\tilde{G}_n$, let g_{n+1} denote an arbitrary lift of this element to $\tilde{G}_{n+1}$. A direct calculation shows that

$$\pi_{n+1,n}(\tilde{\mathcal{L}}_{n+1}) = \sum_{g_n \in \tilde{G}_n} \left(\sum_{s \in U_n/U_{n+1}} f_{K,n+1}(s g_{n+1}) \right) g_n^{-1}. \qquad (4)$$

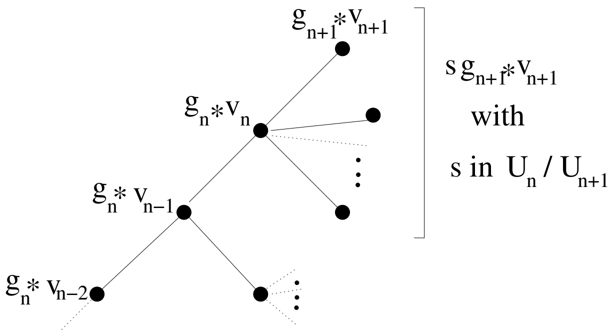

Figure 3: The inner sum

On the other hand,

$$\sum_{s \in U_n/U_{n+1}} f_{K,n+1}(sg_{n+1}) = \sum_{s \in U_n/U_{n+1}} f((sg_{n+1}) \star v_{n+1}). \qquad (5)$$

The sum on the right corresponds to summing the function f over the p vertices which are adjacent to the vertex $g_n \star v_n$ and are different from $g_n \star v_{n-1}$ (see figure 3).

It follows from proposition 2.3 satisfied by f that

$$\begin{aligned} \sum_{s \in U_n/U_{n+1}} f((sg_{n+1}) \star v_{n+1}) &= a_p(E) f(g_n \star v_n) - f(g_n \star v_{n-1}) & (6) \\ &= a_p(E) f_{K,n}(g_n) - f_{K,n-1}(g_n). & (7) \end{aligned}$$

The lemma follows by combining (4), (5), and (7). □

We may write

$$\tilde{G}_\infty = \Delta \times G_\infty,$$

where Δ is the torsion subgroup of $\tilde{G}_\infty$ and G_∞ is its maximal torsion-free quotient, which is topologically isomorphic to $\mathbb{Z}_p$. The image of Δ in $\tilde{G}_n$ is identified with Δ, and the group G_∞ can be written as

$$G_\infty = \lim_{\leftarrow} G_n, \qquad \text{where } G_n := \tilde{G}_{n+1}/\Delta \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

Let $\pi : \mathbb{Z}_p[\tilde{G}_{n+1}] \longrightarrow \mathbb{Z}_p[G_n]$ be the natural homomorphism induced by the projection $\tilde{G}_{n+1} \longrightarrow G_n$. Then for each $n \geq 0$, we set:

$$\mathcal{L}_n := \pi(\tilde{\mathcal{L}}_{n+1}).$$

By abuse of notation, denote again by

$$\pi_{n+1,n} : \mathbb{Z}_p[G_{n+1}] \longrightarrow \mathbb{Z}_p[G_n]$$

the maps induced by the natural group homomorphisms. The elements $\mathcal{L}_n$ inherit from the $\tilde{\mathcal{L}}_n$ the compatibility properties of Lemma 2.6 under these maps, i.e., when p is supersingular:

$$\pi_{n+1,n}(\mathcal{L}_{n+1}) = -\xi_n \mathcal{L}_{n-1}, \qquad \text{for all } n \geq 1. \tag{8}$$

Here $\xi_n := \pi(\tilde{\xi}_{n+1})$ is the element of $\mathbb{Z}_p[G_n]$ given by $\xi_n = \sum_{\sigma \in H_n} \sigma$, where $H_n = \ker(G_n \longrightarrow G_{n-1})$.

Let us fix a topological generator

$$\gamma \in \lim_{\leftarrow} G_n \cong \mathbb{Z}_p.$$

This determines the identification sending γ to $1+T$

$$\Lambda = \lim_{\leftarrow} \mathbb{Z}_p[G_n] \cong \mathbb{Z}_p[\![T]\!].$$

In this way $\mathbb{Z}_p[G_n]$ is identified with $\mathbb{Z}_p[T]/\omega_n \mathbb{Z}_p[T]$, where $\omega_n = (T+1)^{p^n} - 1$, and the element ξ_n is identified with the p^n-power cyclotomic polynomial in $T+1$. (In other words, the roots of $\xi_n(T)$ are of the form $\zeta - 1$, where ζ ranges over all primitive p^n-th roots of unity.) Note that we have

$$\omega_n(T) = T \prod_{j=1}^{n} \xi_j(T).$$

Let us also write

$$\tilde{\omega}_n^+(T) := \prod_{\substack{j=2 \\ j \text{ even}}}^{n} \xi_j(T), \quad \tilde{\omega}_n^-(T) := \prod_{\substack{j=1 \\ j \text{ odd}}}^{n} \xi_j(T),$$

and set $\omega_n^{\pm}(T) = T\tilde{\omega}_n^{\pm}(T)$.
The following technical lemma is straightforward to derive, but we note it for better reference.

Lemma 2.7. *Let n be a positive integer and ϵ denote the sign of $(-1)^n$.*

1. *Multiplication by $\tilde{\omega}_n^{-\epsilon}$ induces a natural isomorphism*
$$\Lambda/(\omega_n^{\epsilon}) \longrightarrow \tilde{\omega}_n^{-\epsilon}\Lambda/(\omega_n).$$
2. *For all $r \geq 1$, multiplication by $\tilde{\omega}_n^{-\epsilon}$ induces a natural isomorphism*
$$\Lambda/(\omega_n^{\epsilon}, p^r) \longrightarrow \tilde{\omega}_n^{-\epsilon}\Lambda/(\omega_n, p^r).$$
3. *If X is a free $\Lambda_{r,n} := \Lambda/(\omega_n, p^r)$-module and $x \in X$ is annihilated by ω_n^{ϵ}, then there is a unique $y \in X/\omega_n^{\epsilon}X$ such that $x = \tilde{\omega}_n^{-\epsilon}y$.*

The following proposition is key in the construction of the plus and minus p-adic L-functions.

Proposition 2.8. *Let ϵ denote the sign of $(-1)^n$. Then*

1. $\omega_n^{\epsilon}\mathcal{L}_n = 0$
2. *There is a unique element $L_n^{\epsilon} \in \Lambda/\omega_n^{\epsilon}\Lambda$ such that $\mathcal{L}_n = \tilde{\omega}_n^{-\epsilon}L_n^{\epsilon}$.*

Proof. For the first assertion, suppose first that $n > 2$ is even. Then
$$\omega_n^{+}\mathcal{L}_n = \omega_{n-2}^{+}\xi_n\mathcal{L}_n = \omega_{n-2}^{+}\xi_n\pi_{n,n-1}(\mathcal{L}_n).$$
But by equation (8),
$$\omega_{n-2}^{+}\xi_n\pi_{n,n-1}(\mathcal{L}_n) = -\omega_{n-2}^{+}\xi_n\xi_{n-2}\mathcal{L}_{n-2}.$$
This allows the statement to be reduced by induction to the case $n = 2$. For this value of n it follows from the direct calculation
$$\omega_2^{+}\mathcal{L}_2 = T\xi_2(T)\mathcal{L}_2 = T\xi_2\pi_{2,1}(\mathcal{L}_2) = -T\xi_1\xi_2\mathcal{L}_0,$$
where the last equality follows from (8). But this expression is 0 because $T\xi_1\xi_2 = 0$ in $\mathbb{Z}_p[G_2]$. The proof when n is odd is identical. For the second (divisibility) assertion, we invoke Lemma 2.7, noting that we have $\omega_n = \omega_n^{\epsilon}\tilde{\omega}_n^{-\epsilon}$. Therefore an element of $\Lambda/\omega_n\Lambda$ annihilated by ω_n^{ϵ} is divisible by $\tilde{\omega}_n^{-\epsilon}$ and the result of the division is unique in $\Lambda/\omega_n^{\epsilon}\Lambda$. □

Let us now denote by
$$\begin{cases} \mathcal{L}_n^{+} = (-1)^{\frac{n}{2}}L_n^{+} & \text{if } n \text{ is even ;} \\ \mathcal{L}_n^{-} = (-1)^{\frac{n+1}{2}}L_n^{-} & \text{if } n \text{ is odd.} \end{cases}$$

Lemma 2.9. *The sequence* $\{\mathcal{L}_n^+\}_{n \text{ even}}$ *is compatible with respect to the natural projections*

$$\Lambda/\omega_n^+ \longrightarrow \Lambda/\omega_{n-2}^+,$$

and likewise for the sequence $\{\mathcal{L}_n^-\}_{n \text{ odd}}$.

Proof. Let us, for all $n \geq 0$, choose lifts of $\mathcal{L}_n$ and $L_n^\pm$ to Λ and denote them by the same symbols. Suppose first that $n \geq 2$ is even. Then we have

$$\mathcal{L}_n = -\xi_{n-1}\mathcal{L}_{n-2} \pmod{\omega_{n-1}}.$$

This implies that there exists $F \in \Lambda$ such that

$$\tilde{\omega}_n^- L_n^+ = -\xi_{n-1}\tilde{\omega}_{n-2}^- L_{n-2}^+ + \omega_{n-1}F.$$

Noting that $\omega_{n-1} = \omega_{n-2}^+\tilde{\omega}_n^-$, we can cancel by $\tilde{\omega}_n^- = \xi_{n-1}\tilde{\omega}_{n-2}$ to obtain

$$L_n^+ = -L_{n-2}^+ + \omega_{n-2}^+ F,$$

which proves the statement when n is even. The case where n is odd is similar. □

Thanks to this lemma we may denote by

$$\mathcal{L}_f^+ := \lim_{\leftarrow} \mathcal{L}_n^+ \in \lim_{\leftarrow} \Lambda/\omega_n^+ \cong \Lambda,$$

and define $\mathcal{L}_f^- \in \Lambda$ similarly. Let $L \mapsto L^*$ denote the involution in Λ sending every group- like element in this completed group ring to its inverse. We set

$$L_p(f,K)^\pm := \mathcal{L}_f^\pm(\mathcal{L}_f^\pm)^*,$$

following definition 1.6 of [BD2].

3 Selmer groups

Class field theory identifies $\tilde{G}_\infty$ with $\mathrm{Gal}(\tilde{K}_\infty/K)$, where $\tilde{K}_\infty$ is the union of all the ring class fields of K of p-power conductor. For each integer $m \geq 0$, the quotient $\tilde{G}_m$ is identified with $\mathrm{Gal}(\tilde{K}_m/K)$, where $\tilde{K}_m$ is the ring class field of K of conductor p^m. The subfield of $\tilde{K}_\infty$ fixed by Δ is the anticyclotomic $\mathbb{Z}_p$-extension K_∞ of K, so that

$$G_\infty = \mathrm{Gal}(K_\infty/K).$$

Under this identification, the group G_m corresponds to the Galois group $\mathrm{Gal}(K_m/K)$, where K_m is defined to be the m-th layer of the $\mathbb{Z}_p$-tower K_∞.

Following the notations of Section 2.1 of [BD2], denote by V_f the two-dimensional Galois representation attached to the modular form f (with coefficients in $\mathbb{Q}_p$) and let T_f denote a $G_{\mathbb{Q}}$ stable $\mathbb{Z}_p$-sub-lattice. The finite modules

$$T_{f,n} := T_f/p^nT_f = (V_f/T_f)[p^n] \qquad (n \geq 1)$$

fit naturally both into a projective and an inductive system, i.e., for all $r \geq n$ there are natural maps

$$T_{f,r} \twoheadrightarrow T_{f,n}, \qquad T_{f,n} \hookrightarrow T_{f,r},$$

which will be used to take both projective and injective limits of cohomology groups associated to the $T_{f,n}$.

The main goal of this section is to define certain *Selmer groups* attached to the Galois representations $T_{f,n}$, and to prove certain basic facts about their structure. For each $m \geq 0$ and $n \geq 1$, the Selmer group $\mathrm{Sel}(K_m, T_{f,n})$ is defined as a subgroup of the (continuous) Galois cohomology group $H^1(K_m, T_{f,n})$ by imposing conditions on restrictions to local decomposition groups.

More precisely, for every rational prime ℓ, let

$$K_{m,\ell} := K_m \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \oplus_{\lambda|\ell} K_{m,\lambda}, \quad H^1(K_{m,\ell}, T_{f,n}) := \oplus_{\lambda|\ell} H^1(K_{m,\lambda}, T_{f,n}).$$

There is a natural restriction map

$$res_\ell : H^1(K_m, T_{f,n}) \longrightarrow H^1(K_{m,\ell}, T_{f,n}).$$

For each rational prime ℓ we define certain *distinguished subgroups*

$$H^1_{\mathrm{fin}}(K_{m,\ell}, T_{f,n}) \subset H^1(K_{m,\ell}, T_{f,n}),$$

referred to as the *finite part* of these local cohomology groups as follows. Let A_f denote the abelian variety associated to the modular form f, as described in greater detail in Section 4. Let $V_p(A_f) := T_p(A_f) \otimes \mathbb{Q}_p$ be the p-adic Galois representation associated to A_f, and let $H^1_{\mathrm{fin}}(K_{m,\ell}, V_p(A_f))$ denote the image of $A_f(K_{m,\ell}) \otimes \mathbb{Z}_p$ in $H^1(K_{m,\ell}, V_p(A_f))$ under the Kummer map. By construction, the two-dimensional Galois representation V_f is a quotient of $V_p(A_f)$. Write

$$\pi_f : V_p(A_f) \longrightarrow V_f, \quad H^1(K_{m,\ell}, V_p(A_f)) \longrightarrow H^1(K_{m,\ell}, V_f)$$

for the associated $G_{\mathbb{Q}}$-equivariant projection, as well as for the maps induced by it on the various local cohomology groups. We define

$$H^1_{\text{fin}}(K_{m,\ell}, V_f) := \pi_f(H^1_{\text{fin}}(K_{m,\ell}, V_p(A_f))),$$

and $H^1_{\text{fin}}(K_{m,\ell}, T_f)$ as the inverse image of $H^1_{\text{fin}}(K_{m,\ell}, V_f)$ under the natural map

$$H^1(K_{m,\ell}, T_f) \longrightarrow H^1(K_{m,\ell}, V_f)$$

induced by the inclusion $T_f \hookrightarrow V_f$. Finally for every $n \geq 1$ we let $H^1_{\text{fin}}(K_{m,\ell}, T_{f,n})$ be the image of $H^1_{\text{fin}}(K_{m,\ell}, T_f)$ in $H^1(K_{m,\ell}, T_{f,n})$ under the map induced by the canonical projection $T_f \longrightarrow T_{f,n}$.

Definition 3.1. The *Selmer group* attached to K_m and $T_{f,n}$ is the group of cohomology classes $s \in H^1(K_m, T_{f,n})$ satisfying

$$\text{res}_\ell(s) \text{ belongs to } H^1_{\text{fin}}(K_{m,\ell}, T_{f,n}), \quad \text{for all } \ell.$$

It is denoted $\text{Sel}(K_m, T_{f,n})$.

We also set

$$\text{Sel}(K_\infty, T_{f,n}) := \lim_{\substack{\longrightarrow \\ m}} \text{Sel}(K_m, T_{f,n}), \quad \text{Sel}(K_\infty, T_{f,\infty}) := \lim_{\substack{\longrightarrow \\ n}} \text{Sel}(K_\infty, T_{f,n}), \tag{9}$$

where the direct limits are taken with respect to the natural maps induced by restriction and the inclusions $T_{f,n} \hookrightarrow T_{f,n'}$.

3.1 Local conditions at $\ell \neq p$

We begin by discussing the groups $H^1_{\text{fin}}(K_{m,\ell}, T_{f,n})$ in the case where $\ell \neq p$.

We define (following [BD2]) the *singular part* of the local cohomology group $H^1(K_{m,\ell}, T_{f,n})$ to be the quotient

$$H^1_{\text{sing}}(K_{m,\ell}, T_{f,n}) := \frac{H^1(K_{m,\ell}, T_{f,n})}{H^1_{\text{fin}}(K_{m,\ell}, T_{f,n})}.$$

If ℓ does not divide N, then

$$H^1_{\text{sing}}(K_{m,\ell}, T_{f,n}) = H^1(I_{m,\ell}, T_{f,n})^{G_{K_\ell}} := \prod_\lambda H^1(I_{m,\lambda}, T_{f,n})^{G_{K_\ell}},$$

where λ runs over the primes of K_m over ℓ and $I_{m,\lambda}$ is the inertia subgroup of $G_{K_{m,\lambda}}$.

Restriction defines a so-called *residue map*

$$\partial_\ell : H^1(K_{m,\ell}, T_{f,n}) \longrightarrow H^1_{\mathrm{sing}}(K_{m,\ell}, T_{f,n})$$

such that the following sequence is exact

$$0 \longrightarrow H^1_{\mathrm{fin}}(K_{m,\ell}, T_{f,n}) \longrightarrow H^1(K_{m,\ell}, T_{f,n}) \longrightarrow H^1_{\mathrm{sing}}(K_{m,\ell}, T_{f,n}).$$

The following gives a local control theorem for the Selmer group.

Lemma 3.2. *For all rational primes $\ell \neq p$, the natural map induced by restriction*

$$H^1_{\mathrm{sing}}(K_\ell, T_{f,n}) \longrightarrow H^1_{\mathrm{sing}}(K_{m,\ell}, T_{f,n})$$

is injective.

For example, when ℓ does not divide N, this follows from the fact that K_m/K is unramified at the primes above ℓ, so that any class which becomes unramified over K_m already had to be unramified over K.

The cup product in local Galois cohomology combined with the Weil pairing $T_{f,n} \times T_{f,n} \longrightarrow \mu_{p^n}$ leads to the non-degenerate *local Tate pairing*

$$H^1(K_{m,\ell}, T_{f,n}) \times H^1(K_{m,\ell}, T_{f,n}) \longrightarrow H^2(K_{m,\ell}, \mu_{p^n}) \xrightarrow{\mathrm{inv}_\ell} \mathbb{Z}/p^n\mathbb{Z},$$

in which the rightmost map is given by

$$\mathrm{inv}_\ell(\kappa) := \sum_{\lambda|\ell} \mathrm{inv}_\lambda(\kappa),$$

where inv_λ is the standard identification of $H^2(K_{m,\lambda}, \mu_{p^n})$ with $\mathbb{Z}/p^n\mathbb{Z}$ given by local class field theory.

It is a standard fact that the groups $H^1_{\mathrm{fin}}(K_{m,\ell}, T_{f,n})$ are *maximal isotropic* for the local Tate pairing, and that this pairing therefore induces a perfect duality

$$H^1_{\mathrm{fin}}(K_{m,\ell}, T_{f,n}) \times H^1_{\mathrm{sing}}(K_{m,\ell}, T_{f,n}) \longrightarrow \mathbb{Z}/p^n\mathbb{Z}.$$

(Cf. Proposition 2.3 of [BD2].)

We now recall the definition of *admissible primes* given in Section 2.2 of [BD2].

Definition 3.3. A rational prime ℓ is said to *n-admissible* relative to f if it satisfies the following conditions:

1. ℓ does not divide pN;
2. ℓ is inert in $K/\mathbb{Q}$;
3. p does not divide $\ell^2 - 1$;
4. p^n divides $\ell + 1 - a_\ell$ or $\ell + 1 + a_\ell$.

One of the motivations for singling out these primes is the following freeness result for the local cohomology group $H^1(K_{m,\ell}, T_{f,n})$ when ℓ is n-admissible.

Lemma 3.4. *If ℓ is an n-admissible prime, then*

1. *The groups $H^1_{\mathrm{fin}}(K_{m,\ell}, T_{f,n})$ and $H^1_{\mathrm{sing}}(K_{m,\ell}, T_{f,n})$ are free of rank one over $\Lambda_{n,m} = \Lambda/(p^n, \omega_m)$.*
2. *The group $H^1(K_{m,\ell}, T_{f,n})$ is free of rank two over $\Lambda_{n,m}$.*

Proof. See Lemma 2.7 of [BD2]. □

An important caveat that needs to be noted is that the finite part at ℓ does not just depend on the underlying Galois representation $T_{f,n}$, but on the Galois representation V_f from which it arises. For example, if $T_{f,n}$ comes from the p-division points of an abelian variety A_f with good reduction at ℓ, then the representation $T_{f,n}$ is of course unramified, and $H^1_{\mathrm{fin}}(K_{m,\ell}, T_{f,n})$ merely consists of the *unramified* cohomology classes. This is not the case if $T_{f,n}$ is unramified but arises from an abelian variety with multiplicative reduction at ℓ. If ℓ is a prime which divides N exactly, then V_f is is an *ordinary* representation of $G_{\mathbb{Q}_\ell}$: it contains a unique one-dimensional $\mathbb{Q}_p$-vector subspace which is stable under the action of the decomposition group at ℓ. Let $T^{(\ell)}_{f,n}$ denote the corresponding rank one $(\mathbb{Z}/p^n\mathbb{Z})$-submodule of $T_{f,n}$. Then $H^1_{\mathrm{fin}}(K_{m,\ell}, T_{f,n})$ is the image in $H^1(K_{m,\ell}, T_{f,n})$ of $H^1(K_{m,\ell}, T^{(\ell)}_{f,n})$.

3.2 Local conditions at p

In the supersingular setting, the classical definition of the Selmer group $\mathrm{Sel}(K_\infty, T_{f,\infty})$ given in (9) suffers from the fact that the resulting object is not a co-torsion module over the Iwasawa algebra $\Lambda = \mathbb{Z}_p[\![G_\infty]\!]$. The idea is to cut down the size of this Selmer group by imposing *more stringent* local conditions at the primes above p.

We will follow closely Sections 4 and 6 of [IP] with some adjustments due to the fact that here we work with torsion coefficients. In order to define the appropriate subgroups of $H^1_{\mathrm{fin}}(K_{m,p}, T_{f,n})$, we need to make the following assumptions which are satisfied in our application:

Assumptions 3.5. *1. The prime p is split in K, so that it can be written $p = \mathfrak{p}\bar{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime of K.*

2. The prime $\mathfrak{p}$ is totally ramified in the anticyclotomic $\mathbb{Z}_p$-extension K_∞ attached to K.

3. The Galois representation $T_{f,n}$ is isomorphic (as a representation of $G_{\mathbb{Q}_p}$) to $E[p^n]$, where E is an elliptic curve over $\mathbb{Q}_p$ with supersingular reduction at p.

Note that this implies, in particular, that

$$a_p(f) \equiv 0 \pmod{p^n}.$$

Recall that K_m denotes the m-th layer in the anticyclotomic $\mathbb{Z}_p$-extension K_∞. Let $K_{m,p} := K_m \otimes \mathbb{Q}_p = K_{m,\mathfrak{p}} \oplus K_{m,\bar{\mathfrak{p}}}$ denote the completion of K_m at p. Let $\widehat{E}$ denote the formal group of $E_{\mathbb{Q}_p}$. First we will recall the description of

$$\widehat{E}(K_{m,p}) := \widehat{E}(K_{m,\mathfrak{p}}) \oplus \widehat{E}(K_{m,\bar{\mathfrak{p}}})$$

as a $\mathbb{Z}_p[G_m] = \Lambda_m$-module, for all $m \geq 0$.

Since the discussion in this section is purely local, we will lighten notations by letting $\{L_m\}_{m\geq 0}$ denote either of the following towers of local fields: $\{K_{m,\mathfrak{p}}\}_{m\geq 0}$ or $\{K_{m,\bar{\mathfrak{p}}}\}_{m\geq 0}$.

The following theorem is essential in defining the plus and minus Selmer groups attached to $T_{f,n}$.

Theorem 3.6. *For $m \geq 0$ there exist points $d_m \in \widehat{E}(L_m)$ such that*

1. *$Tr^m_{m-1}(d_m) = -d_{m-2}$ for all $m \geq 2$*

2. *$Tr^1_0(d_1) = ud_0$ with $u \in \mathbb{Z}_p^\times$*

3. *d_m, d_{m-1} generate $\widehat{E}(L_m)$ as a $\mathbb{Z}_p[G_m]$-module and d_0 generates $\widehat{E}(L_0)$ as a $\mathbb{Z}_p$-module.*

This theorem is proved in [IP]. (See Theorem 4.5 of [IP].)

Using the sequence of points $\{d_m\}_{m\geq 0}$ we consider two subsequences

$$d_m^+ = \begin{cases} d_m & \text{if } m \text{ is even;} \\ d_{m-1} & \text{if } m \text{ is odd;} \end{cases} \qquad d_m^- = \begin{cases} d_{m-1} & \text{if } m \geq 2 \text{ is even;} \\ d_m & \text{if } m \text{ is odd.} \end{cases}$$

Now we define $\widehat{E}^\pm(L_m) := \Lambda_m d_m^\pm \subset \widehat{E}(L_m)$.

Let us remark that the Λ_m-submodule $\widehat{E}^\pm(L_m)$ thus defined is independent of the choice of the sequence of points $\{d_m\}_{m\geq 0}$ as in Theorem 3.6. (See Lemma 4.13 of [IP].)

Let us now fix integers m, n.

Lemma 3.7. *The natural map*

$$j : \widehat{E}^\pm(L_m)/p^n\widehat{E}^\pm(L_m) \longrightarrow \widehat{E}(L_m)/p^n\widehat{E}(L_m)$$

is injective for all m, n.

Proof. We consider the case where the sign is $+$, the other case being proved in a similar way. Let $P \in \widehat{E}^+(L_m)$ be a point whose image under j is 0. Then there exists $Q \in \widehat{E}(L_m)$ such that $P = p^nQ$. Since ω_m^+ is the exact annihilator of $\widehat{E}^+(L_m)$ in $\widehat{E}(L_m)$ (cf. Proposition 4.11 of [IP]) we have

$$p^n(\omega_m^+Q) = 0,$$

and as there are no non-zero p-power torsion points in $\widehat{E}(L_M)$, we conclude that

$$\omega_m^+Q = 0.$$

Hence Q itself belongs to $\widehat{E}^+(L_m)$, which proves the lemma. □

Recall from Section 3.1 that local Tate duality induces perfect pairings

$$\langle\ ,\ \rangle_{m,n} : H^i(L_m, T_{E,n}) \times H^{2-i}(L_m, T_{E,n}) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

and

$$\langle\ ,\ \rangle_m : H^i(L_m, T_pE) \times H^{2-i}(L_m, E[p^\infty]) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

Let us define, following Section 4.3 of [IP],

$$\begin{aligned} H^1_{\mathrm{fin}\,\pm}(L_m, T_{f,n}) &:= (\widehat{E}^\pm(L_m) \otimes \mathbb{Z}/p^n\mathbb{Z}), \\ H^1_{\mathrm{fin}}(L_m, T_{f,n}) &:= (\widehat{E}(L_m) \otimes \mathbb{Z}/p^n\mathbb{Z}), \\ H^1_\pm(L_m, T_{f,n}) &:= (\widehat{E}^\pm(L_m) \otimes \mathbb{Z}/p^n\mathbb{Z})^\perp, \end{aligned}$$

where the orthogonal complement in the last definition is taken relative to the pairing $\langle\ ,\ \rangle_m$. We'll also write

$$H^1_\pm(L_m, T_{E,n}) := (\widehat{E}^\pm(L_m) \otimes \mathbb{Z}/p^n\mathbb{Z})^\perp,$$

with the orthogonal complement taken under the pairing $\langle\ ,\ \rangle_{m,n}$.

Lemma 3.8. $H^0(L_m, E[p^n]) = H^2(L_m, E[p^n]) = 0.$

Proof. This follows from Lemma 4.6 of [IP] and the non-degeneracy of the local Tate pairing. □

Lemma 3.9. *$H^1_\pm(L_m, T_{f,n})$ is a free $\mathbb{Z}/p^n\mathbb{Z}[G_m]$-module of rank 1.*

Proof. Taking the L_m-cohomology of the exact sequences

$$0 \to T_pE \xrightarrow{p^n} T_pE \longrightarrow T_{E,n} \to 0, \quad 0 \to T_{E,n} \longrightarrow E[p^\infty] \xrightarrow{p^n} E[p^\infty] \to 0$$

and using Lemma 3.8 yields the natural isomorphisms of $\mathbb{Z}/p^n\mathbb{Z}[G_m]$-modules

$$H^1(L_m, T_{E,n}) \cong H^1(L_m, T_pE)/p^n H^1(L_m, T_pE)$$

and

$$H^1(L_m, T_{E,n}) \cong H^1(L_m, E[p^\infty])[p^n].$$

The pairing $\langle\ ,\ \rangle_{m,n}$ is naturally induced from the pairing $\langle\ ,\ \rangle_m$ under these identifications. Therefore, since $\widehat{E}^\pm(L_m) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is a p-divisible group we immediately obtain

$$\begin{aligned} H^1_\pm(L_m, T_{E,n}) &\cong (\widehat{E}^\pm(L_m) \otimes \mathbb{Z}/p^n\mathbb{Z})^\perp \\ &\cong (\widehat{E}^\pm(L_m) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\perp / p^n (\widehat{E}^\pm(L_m) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\perp. \end{aligned}$$

This yields the isomorphism

$$H^1_\pm(L_m, T_{E,n}) \cong H^1_\pm(L_m, T_pE)/p^n H^1_\pm(L_m, T_pE).$$

Proposition 4.16 of [IP] implies that $H^1_\pm(L_m, T_pE)$ is a free $\mathbb{Z}_p[G_m]$-module of rank 1. Lemma 3.9 follows. □

The following result, which is a consequence of Theorem 10.1 of [GIP], shows that the subgroup $H^1_{\mathrm{fin}}(K_{m,p}, T_{f,n})$ depends only on the Galois representation $T_{f,n}$, unlike its counterpart for $\ell \neq p$ in general, so that in particular it behaves well under congruences. As [GIP] is not yet available we will sketch here the main arguments of the proof. Let $f_1, f_2 \in S_2(\mathcal{V}/\Gamma)$ and let us denote by $T_i := T_{f_i}$ and $T_{i,n} := T_{f_i,n}$ for $i = 1, 2$ and some $n \geq 1$.

Theorem 3.10. *Suppose that the $G_{\mathbb{Q}_p}$-representations T_1 and T_2 are congruent modulo p^n, i.e. we have an isomorphism*

$$\iota : T_{1,n} \cong T_{2,n}$$

as $\mathbb{Z}/p^n\mathbb{Z}[G_{\mathbb{Q}_p}]$-modules. We'll further assume that Assumptions 3.5 hold for $T_{1,n}$ (and consequently also for $T_{2,n}$) and that L is one of the local fields $K_{m,\mathfrak{p}}$ or $K_{m,\bar{\mathfrak{p}}}$ for some $m \geq 0$. Then ι induces a natural isomorphism

$$g_L : H^1_{\mathrm{fin}}(L, T_{1,n}) \longrightarrow H^1_{\mathrm{fin}}(L, T_{2,n}).$$

Proof. First we have natural isomorphisms and inclusions

$$H^1_{\mathrm{fin}}(L, T_i)/p^n H^1_{\mathrm{fin}}(L, T_i) \cong H^1_{\mathrm{fin}}(L, T_{i,n}) \hookrightarrow H^1(L, T_{i,n}), \qquad \text{for } i = 1, 2$$

as a consequence of the assumptions and lemma 3.8. Therefore the conclusion of the theorem makes sense.
Second, given the totally ramified extension $L/\mathbb{Q}_p$ we perform (see [Fa] and [Br]) the following construction. Let π be a uniformizer of L and let

$$E(u) = u^e + a_1 u^{e-1} + ... + a_e \in \mathbb{Z}_p[u]$$

be the minimal polynomial of π over $\mathbb{Z}_p$. Let S denote the p-adic completion of the $\mathbb{Z}_p$-algebra $\mathbb{Z}_p[u, u^{ie}/i!]_{i \in \mathbb{N}} \subset \mathbb{Q}_p[u]$. It has the following structure:

1. a continuous $\mathbb{Z}_p$-linear Frobenius $\sigma : S \longrightarrow S$ such that $\sigma(u) = u^p$;

2. a natural continuous derivation $d : S \longrightarrow \Omega_{S/\mathbb{Z}_p}$;

3. a decreasing filtration $(\mathrm{Fil}^i S)_{i \in \mathbb{N}}$, where $\mathrm{Fil}^i S$ is the p-adic completion of $\sum_{j \geq i} (E(u)^j/j!)S$. (One checks that $\mathrm{Fil}^i S$ is an ideal of S.)

Let us consider the Galois representations T_1, T_2 as above, denote by D_1, D_2 the strongly divisible lattices attached to T_1, T_2 respectively as in [FL] and set $M_i := D_i \otimes_{\mathbb{Z}_p} S$, for $i = 1, 2$. Let finally M be any one of the S-modules M_1, M_2, M_1/p^nM_1, or M_2/p^nM_2. Then M is endowed with the following structure:

1. a one step filtration $M_0 \subset M$;
2. σ-linear Frobenii $\varphi : M \to M$ and $\varphi_0 : M_0 \to M$ such that $\varphi|_{M_0} = p\varphi_0$;
3. a connection (nilpotent modulo p) $\nabla : M \longrightarrow M \otimes_S \Omega_{S/\mathbb{Z}_p}$ such that $\nabla \circ \varphi_0 = (\varphi/p) \circ \nabla|_{M_0}$.

Given M as above we define the double complex of $\mathbb{Z}_p$-modules

$$C^{\bullet,\bullet}(M) : \quad \begin{tikzcd} M_0 \arrow[r, "\nabla"] \arrow[d, "\alpha"'] & M \otimes_S \Omega_{S/\mathbb{Z}_p} \arrow[d, "\beta"] \\ M \arrow[r, "\nabla"] & M \otimes_S \Omega_{S/\mathbb{Z}_p}, \end{tikzcd}$$

where $\alpha = \varphi_0 - 1$ and $\beta = -(1 - \varphi/p)$. Let us write

$$H^n(M) := H^n(C^{\bullet,\bullet}(M)), \qquad \text{for } n \geq 0.$$

Then under the conditions of the theorem one can prove (for the details see [GIP]) that $H^2(M) = 0$ and that there is a canonical and functorial isomorphism

$$H^1(M_i) \cong H^1_{\text{fin}}(L, T_i) \text{ for } i = 1, 2.$$

From the exact sequences

$$0 \longrightarrow T_i \xrightarrow{p^n} T_i \longrightarrow T_{i,n} \longrightarrow 0$$

for $i = 1, 2$ we deduce the isomorphisms:

$$H^1(M_i/p^nM_i) \cong H^1_{\text{fin}}(L, T_i)/p^nH^1_{\text{fin}}(L, T_i) \cong H^1_{\text{fin}}(T_{i,n}).$$

The fact that $T_{1,n}$ and $T_{2,n}$ are isomorphic implies that the same is true for M_1/p^nM_1 and M_2/p^nM_2. The result follows. □

We can use Theorem 3.10 to meaningfully define the restricted local conditions at p for f. Namely, assume that the Assumptions 3.5 hold. In particular T_f is congruent to T_pE modulo p^n so we define $H^{1,\pm}_{\mathrm{fin}}(K_{m,p}, T_{f,n})$ to be the image of $\widehat{E}^{\pm}(K_{m,p})/p^n\widehat{E}^{\pm}(K_{m,p})$ under the composition

$$\widehat{E}(K_{m,p})/p^n\widehat{E}(K_{m,p}) \cong H^1_{\mathrm{fin}}(K_{m,p}, T_{E,n}) \cong H^1_{\mathrm{fin}}(K_{m,p}, T_{f,n})$$

where the first isomorphism is the Kummer map and the second is provided by Theorem 3.10 via local duality. We also define the group $H^1_{\pm}(K_{m,p}, T_{f,n})$ to be the orthogonal complement of $H^{1,\pm}_{\mathrm{fin}}(K_{m,p}, T_{f,n})$ under local duality. Clearly this group is the image of $H^1_{\pm}(K_{m,p}, T_{E,n})$ under the isomorphism $H^1(K_{m,p}, T_{E,n}) \cong H^1(K_{m,p}, T_{f,n})$ induced by ι.

We recall that $\Lambda_{n,m} := \mathbb{Z}/p^n\mathbb{Z}[G_m] = \Lambda_m/p^n$ denotes the group ring of G_m with mod p^n coefficients. From the previous discussion, we have

Corollary 3.11. *The local cohomology groups $H^1_{\pm}(K_{m,p}, T_{f,n})$ are free $\Lambda_{n,m}$-modules of rank two.*

Proof. Since $p = \mathfrak{p}\bar{\mathfrak{p}}$, we have

$$H^1_{\pm}(K_{m,p}, T_{f,n}) = H^1_{\pm}(K_{m,\mathfrak{p}}, T_{f,n}) \oplus H^1_{\pm}(K_{m,\bar{\mathfrak{p}}}, T_{f,n}).$$

But each of the summands on the right is a free $\Lambda_{n,m}$-module, by Lemma 3.9. The result follows. □

3.3 Generalised Selmer groups

We are now in a position to define more general Selmer groups that will play a key role in our argument. We retain the notations and assumptions of earlier sections; in particular Assumption 3.5 of Section 3.2.

Let

$$\Gamma_m = \mathrm{Gal}(K_\infty/K_m), \qquad \text{so that } G_m = \Gamma/\Gamma_m.$$

If s belongs to $H^1(K_m, T_{f,n})$ and ℓ is a rational prime we denote by $s_\ell := \mathrm{res}_\ell(s)$ the image of s in $H^1(K_{m,\ell}, T_{f,n})$ under restriction.

Definition 3.12. Let m and n be non-negative integers. The *unrestricted Selmer group* attached to f, n, and K_m, denoted $\mathrm{Sel}_{\Box}(K_m, T_{f,n})$, is the group of classes $s \in H^1(K_m, T_{f,n})$ satisfying

$$s_\ell \in H^1_{\mathrm{fin}}(K_{m,\ell}, T_{f,n}) \text{ for all } \ell \neq p.$$

The subgroups

$$\mathrm{Sel}_0(K_m, T_{f,n}) \subset \mathrm{Sel}_{\pm}(K_m, T_{f,n}) \subset \mathrm{Sel}(K_m, T_{f,n}) \subset \mathrm{Sel}_{\Box}(K_m, T_{f,n})$$

are defined by the additional conditions:

1. $s \in \mathrm{Sel}_0(K_m, T_{f,n})$ if $s_p = 0$;

2. $s \in \mathrm{Sel}_{\pm}(K_m, T_{f,n})$ if $s_p \in H^1_{\mathrm{fin}\,\pm}(K_{m,p}, T_{f,n})$;

3. $s \in \mathrm{Sel}(K_m, T_{f,n})$ if $s_p \in H^1_{\mathrm{fin}}(K_{m,p}, T_{f,n})$.

We also define

$$\begin{aligned}\mathrm{Sel}_{\sharp}(K_\infty, T_{f,n}) &:= \lim_{\rightarrow, m} \mathrm{Sel}_{\sharp}(K_m, T_{f,n}),\\ \mathrm{Sel}_{\sharp}(K_\infty, T_{f,\infty}) &:= \lim_{\rightarrow, n} \mathrm{Sel}_{\sharp}(K_\infty, T_{f,n}),\end{aligned}$$

where the transition maps for the inductive limit are restrictions and the inclusions $T_{f,n} \hookrightarrow T_{f,n'}$, and $\sharp$ is either 0, $\pm$, or $\Box$.

Let S be a square-free integer prime to N.

Definition 3.13. The *generalized Selmer group* $\mathrm{Sel}_{S,\sharp}(K_m, T_{f,n})$ is the set of classes in $\mathrm{Sel}_{\sharp}(K_m, T_{f,n})$ satisfying

$$s_\ell = 0 \quad \text{for all } \ell | S.$$

Definition 3.14. Let $\sharp = 0, \mathrm{fin}, \pm$, or $\Box$. The *dual Selmer group* attached to f, n, K_m, S and $\sharp$ is defined to be the subgroup $H^1_{S,\sharp}(K_m, T_{f,n})$ of classes $\kappa \in H^1(K_m, T_{f,n})$ satisfying

1. $\kappa_\ell \in H^1_{\mathrm{fin}}(K_{m,\ell}, T_{f,n})$ for all rational primes ℓ not dividing pS;

2. κ_p belongs to $H^1_{\sharp}(K_{m,p}, T_{f,n})$ if $\sharp \in \{\mathrm{fin}, \pm\}$, and $\kappa_p = 0$ if $\sharp = 0$;

3. κ_ℓ is arbitrary if $\ell | S$.

Note the sequence of inclusions

$$H^1_{S,0}(K_m, T_{f,n}) \subset H^1_{S,\mathrm{fin}}(K_m, T_{f,n}) \subset H^1_{S,\pm}(K_m, T_{f,n}) \subset H^1_{S,\Box}(K_m, T_{f,n}).$$

As in [BD2], denote by

$$\widehat{H}^1(K_\infty, T_{f,n}) = \lim_{\leftarrow, m} H^1(K_m, T_{f,n}),$$

where the transition maps are co-restrictions. Similar conventions are adopted in defining $\widehat{H}^1(K_{\infty,p}, T_{f,n})$.

Both $\mathrm{Sel}_{S,\sharp}(K_m, T_{f,n})$ and $H^1_{S,\sharp}(K_m, T_{f,n})$ are special cases of the general notion of an *abstract Selmer group*: a subgroup of the global cohomology group $H^1(K_m, T_{f,n})$ defined by local conditions which agree with the unramified classes, for all but finitely many primes of K_m. The following pairs are *dual Selmer groups* in the sense that the local conditions defining them are orthogonal to each other under the local Tate pairings:

$$\begin{array}{rcl} \mathrm{Sel}_{S,0}(K_m, T_{f,n}) & \text{and} & H^1_{S,\square}(K_m, T_{f,n}); \\ \mathrm{Sel}_{S,\pm}(K_m, T_{f,n}) & \text{and} & H^1_{S,\pm}(K_m, T_{f,n}); \\ \mathrm{Sel}_{S}(K_m, T_{f,n}) & \text{and} & H^1_{S,\mathrm{fin}}(K_m, T_{f,n}); \\ \mathrm{Sel}_{S,\square}(K_m, T_{f,n}) & \text{and} & H^1_{S,0}(K_m, T_{f,n}). \end{array}$$

Finally we define

$$\widehat{H}^1_{S,\sharp}(K_\infty, T_{f,n}) := \lim_{\leftarrow, m} H^1_{S,\sharp}(K_m, T_{f,n}),$$

where the transition maps are co-restrictions.

3.4 Freeness results for Selmer groups

The Euler system of this section is constructed (just like the Euler system of [BD2]) from a system of Heegner points on a collection of Shimura curves indexed by certain admissible primes ℓ. The main new difficulty arising in the supersingular setting is that the classes manufactured directly from these Heegner points are not compatible under norms (co-restriction). To obtain a norm-compatible family of cohomology classes it is necessary to divide the classes obtained "directly" from Heegner points by certain products of p-power cyclotomic polynomials, a process which mirrors the division performed in the construction of the p-adic L-function in Section 2 following [Po1]. In order to show that this division can be performed, a number of results concerning the structure of generalized Selmer groups as modules over the group rings $\Lambda_{n,m}$ are required.

Let ℓ be an n-admissible prime. Note (cf. the discussion preceding Theorem 4.1 of [BD2]) the *canonical* direct sum decomposition:

$$\widehat{H}^1(K_{\ell,\infty}, T) = \widehat{H}^1_{\mathrm{fin}}(K_{\ell,\infty}, T) \oplus \widehat{H}^1_{\mathrm{sing}}(K_{\ell,\infty}, T).$$

Denote (as in [BD2]) by v_ℓ and ∂_ℓ the projections onto the first and second factors. We recall the following proposition from [BD2] that makes it possible to produce many n-admissible primes.

Proposition 3.15. *Let s be any nonzero element of $H^1(K, T_{f,1})$. There exist infinitely many n-admissible primes ℓ relative to f such that $\partial_\ell(s) = 0$ and $v_\ell(s) \neq 0$.*

Proof. This is Theorem 3.2 of [BD2], whose proof relies on a careful application of the Chebotarev density theorem, and makes no use of the local properties of $T_{f,1}$ at p, so that it applies equally well to the supersingular case. □

Adopting the terminology of Definition 2.22 of [BD1], we make the following definition.

Definition 3.16. A square-free product S of n-admissible primes is said to be *n-admissible* if the natural map

$$\mathrm{Sel}_\square(K, T_{f,n}) \longrightarrow \oplus_{\ell|S} H^1_{\mathrm{fin}}(K_\ell, T_{f,n})$$

is injective.

Note that, if S is n-admissible, then

$$\mathrm{Sel}_{S,\square}(K, T_{f,n}) = 0. \tag{10}$$

Recall that $\Lambda_{n,m} = \mathbb{Z}/p^n\mathbb{Z}[G_m] = \Lambda/(\omega_m, p^n)\Lambda$ is the group ring at level m with $\mathbb{Z}/p^n\mathbb{Z}$ coefficients. Let I be the augmentation ideal of $\Lambda_{n,m}$ and denote by $\mathfrak{m} = \langle p, I\rangle$ the maximal ideal of this local ring. We begin by noting the following "control theorems" for the Selmer groups that have been introduced:

Lemma 3.17. *If S is an n-admissible set, then the natural maps induced by restriction and the inclusion $T_{f,1} \longrightarrow T_{f,n}$*

$$\begin{array}{rcl} \mathrm{Sel}_{S,\square}(K, T_{f,1}) & \longrightarrow & \mathrm{Sel}_{S,\square}(K_m, T_{f,n})[\mathfrak{m}], \\ H^1_{S,0}(K, T_{f,1}) & \longrightarrow & H^1_{S,0}(K_m, T_{f,n})[\mathfrak{m}] \end{array}$$

are isomorphisms.

Proof. Consider the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_{S,\Box}(K, T_{f,n}) \arrow[r] \arrow[d] & H^1(K, T_{f,n}) \arrow[r] \arrow[d] & \Omega_S(K) \arrow[d] \\
0 \arrow[r] & \mathrm{Sel}_{S,\Box}(K_m, T_{f,n})^{G_m} \arrow[r] & H^1(K_m, T_{f,n})^{G_m} \arrow[r] & \Omega_S(K_m),
\end{tikzcd} \tag{11}$$

where

$$\begin{aligned}
\Omega_S(K) &:= \left(\oplus_{\ell|S} H^1(K_\ell, T_{f,n})\right) \oplus \left(\oplus_{\ell\nmid pS} H^1_{\mathrm{sing}}(K_\ell, T_{f,n})\right), \\
\Omega_S(K_m) &:= \left(\oplus_{\ell|S} H^1(K_{m,\ell}, T_{f,n})\right) \oplus \left(\oplus_{\ell\nmid pS} H^1_{\mathrm{sing}}(K_{m,\ell}, T_{f,n})\right).
\end{aligned}$$

The inflation-restriction sequence for $T_{f,n}$ implies that the middle vertical map in (11) is an isomorphism, because $T_{f,n}^{G_m} = 0$. The rightmost vertical map is injective, by Lemma 3.2 and the fact that primes in S split completely in K_m/K. It follows from the five-lemma that $\mathrm{Sel}_{S,\Box}(K, T_{f,n}) = \mathrm{Sel}_{S,\Box}(K_m, T_{f,n})^{G_m}$, and therefore

$$\begin{aligned}
\mathrm{Sel}_{S,\Box}(K_m, T_{f,n})[\mathfrak{m}] &= \mathrm{Sel}_{S,\Box}(K_m, T_{f,n})[I][p] = \\
&= \mathrm{Sel}_{S,\Box}(K, T_{f,n})[p] = \mathrm{Sel}_{S,\Box}(K, T_{f,1}),
\end{aligned}$$

where the last equality follows from the fact that $H^0(K, T_{f,n-1}) = 0$. The proof of the second assertion, in which $\Box$ is replaced by 0, uses in addition the injectivity of the map $H^1(K_p, T_{f,n}) \longrightarrow H^1(K_{m,p}, T_{f,n})^{G_m}$ in the analysis of the diagram analogue to diagram 11 (which follows from the fact that $T_{f,n}^{G_{K_{m,p}}} = 0$), but is otherwise the same. $\Box$

Lemma 3.18. *If S is an n-admissible set, then $\mathrm{Sel}_{S,\sharp}(K_m, T_{f,n}) = 0$, for all m and $\sharp = 0, \pm, \mathrm{fin}$, or $\Box$.*

Proof. It suffices to show that the finite $\Lambda_{n,m}$-module $M := \mathrm{Sel}_{S,\Box}(K_m, T_{f,n})$ is trivial, since this Selmer group contains all the others. By Lemma 3.17 and (10),

$$M[\mathfrak{m}] = \mathrm{Sel}_{S,\Box}(K, T_{f,1}) = 0,$$

and hence $M = 0$. $\Box$

The following proposition gives explicit formulae for the cardinality of the global cohomology groups $H^1_{S,\sharp}(K_m, T_{f,n})$.

Proposition 3.19. *Let $t := \#S - 2$, and let $\delta_m := [K_m : K] = p^m$. For all n-admissible sets S, and for all $m \geq 0$,*

$$\begin{aligned} \#H^1_{S,0}(K_m, T_{f,n}) &= p^{nt\delta_m}, \\ \#H^1_{S,\square}(K_m, T_{f,n}) &= \#H^1_{S,0}(K_m, T_{f,n})\#H^1(K_{m,p}, T_{f,n}). \end{aligned}$$

Proof. A general theorem arising from the Poitou-Tate exact sequence in Galois cohomology (cf. for example Theorem 2.19 of [DDT]) relates the cardinalities of a Selmer group and its dual, expressing the ratio of these cardinalities as a product of simple local terms. In the present context, Theorem 2.19 of [DDT] gives:

$$\begin{aligned} \frac{\#H^1_{S,0}(K_m, T_{f,n})}{\#\mathrm{Sel}_{S,\square}(K_m, T_{f,n})} &= \left(\prod_{\ell | S\infty} \frac{\#H^1(K_{m,\ell}, T_{f,n})}{\#H^0(K_{m,\ell}, T_{f,n})} \right), \\ \frac{\#H^1_{S,\square}(K_m, T_{f,n})}{\#\mathrm{Sel}_{S,0}(K_m, T_{f,n})} &= \left(\prod_{\ell | S\infty} \frac{\#H^1(K_{m,\ell}, T_{f,n})}{\#H^0(K_{m,\ell}, T_{f,n})} \right) \times \#H^1(K_{m,p}, T_{f,n}). \end{aligned}$$

By Lemma 3.18, the denominators occurring in the left-hand sides of these formulae are equal to 1. Furthermore, we already know from Lemma 3.4 that

$$\frac{\#H^1(K_{m,\ell}, T_{f,n})}{\#H^0(K_{m,\ell}, T_{f,n})} = \begin{cases} p^{n\delta_m} & \text{if } v|S; \\ p^{-2n\delta_m} & \text{if } v = \infty. \end{cases}$$

The Proposition follows. □

The usefulness of the concept of n-admissible set lies in the following two propositions concerning the groups $H^1_{S,0}(K_m, T_{f,n})$ and $H^1_{S,\pm}(K_m, T_{f,n})$. These propositions can be viewed as global analogues of Lemma 3.4 and Corollary 3.11.

Proposition 3.20. *If S is an n-admissible set, then the group $H^1_{S,0}(K_m, T_{f,n})$ is free of rank $t := \#S - 2$ over $\Lambda_{n,m}$.*

Proof. Consider the module $M := (H^1_{S,0}(K_m, T_{f,n}))^\vee$, where the superscript $\vee$ denotes the Pontryagin dual. We have

$$M/\mathfrak{m}M = (H^1_{S,0}(K_m, T_{f,n})[\mathfrak{m}])^\vee = (H^1_{S,0}(K, T_{f,1}))^\vee \simeq (\mathbb{Z}/p\mathbb{Z})^t,$$

where the second equality follows from Lemma 3.17 and the third isomorphism from Proposition 3.19 with $m = 0$ and $n = 1$. Let $\xi_1, \dots, \xi_t$ be a set of elements of M which map to a basis for $M/\mathfrak{m}M$. By Nakayama's lemma, these elements generate M as a $\Lambda_{n,m}$-module, and yield a surjective map $\Lambda_{n,m}^t \to M$ of $\Lambda_{n,m}$-modules. Proposition 3.19 implies that $\#M = \#(\Lambda_{n,m}^t)$, and hence this map is an isomorphism. It follows that the module M is free of rank t, and therefore

$$H^1_{S,0}(K_m, T_{f,n}) \simeq (\Lambda_{n,m}^\vee)^t.$$

The local ring $\Lambda_m := \mathbb{Z}_p[G_m] = \mathbb{Z}_p[t]/(t^{p^m} - 1)$ is a local complete intersection in the sense of Definition 5.1 of [DDT]. Hence by Proposition 5.9 of [DDT], it is Gorenstein in the sense of Definition 5.8 in [DDT], i.e.,

$$\mathrm{Hom}_{\mathbb{Z}_p}(\Lambda_m, \mathbb{Z}_p) \simeq \Lambda_m.$$

It follows that

$$\mathrm{Hom}_{\mathbb{Z}/p^n\mathbb{Z}}(\Lambda_{n,m}, \mathbb{Z}/p^n\mathbb{Z}) \simeq \Lambda_{n,m}.$$

This proves Proposition 3.20. □

Proposition 3.21. *If S is an n-admissible set, then the group $H^1_{S,\pm}(K_m, T_{f,n})$ is free of rank $\#S$ over $\Lambda_{n,m}$.*

Proof. The natural sequence

$$0 \longrightarrow H^1_{S,0}(K_m, T_{f,n}) \longrightarrow H^1_{S,\Box}(K_m, T_{f,n}) \longrightarrow H^1(K_{m,p}, T_{f,n}) \longrightarrow 0$$

is exact. This assertion follows from the definition of the objects involved, for all but the penultimate map, whose surjectivity is a consequence of the second assertion in Proposition 3.19. It follows that the sequence

$$0 \longrightarrow H^1_{S,0}(K_m, T_{f,n}) \longrightarrow H^1_{S,\pm}(K_m, T_{f,n}) \longrightarrow H^1_{\pm}(K_{m,p}, T_{f,n}) \longrightarrow 0$$

is exact. Proposition 3.21 now follows from Corollary 3.11 and Proposition 3.20. □

4 Construction of the Euler system

We maintain the notations of the previous sections, and fix an n-admissible prime ℓ for f. Let $X := X_{N^+,N^-\ell}$ be the Shimura curve introduced in Section

5.1 of [BD2], and let $P_m \in X(\tilde{K}_m)$ be the Heegner point of conductor p^m defined in Section 6 of [BD2], where the integers which are denoted M^+ and M^- in that section are set to be equal to N^+ and $N^-\ell$ respectively. Note that, unlike the setting that is considered in Section 6 of [BD2], the integer M^+ is now assumed to be prime to p. The behaviour of Heegner points under norms (cf. for example Proposition 3.10 of [Da]) implies that the Heegner points P_m satisfy the following compatibilities (expressed as equalities of divisors on X) for all $m \geq 1$:

$$\mathrm{Tr}_m^{m+1}(P_{m+1}) = T_p P_m - P_{m-1},$$

where Tr_m^{m+1} denotes the Galois trace from the $m+1$-st layer to the m-th layer (i.e., from $\tilde{K}_{m+2}$ to $\tilde{K}_{m+1}$, or from K_{m+1} to K_m), and T_p is the p-th Hecke operator. Let g be an eigenform of weight 2 on X such that $T_{g,n} \cong T_{f,n} = T$ as Galois modules. Such an eigenform exists by condition 4 in the definition of n-admissible primes: cf. Proposition 3.12 of [BD2].

In order to replace the points P_m on X by degree zero divisors, we choose a fixed auxiliary prime q which does not divide N, ℓ, or p, and let

$$\tilde{P}_m := (T_q - (q+1))P_m \in \mathrm{Div}^0(X).$$

Denote by the same symbol the image of this divisor in the Jacobian $\mathrm{Jac}(X)$ of X.

Let $\tilde{\kappa}(\ell)_m$ denote the image of $\tilde{P}_m$ in $H^1(\tilde{K}_m, \mathrm{Jac}(X)[p^n])$ under the global Kummer map. Write $\kappa(\ell)_m$ for the image of $\tilde{\kappa}(\ell)_m$ under the composition

$$H^1(\tilde{K}_m, \mathrm{Jac}(X)[p^n]) \longrightarrow H^1(\tilde{K}_m, T_{g,n}) \longrightarrow H^1(K_m, T_{g,n}) \cong H^1(K_m, T).$$

The first map is induced by "projection onto the g-isotypical component" $\mathrm{Jac}(X)[p^n] \longrightarrow T_{g,n}$, the second is co-restriction and the third is induced by the isomorphism $T_{g,n} \cong T$.

Proposition 4.1. *The element $\kappa(\ell)_m$ belongs to $H^1_{\ell,\mathrm{fin}}(K_m, T)$.*

Proof. Everything follows from Section 7 and the beginning of Section 8 of [BD2] except the behaviour of the class under localization at primes above p. Let $\mathfrak{p}$ be a prime of K_m above p, then by the properties of the Kummer map and of co-restriction we have $\tilde{\kappa}(\ell)_{m,\mathfrak{p}} \in H^1_{\mathrm{fin}}(K_{m,\mathfrak{p}}, T_{g,n})$. Now apply Theorem 3.10 and deduce that $\tilde{\kappa}(\ell)_{m,\mathfrak{p}} \in H^1_{\mathrm{fin}}(K_{m,\mathfrak{p}}, T)$. Hence $\kappa(\ell)_{m,p}$ belongs to $H^1_{\mathrm{fin}}(K_{m,p}, T)$. □

The classes $\kappa(\ell)_m$ satisfy the compatibility relations under the trace maps

$$\mathrm{Tr}_m^{m+1}(\kappa(\ell)_{m+1}) = -\kappa(\ell)_{m-1}.$$

Therefore we have

Lemma 4.2. *Let ϵ denote the sign of $(-1)^m$. Then $\omega_m^\epsilon \kappa(\ell)_m = 0$.*

Proof. Let ξ_k denote the p^k-th cyclotomic polynomial in $T+1$ as in Section 2, and suppose without loss of generality that m is even. Then

$$\omega_m^+\kappa(\ell)_m = \omega_{m-2}^+\xi_m\kappa(\ell)_m = \omega_{m-2}^+\mathrm{Tr}_{m-1}^m(\kappa(\ell)_m) = -\omega_{m-2}^+\kappa(\ell)_{m-2}.$$

The result now follows by induction, using the fact that $T\kappa(\ell)_0 = 0$. The proof when m is odd is identical. □

Let S be a square-free product of primes which is n-admissible in the sense of Definition 3.16. We can view the class $\kappa(\ell)$ as an element of the larger $\Lambda_{n,m}$-module $H^1_{S,\pm}(K_m, T_{f,n})$. It is useful to do so because of the following proposition:

Proposition 4.3. *There exists a unique class*

$$\eta(\ell)_m^\epsilon \in H^1_{S,\epsilon}(K_m, T)/\omega_m^\epsilon H^1_{S,\epsilon}(K_m, T)$$

such that

$$\tilde{\omega}_m^{-\epsilon}\eta(\ell)_m^\epsilon = \kappa(\ell)_m.$$

Proof. This follows from the fact that $H^1_{S,\pm}(K_m, T)$ is a free $\Lambda_{n,m}$-module by Proposition 3.21, using Lemma 4.2 and Lemma 2.7. □

Now define the global cohomology classes indexed by the n-admissible primes ℓ:

$$\begin{aligned} \kappa(\ell)_m^+ &:= (-1)^{\frac{m}{2}}\eta(\ell)_m \in H^1_{S,+}(K_m, T)/\omega_m^+ \quad \text{if } m \text{ is even;} &(12)\\ \kappa(\ell)_m^- &:= (-1)^{\frac{m+1}{2}}\eta(\ell)_m \in H^1_{S,-}(K_m, T)/\omega_m^- \quad \text{if } m \text{ is odd.} \end{aligned}$$

An argument identical to the one used in the proof of Lemma 2.9 shows that the sequences $\{\kappa(\ell)_m^+\}_{m \text{ even}}$ and $\{\kappa(\ell)_m^-\}_{m \text{ odd}}$ are compatible under corestriction, so that we can write

$$\kappa(\ell)^\pm := \lim_{\leftarrow} \kappa(\ell)_m^\pm. \qquad (13)$$

This element belongs to

$$\varprojlim H^1_{S,\pm}(K_m,T)/\omega_m^{\pm} \cong \varprojlim (H^1_{S,\pm}(K_m,T)\otimes\Lambda/(\omega_m^{\pm},p^n)) = \widehat{H}^1_{S,\pm}(K_\infty,T).$$

Let ℓ be an n-admissible prime dividing S. Note that both $\widehat{H}^1_{\mathrm{fin}}(K_{\infty,\ell},T)$ and $\widehat{H}^1_{\mathrm{sing}}(K_{\infty,\ell},T)$ are isomorphic to Λ/p^n by Lemma 3.4.

As in [BD2], the classes $\kappa(\ell)^{\pm}$ satisfy two key reciprocity laws relating them to the p-adic L-functions $\mathcal{L}_f^{\pm}$ defined in Section 2. The first reciprocity law concerns the properties of the class $\kappa(\ell)^{\pm}$ at the prime ℓ.

Proposition 4.4. *The class $\kappa(\ell)^{\pm}$ satisfies:*

$$v_\ell(\kappa(\ell)^{\pm}) = 0, \qquad \partial_\ell(\kappa(\ell)^{\pm}) \equiv \mathcal{L}_f^{\pm} \pmod{p^n},$$

where the equality holds in Λ/p^n, up to multiplication by elements of $\mathbb{Z}_p^\times$ and G_∞.

Proof. Let us fix $m \geq 0$ and consider the following commutative diagram

$$\begin{tikzcd}
H^1_{S,\pm}(K_m,T)/\omega_m^{\pm} \arrow[r, "\partial_\ell"] & H^1(K_{m,\ell},T)/\omega_m^{\pm} \arrow[r, phantom, "="] & \Lambda/(\omega_m^{\pm},p^n) \\
H^1_{S,\pm}(K_m,T) \arrow[u] \arrow[r, "\partial_\ell"] & H^1(K_{m,\ell},T) \arrow[u] \arrow[r, phantom, "="] & \Lambda/(\omega_m,p^n) \arrow[u] \\
H^1_{S,\mathrm{fin}}(K_m,T) \arrow[u, phantom, "\cup"] \arrow[r, "\partial_\ell"] & H^1(K_{m,\ell},T) \arrow[u, equal] \arrow[r, phantom, "="] & \Lambda/(\omega_m,p^n) \arrow[u, equal]
\end{tikzcd}$$

The proof of the first explicit reciprocity law given in Section 8 of [BD2] adapts without change to the classes $\kappa(\ell)_m$ considered here and yields

$$\partial_\ell(\kappa(\ell)_m) = \mathcal{L}_m$$

up to units in $\Lambda_{n,m}$. Moreover as

$$\kappa(\ell)_m = (-1)^{[\frac{m+1}{2}]}\tilde{\omega}_m^{\mp}\kappa(\ell)_m^{\pm},$$

we have

$$(-1)^{[\frac{m+1}{2}]}\tilde{\omega}_m^{\mp}\partial_\ell(\kappa(\ell)_m^{\pm}) = \mathcal{L}_m = (-1)^{[\frac{m+1}{2}]}\tilde{\omega}_m^{\mp}\mathcal{L}_m^{\pm}$$

in $\tilde{\omega}_m^{\mp}\Lambda/(\omega_m,p^n)$. Using the isomorphism of Lemma 2.7 we conclude that

$$\partial_\ell(\kappa(\ell)_m^{\pm}) = \mathcal{L}_m^{\pm}$$

in $\Lambda/(\omega_m^{\pm},p^n)$ up to units in this ring. □

Let ℓ_1 and ℓ_2 be distinct n-admissible primes relative to f, such that p^n divides $\ell_1 + 1 - \epsilon_1 a_{\ell_1}(f)$ and $\ell_2 + 1 - \epsilon_2 a_{\ell_2}(f)$, for ϵ_1 and ϵ_2 equal to ± 1. It is further assumed that the pair (ℓ_1, ℓ_2) is *rigid* in the sense of Section 3.3 of [BD2].

The second reciprocity law describes the localization of $\kappa(\ell_1)$ at ℓ_2. Note that this localization belongs to the finite part of the local cohomology group at ℓ_2.

Let B' be the definite quaternion algebra of discriminant $\mathrm{Disc}(B)\ell_1\ell_2$, let R' be an Eichler $\mathbb{Z}[1/p]$-order of level N^+ in B' and let $\Gamma' := (R')^\times/\mathbb{Z}[1/p]^\times$. The theory of congruences between modular forms yields the following proposition:

Proposition 4.5. *There exists an eigenform $g \in S_2(\mathcal{T}/\Gamma', \mathbb{Z}/p^n\mathbb{Z})$ such that the following equalities modulo p^n hold:*

$$T_q g \equiv a_q(f) g \quad (q \not| N\ell_1\ell_2), \qquad U_q g \equiv a_q(f) g \quad (q|N), \tag{14}$$

$$U_{\ell_1} g \equiv \epsilon_1 g, \quad U_{\ell_2} g \equiv \epsilon_2 g.$$

Furthermore (because of the assumption that the pair (ℓ_1, ℓ_2) is rigid) the form g can be lifted to an eigenform with coefficients in $\mathbb{Z}_p$ satisfying (14) above. This form is p-isolated.

Proof. The existence of the mod p^n eigenform g, which relies on the concepts and notations introduced in Sections 5 and 9 of [BD2], is proved in Theorem 9.3 of [BD2]. □

For any class $\kappa \in \widehat{H}^1_{S,\pm}(K_\infty, T)$, and any n-admissible prime ℓ which does not divide S, write $v_\ell(\kappa)$ for the natural image of κ in $\widehat{H}^1_{\mathrm{fin}}(K_{\infty,\ell}, T_{f,n})$ under the restriction map at ℓ. Note again that the target module for v_ℓ is isomorphic to $\Lambda/p^n\Lambda$ by Lemma 2.7 of [BD2]. With these notations we are ready to state the second explicit reciprocity law.

Proposition 4.6. *The equality*

$$v_{\ell_2}(\kappa(\ell_1)^\pm) = \mathcal{L}_g^\pm$$

holds in $\widehat{H}^1_{\mathrm{fin}}(K_{\infty,\ell_2}, T_{f,n}) \simeq \Lambda/p^n\Lambda$, up to multiplication by elements of $\mathbb{Z}_p^\times$ and G_∞.

Proof. This is essentially Theorem 4.2 of [BD2], whose proof, explained in Section 9 of that article, adapts to the setting where $a_p = 0$, the class $\kappa(\ell_1)$ is replaced by $\kappa(\ell_1)^{\pm}$ and $\mathcal{L}_g$ is replaced by $\mathcal{L}_g^{\pm}$. □

We record the following consequence of Propositions 4.4 and 4.6:

Corollary 4.7. *For all pairs of n-admissible primes (ℓ_1, ℓ_2) attached to f, the equality*

$$v_{\ell_1}(\kappa(\ell_2)^{\pm}) = v_{\ell_2}(\kappa(\ell_1)^{\pm})$$

holds in $\Lambda/p^n\Lambda$, up to multiplication by elements of $\mathbb{Z}_p^{\times}$ and G_∞.

5 Proof of the main result

Following Section 2.1 of [BD2], we make the following assumptions on the mod p Galois representation attached to f which correspond to some of the hypotheses made in Assumption 1.6 on E.

Assumption 5.1. *The Galois representation attached to $T_{f,1}$ has image isomorphic to $\mathbf{GL}_2(\mathbb{F}_p)$. Furthermore, for all ℓ dividing N exactly, the Galois representation $T_{f,1}$ has a unique* $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$*-stable one-dimensional subspace.*

Thanks to the reciprocity laws given in proposition 4.4 and 4.6 of the previous section, the classes $\kappa(\ell)^{\pm} \in \widehat{H}^1_{\{\ell,\pm\}}(K_\infty, T_{f,n})$ indexed by the n-admissible primes attached to f enjoy exactly the same properties as the classes $\kappa(\ell)$ used in [BD2] in the study of the main conjecture in the ordinary case. They will be used to show:

Theorem 5.2. *Let f be an eigenform in $S_2(\mathcal{V}/\Gamma)$ with coefficients in $\mathbb{Z}_p$ which is p-isolated and satisfies assumption 5.1 above. Then the characteristic power series of* $(\mathrm{Sel}_{\pm}(K_\infty, T_{f,\infty}))^{\vee}$ *divides the p-adic L-function $L_p^{\pm}(f, K)$.*

The proof (as well as the statement!) of this theorem is identical to that of Theorem 4.4. of [BD2], after replacing $\mathrm{Sel}(K_\infty, T_{f,\infty})$ by $\mathrm{Sel}_{\pm}(K_\infty, T_{f,\infty})$ and $\kappa(\ell)$ by $\kappa(\ell)^{\pm}$. Before launching into this proof, let us first make the following general comments.

1. Unlike the approach that is followed in [Ka], where p-Selmer groups are bounded via global cohomology classes whose local behaviour at the

prime p is related to p-adic L-functions, our approach adapts to the supersingular setting the ideas of [BD2], where the p-Selmer group is controlled using global classes whose local behaviour at primes $\ell \neq p$ is related to p-adic L-series. The main new difficulty in the supersingular case lies in the construction of the classes $\kappa(\ell)^{\pm}$ satisfying the same relation to the Pollack-style p-adic L-functions $\mathcal{L}_f^{\pm}$ and $\mathcal{L}_g^{\pm}$ as the classes $\kappa(\ell)$ did with $\mathcal{L}_f$ and $\mathcal{L}_g$. With these classes in hand, the argument of [BD2] never involves the local behaviour of the Galois representations $T_{f,n}$ and $T_{f,n}$ at p, but only at n-admissible primes $\ell \neq p$ which split completely in K_∞/K. This is why the Euler system argument in the proof of Theorem 4.4 of [BD2] extends to the supersingular setting without raising new difficulties or requiring substantial modifications.

2. Our approach to Theorem 5.2 is to prove it by induction, reducing the statement about f to an identical one about g for an appropriately chosen modular form g which is congruent to f modulo p^n. It is for this reason that a more general main conjecture (applying to all modular eigenforms on definite quaternion algebras with $\mathbb{Z}_p$-coefficients, and not just those associated to elliptic curves) is needed even if one is only interested in establishing Theorem 1.4 of the introduction.

Proof of Theorem 5.2: For the convenience of the reader, we recall here the main lines of the argument, with an emphasis on the aspects that are specific to the supersingular setting. Note however that we follow the strategy of the proof of Theorem 4.4 of [BD2] very closely, and that the modifications that need to be made to this proof are comparatively minor.

Proposition 3.1 of [BD2], implies that it is enough to show that

$$\varphi(\mathcal{L}_f^{\pm})^2 \text{ belongs to } \mathrm{Fitt}_{\mathcal{O}}((\mathrm{Sel}_{\pm}(K_\infty, T_{f,n}))^\vee \otimes_\varphi \mathcal{O}), \tag{15}$$

for all homomorphisms φ of Λ into a discrete valuation ring $\mathcal{O}$. Fix $\mathcal{O}$, φ, and n, write π for a uniformiser of $\mathcal{O}$, and let $e := \mathrm{ord}_\pi(p)$ be absolute ramification degree of $\mathcal{O}$. Write

$$t_f := \mathrm{ord}_\pi(\varphi(\mathcal{L}_f^{\pm})).$$

Assume without loss of generality that
1. $t_f < \infty$. (Otherwise, $\varphi(\mathcal{L}_f^{\pm}) = 0$ and (16) is trivially verified.)
2. The group $(\mathrm{Sel}_{\pm}(K_\infty, T_{f,n}))^\vee \otimes \mathcal{O}$ is non-trivial. (Otherwise, its Fitting ideal is equal to $\mathcal{O}$ and (16) is trivially verified.)

We propose to show that

$$\varphi(\mathcal{L}_f^{\pm})^2 \text{ belongs to } \mathrm{Fitt}_{\mathcal{O}}((\mathrm{Sel}_{\pm}(K_\infty, T_{f,n}))^\vee \otimes_\varphi \mathcal{O}) \tag{16}$$

by induction on t_f.

We begin by using the classes $\kappa(\ell)^{\pm}$ to construct global cohomology classes that will be used to bound $\mathrm{Sel}_{\pm}(K_\infty, T_{f,n})$. Let ℓ be any $(n+t_f)$-admissible prime, and let S be a square-free product of $(n+t_f)$-admissible primes with $\ell|S$. Let

$$\kappa(\ell)^{\pm} \in \widehat{H}^1_{\{\ell\},\pm}(K_\infty, T_{f,n+t_f}) \subset \widehat{H}^1_{S,\pm}(K_\infty, T_{f,n+t_f})$$

be the cohomology class attached to ℓ in (13), and denote by $\kappa_\varphi(\ell)^{\pm}$ the natural image of this class in

$$\mathcal{M} := \widehat{H}^1_S(K_\infty, T_{f,n+t_f}) \otimes_\varphi \mathcal{O}.$$

Note that this module is free over $\mathcal{O}/p^{(n+t_f)}$, by Proposition 3.21. By Proposition 4.4,

$$\mathrm{ord}_\pi(\kappa_\varphi(\ell)^{\pm}) \leq \mathrm{ord}_\pi(\partial_\ell \kappa_\varphi(\ell)^{\pm}) = \mathrm{ord}_\pi(\varphi(\mathcal{L}_f^{\pm})) = t_f,$$

so that $t := \mathrm{ord}_\pi(\kappa_\varphi(\ell)^{\pm}) \leq t_f$. Choose an element $\tilde{\kappa}_\varphi(\ell)^{\pm} \in \mathcal{M}$ satisfying

$$\pi^t \tilde{\kappa}_\varphi(\ell)^{\pm} = \kappa_\varphi(\ell)^{\pm}. \tag{17}$$

Note that $\tilde{\kappa}_\varphi(\ell)^{\pm}$ is well defined modulo the π^t-torsion subgroup of $\mathcal{M}$, which is contained in the kernel of the natural homomorphism

$$\widehat{H}^1_S(K_\infty, T_{f,n+t_f}) \otimes_\varphi \mathcal{O} \longrightarrow \widehat{H}^1_S(K_\infty, T_{f,n}) \otimes_\varphi \mathcal{O}.$$

Let $\kappa'_\varphi(\ell)^{\pm}$ denote the image of $\tilde{\kappa}_\varphi(\ell)^{\pm}$ in $\widehat{H}^1_S(K_\infty, T_{f,n}) \otimes \mathcal{O}$. Note that this class does not depend on the choice of $\tilde{\kappa}_\varphi(\ell)^{\pm}$ satisfying (17). The key properties of the class $\kappa'_\varphi(\ell)^{\pm}$ are summarized in the following two Lemmas. 5.3 and 5.4 below.

Lemma 5.3. *The class $\kappa'_\varphi(\ell)^{\pm}$ belongs to $\widehat{H}^1_{\ell,\pm}(K_\infty, T_{f,n}) \otimes_\varphi \mathcal{O}$, and*

1. $\mathrm{ord}_\pi(\kappa'_\varphi(\ell)^{\pm}) = 0$.
2. $v_\ell(\kappa'_\varphi(\ell)^{\pm}) = 0$, *and* $\mathrm{ord}_\pi(\partial_\ell \kappa'_\varphi(\ell)^{\pm}) = t_f - t$.

Proof. The fact that $\kappa'_\varphi(\ell)^\pm$ belongs to $\widehat{H}^1_{\ell,\pm}(K_\infty, T_{f,n}) \otimes_\varphi \mathcal{O}$ follows from the fact that $\kappa(\ell)^\pm$ belongs to $\widehat{H}^1_{\ell,\pm}(K_\infty, T_{f,n+t_f})$. Property 1 follows from the construction of $\kappa'_\varphi(\ell)^\pm$, while property 2 is a direct consequence of Proposition 4.4. □

Lemma 5.4. *The residue $\partial_\ell(\kappa'_\varphi(\ell)^\pm)$ belongs to the kernel of the natural homomorphism*

$$\eta_\ell : \widehat{H}^1_{\mathrm{sing}}(K_{\infty,\ell}, T_{f,n}) \otimes_\varphi \mathcal{O} \longrightarrow (\mathrm{Sel}_\pm(K_\infty, T_{f,n}))^\vee \otimes_\varphi \mathcal{O}.$$

Proof. The proof is the same as that of Lemma 4.6 of [BD2]. □

We now turn to the proof of (16) when $t_f = 0$—the basis for the induction argument.

Proposition 5.5. *If $t_f = 0$, (i.e., $\mathcal{L}_f^\pm$ is a unit) then $(\mathrm{Sel}_\pm(K_\infty, T_{f,n}))^\vee$ is trivial.*

Proof. The proof is the same as that of Proposition 4.7 of [BD2], which makes no use of the hypothesis that p is ordinary. □

Turning now to the general case of equation (16), let Π be the set of rational primes ℓ satisfying the following conditions:

1. ℓ is $(n + t_f)$-admissible.
2. The quantity $t = \mathrm{ord}_\pi(\kappa_\varphi(\ell)^\pm)$ is minimal, among all primes satisfying condition 1.

Proposition 3.15 implies that Π is non-empty. Let t be the common value of $\mathrm{ord}_\pi(\kappa_\varphi(\ell)^\pm)$ for all $\ell \in \Pi$. Note that $t \leq t_f$ by definition.

Lemma 5.6. *The integer t is strictly less than t_f.*

Proof. See Proposition 4.8 of [BD2]. □

Before stating the next lemma, we need to recall the notion of *rigid pairs* of n-admissible primes that is defined in Section 3.3 of [BD2]. This notion relies on the Selmer group $\mathrm{Sel}_S(\mathbb{Q}, W_f)$ attached to the 3-dimensional mod p representation $W_f := \mathrm{ad}_0(T_{f,1})$ consisting of trace 0 endomorphisms of $T_{f,1}$, and to a square-free product S of 1-admissible primes. The definition of this Selmer group is the same as in Definition 3.5 of [BD2], except that, since W_f

is not ordinary at p, but is crystalline, the group $H^1_{\mathrm{fin}}(\mathbb{Q}_p, W_f)$ is defined to be the set of cohomology classes that are crystalline at p. With this change, it is still true that f is p-isolated precisely when $\mathrm{Sel}_1(\mathbb{Q}, W_f) = 0$. (This is just Proposition 3.6. of [BD2] whose proof applies just as well to the case where f is non-ordinary at p.) Following Definition 3.9 of [BD2], we say that a pair (ℓ_1, ℓ_2) of n-admissible primes is a *rigid pair* if $\mathrm{Sel}_{\ell_1\ell_2}(\mathbb{Q}, W_f)$ is trivial.

Lemma 5.7. *There exist primes $\ell_1, \ell_2 \in \Pi$ such that (ℓ_1, ℓ_2) is a rigid pair.*

Proof. See Lemma 4.9 of [BD2] whose proof adapts without change to the supersingular setting. □

Let (ℓ_1, ℓ_2) be a rigid pair of $(n + t_f)$-admissible primes in Π, whose existence is guaranteed by Lemma 5.7. By Proposition 4.6, note that $t = t_g = \mathrm{ord}_\pi(\varphi(\mathcal{L}_g))$, where g is the p-isolated eigenform in $S_2(\mathcal{T}/\Gamma')$ attached to f and (ℓ_1, ℓ_2) through proposition 4.5.

Recall the Selmer group

$$\mathrm{Sel}_{\ell_1\ell_2,\pm}(K_\infty, T_{f,n}) \subset \mathrm{Sel}_\pm(K_\infty, T_{f,n})$$

consisting of classes which are locally trivial at the primes dividing ℓ_1 and ℓ_2. By definition, there is a natural exact sequence of Λ-modules

$$0 \longrightarrow S^f_{\ell_1\ell_2} \longrightarrow (\mathrm{Sel}_\pm(K_\infty, T_{f,n}))^\vee \longrightarrow (\mathrm{Sel}_{\ell_1\ell_2,\pm}(K_\infty, T_{f,n}))^\vee \longrightarrow 0, \quad (18)$$

where $S^f_{\ell_1\ell_2}$ denotes the kernel of the natural surjection of duals of Selmer groups. Note the natural surjection given by local Tate duality:

$$\eta_f : (\widehat{H}^1_{\mathrm{sing}}(K_{\infty,\ell_1}, T_{f,n}) \oplus \widehat{H}^1_{\mathrm{sing}}(K_{\infty,\ell_2}, T_{f,n})) \longrightarrow S^f_{\ell_1\ell_2}$$

induced from the inclusion

$$(S^f_{\ell_1\ell_2})^\vee \subset H^1_{\mathrm{fin}}(K_{\infty,\ell_1}, T_{f,n}) \oplus H^1_{\mathrm{fin}}(K_{\infty,\ell_2}, T_{f,n}).$$

The domain of η_f is isomorphic to $(\Lambda/p^n\Lambda)^2$, by Lemma 2.7 of [BD2]. Let η_f^φ denote the map induced from η_f after tensoring by $\mathcal{O}$ via φ. The domain of η_f^φ is isomorphic to $(\mathcal{O}/p^n\mathcal{O})^2$. By Lemma 5.4, the kernel of η_f^φ contains the vectors $(\partial_{\ell_1}\kappa'_\varphi(\ell_1)^\pm, 0)$ and $(0, \partial_{\ell_2}\kappa'_\varphi(\ell_2)^\pm)$ in

$$\left(\widehat{H}^1_{\mathrm{sing}}(K_{\infty,\ell_1}, T_{f,n}) \oplus \widehat{H}^1_{\mathrm{sing}}(K_{\infty,\ell_2}, T_{f,n})\right) \otimes_\varphi \mathcal{O} \simeq (\mathcal{O}/p^n\mathcal{O})^2.$$

By part 3 of Lemma 5.3,

$$t_f - t_g = \mathrm{ord}_\pi(\partial_{\ell_1}\kappa'_\varphi(\ell_1)^\pm) = \mathrm{ord}_\pi(\partial_{\ell_2}\kappa'_\varphi(\ell_2)^\pm).$$

Hence

$$\pi^{2(t_f - t_g)} \text{ belongs to the Fitting ideal of } S^f_{\ell_1\ell_2} \otimes_\varphi \mathcal{O}. \qquad (19)$$

One may repeat the same argument with the modular form g. Thus we have an exact sequence similar to (18) but involving g instead of f:

$$0 \longrightarrow S^g_{\ell_1\ell_2} \longrightarrow (\mathrm{Sel}_\pm(K_\infty, T_{g,n}))^\vee \longrightarrow (\mathrm{Sel}_{\ell_1\ell_2,\pm}(K_\infty, T_{g,n})))^\vee \longrightarrow 0, \quad (20)$$

as well as a surjection given by local Tate duality:

$$\eta_g : (\widehat{H}^1_{\mathrm{fin}}(K_{\infty,\ell_1}, T_{f,n}) \oplus \widehat{H}^1_{\mathrm{fin}}(K_{\infty,\ell_2}, T_{f,n})) \longrightarrow S^g_{\ell_1\ell_2}.$$

By global reciprocity, the kernel of the map η_g^φ obtained from η_g after tensoring by $\mathcal{O}$ via φ contains the elements

$$(v_{\ell_1}\kappa'_\varphi(\ell_1)^\pm, v_{\ell_2}\kappa'_\varphi(\ell_1)^\pm) = (0, v_{\ell_2}\kappa'_\varphi(\ell_1)^\pm)$$

as well as $(v_{\ell_1}\kappa'_\varphi(\ell_2)^\pm, 0)$. But

$$\mathrm{ord}_\pi(v_{\ell_2}\kappa'_\varphi(\ell_1)^\pm) = \mathrm{ord}_\pi(v_{\ell_1}\kappa'_\varphi(\ell_2)^\pm) = t_g - t = 0.$$

It follows that the module $S^g_{\ell_1\ell_2} \otimes_\varphi \mathcal{O}$ is trivial, and the natural surjection

$$(\mathrm{Sel}_\pm(K_\infty, T_{g,n}))^\vee \otimes_\varphi \mathcal{O} \longrightarrow (\mathrm{Sel}_{\ell_1\ell_2,\pm}(K_\infty, T_{g,n}))^\vee \otimes_\varphi \mathcal{O} \text{ is an isomorphism.} \quad (21)$$

Recall that, by Lemma 5.6,

$$t_g < t_f,$$

and that the eigenform g satisfies all the hypotheses of Theorem 5.2. (The fact that g is p-isolated follows from the fact that (ℓ_1, ℓ_2) is a rigid pair of admissible primes.) By the induction hypothesis,

$$\varphi(\mathcal{L}_g)^2 \text{ belongs to the Fitting ideal of } (\mathrm{Sel}_\pm(K_\infty, T_{g,n}))^\vee \otimes_\varphi \mathcal{O}. \qquad (22)$$

The theory of Fitting ideals implies that

$$\begin{array}{rcl} \pi^{2t_f} & = & \pi^{2(t_f - t_g)}\pi^{2t_g} \\ & \in & \mathrm{Fitt}_\mathcal{O}(S^f_{\ell_1\ell_2} \otimes \mathcal{O})\,\mathrm{Fitt}_\mathcal{O}((\mathrm{Sel}_\pm(K_\infty, T_{g,n}))^\vee \otimes \mathcal{O}), \quad \text{by (19) and (22)} \\ & = & \mathrm{Fitt}_\mathcal{O}(S^f_{\ell_1\ell_2} \otimes \mathcal{O})\,\mathrm{Fitt}_\mathcal{O}((\mathrm{Sel}_{\ell_1\ell_2,\pm}(K_\infty, T_{g,n}))^\vee \otimes \mathcal{O}), \quad \text{by (21).} \end{array}$$

But note that $\mathrm{Sel}_{\ell_1\ell_2,\pm}(K_\infty, T_{g,n}) = \mathrm{Sel}_{\ell_1\ell_2,\pm}(K_\infty, T_{f,n})$ by definition, in light of the fact that the Galois modules $T_{f,n}$ and $T_{g,n}$ are isomorphic, and that the local conditions used to define the associated Selmer groups are the same outside of ℓ_1 and ℓ_2. It follows that

$$\begin{aligned} \pi^{2t_f} &\in \mathrm{Fitt}_{\mathcal{O}}(S^f_{\ell_1\ell_2} \otimes \mathcal{O})\,\mathrm{Fitt}_{\mathcal{O}}((\mathrm{Sel}_{\ell_1\ell_2,\pm}(K_\infty, T_{f,n}))^\vee \otimes \mathcal{O}) \\ &\subset \mathrm{Fitt}_{\mathcal{O}}((\mathrm{Sel}_{\pm}(K_\infty, T_{f,n}))^\vee \otimes \mathcal{O}), \text{ by (18).} \end{aligned}$$

Hence $\varphi(\mathcal{L}_f^{\pm})^2$ belongs to the Fitting ideal of $(\mathrm{Sel}_{\pm}(K_\infty, T_{f,n}))^\vee \otimes_\varphi \mathcal{O}$, and (16) is therefore proved. Theorem 5.2 follows.

Note finally that Theorem 1.4 follows from Theorem 5.2 specialized to the case where f has integer Hecke eigenvalues, and hence corresponds to a modular elliptic curve E via the Eichler-Shimura construction combined with the Jacquet-Langlands correspondence.

References

[BD1] M. Bertolini and H. Darmon. *Derived heights and generalized Mazur-Tate regulators*. Duke Math. J. **76** (1994) 75–111.

[BD2] M. Bertolini and H. Darmon. *Iwasawa's Main Conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions*. Annals of Mathematics **162** (2005) 1-64.

[BK] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, I, (1990), 333-401, Birkhäuser.

[Br] C. Breuil, *Représentations p-adiques semi-stables et transversalité de Griffith*, Math.Ann.**307** (1997), 191-224

[Da] H. Darmon. Rational points on modular elliptic curves. CBMS Regional Conference Series in Mathematics, **101**. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004.

[DDT] H. Darmon, F. Diamond, and R. Taylor, *Fermat's Last Theorem*, Current Developments in Mathematics 1, 1995, International Press, pp. 1-157. Reprinted in Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), 2–140, International Press, Cambridge, MA, 1997.

[Fa] G. Faltings, *Integral crystalline cohomology over very ramified valuation rings*, Journal of AMS, **12**, No 1, (1999), 117-144

[FL] J.-M. Fontaine and G. Laffaille, *Constructions de représentations p-adiques*, Ann.Sci.Éc.Norm.Sup., **15**, (1988), 547-608

[GIP] R. Greenberg, A. Iovita, R. Pollack, *On Iwasawa Invariants of Elliptic Curves at Supersingular Primes*, preprint

[IP] A. Iovita and R. Pollack. *Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields.* Crelle, to appear.

[Ka] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms.* in Cohomologies p-adiques et applications arithmétiques. III. Astérisque No. 295 (2004), ix, 117–290.

[Kob] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. 152 (2003), no. 1, 1–36.

[Kol] V.A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $\underline{III}(E, \mathbb{Q})$ for a subclass of Weil curves.* Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), no. 3, 522–540, 670–671; translation in Math. USSR-Izv. 32 (1989), no. 3, 523–541.

[Ku] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, Invent. Math. **149** (2002), 195–224.

[PR1] B. Perrin-Riou, *Théorie d'Iwasawa p-adique locale et globale.* Invent. Math. **99** (1990), no. 2, 247–292.

[PR2] B. Perrin-Riou, *Fonctions L p-adiques d'une courbe elliptique et points rationnels.* Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 945–995.

[PR3] B. Perrin-Riou, *Théorie d'Iwasawa des représentations p-adiques sur un corps local.* Invent. Math. **115** (1994), no. 1, 81–161.

[PR4] B. Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, preprint.

[Po1] R. Pollack. *On the p-adic L-function of a modular form at a supersingular prime.* Duke Mathematical Journal **118** (2003) no. 3, 523–558.

[Po2] R. Pollack, An algebraic version of a theorem of Kurihara, Journal of Number Theory **110/1** (2004), 164–177.

[Ta] J. Tate, Duality theorems in Galois cohomology over number fields, in *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, 288–295, Inst. Mittag-Leffler, Djursholm, 1963.

[Va] V. Vatsal, Uniform distribution of Heegner points, Invent. Math. **148** (2002), no. 1, 1–46.