NON-VANISHING OF KOLYVAGIN SYSTEMS AND IWASAWA THEORY

ASHAY BURUNGALE, FRANCESC CASTELLA, GIADA GROSSI, AND CHRISTOPHER SKINNER

Abstract. Let $E/\mathbb{Q}$ be an elliptic curve and p an odd prime. In 1991 Kolyvagin conjectured that the system of cohomology classes for the p-adic Tate module of E derived from Heegner points on E over ring class fields of an imaginary quadratic field K is non-trivial. In this paper we prove Kolyvagin's conjecture in the cases where p is a prime of good ordinary reduction for E that splits in K and a p-adic anticyclotomic Iwasawa Main Conjecture for E/K holds. In particular, our results cover many cases where p is an Eisenstein prime, complementing W. Zhang's progress towards the conjecture.

Our methods also yield a proof of a refinement of Kolyvagin's conjecture expressing the divisibility index of the p-adic Heegner point Kolyvagin system in terms of the Tamagawa numbers of E, as conjectured by W. Zhang in 2014, as well as proofs of analogous results for the Kolyvagin systems obtained from the cyclotomic Euler system of Beilinson–Kato elements.

Contents

Introduction

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and let p be an odd prime of good ordinary reduction for E. In this paper we prove Kolyvagin's conjecture on the non-vanishing of the p-adic Heegner point Kolyvagin system under mild conditions (cf. Theorem A). When p is non-Eisenstein for E, the conjecture was first proved by W. Zhang in many cases. The approach introduced in this paper covers the general non-Eisenstein case, as well as the first general cases where p is Eisenstein for E. Moreover, in the former case we prove the *refined* Kolyvagin conjecture due to W. Zhang, expressing the divisibility index of the Heegner point Kolyvagin system in terms of the Tamagawa numbers of E (cf. Theorem B). Following a similar strategy, we also prove analogous results for the Kolyvagin system derived from Beilinson–Kato elements (cf. Theorem C).

0.1. Main results.

Date: December 14, 2023.

Kolyvagin's conjecture. Let K be an imaginary quadratic field of discriminant $-D_K < 0$ such that

$$\text{every prime } \ell | N \text{ splits in } K, \tag{Heeg}$$

and fix an integral ideal $\mathfrak{N} \subset \mathcal{O}_K$ with $\mathcal{O}_K/\mathfrak{N} = \mathbb{Z}/N\mathbb{Z}$. Assume also that

$$D_K \text{ is odd and } D_K \neq -3. \tag{disc}$$

For each positive integer m prime to N, let $\mathcal{O}_m = \mathbb{Z} + m\mathcal{O}_K$ be the order of K of conductor m and denote by $K[m]$ the corresponding ring class field extension of K.

By the theory of complex multiplication, the cyclic N-isogeny between complex CM elliptic curves

$$\mathbb{C}/\mathcal{O}_m \to \mathbb{C}/(\mathfrak{N} \cap \mathcal{O}_m)^{-1}$$

defines a point $x_m \in X_0(N)(K[m])$. Fix a modular parameterisation

$$\pi : X_0(N) \to E. \tag{0.1}$$

The *Heegner point* of conductor m is defined by

$$P[m] := \pi(x_m) \in E(K[m]). \tag{0.2}$$

We call ℓ a *Kolyvagin prime* if ℓ is inert in K, coprime to Np, and

$$M(\ell) := \min\{\mathrm{ord}_p(\ell+1), \mathrm{ord}_p(a_\ell)\} > 0,$$

where $a_\ell := \ell + 1 - |\tilde{E}(\mathbb{F}_\ell)|$ and $\mathrm{ord}_p(x)$ denotes the p-adic valuation of an integer x. Let $\mathcal{N}_{\mathrm{Heeg}}$ be the set of squarefree products of Kolyvagin primes, and for $n \in \mathcal{N}_{\mathrm{Heeg}}$ put

$$M(n) := \min\{M(\ell) \,:\, \ell \mid n\}$$

if $n > 1$ and $M(1) := \infty$. Let $T = T_pE$ be the p-adic Tate module of E, and suppose that

$$E(K)[p] = 0. \tag{tor}$$

From the Kummer images of the Heegner points $P[n]$, Kolyvagin constructed a system of classes

$$\bigl\{\kappa_n^{\mathrm{Heeg}} \in \mathrm{H}^1(K, T/I_nT) \,:\, n \in \mathcal{N}_{\mathrm{Heeg}}\bigr\}, \quad \text{where } I_n = p^{M(n)}\mathbb{Z}_p.$$

In particular, κ_1^{Heeg} is the image of the Heegner point $P_K := \mathrm{Tr}_{K[1]/K}(P[1]) \in E(K)$ under the Kummer map

$$E(K) \otimes \mathbb{Z}_p \to \mathrm{H}^1(K, T),$$

and so by the Gross–Zagier formula [GZ86], $\kappa_1^{\mathrm{Heeg}} \neq 0$ if and only if $L'(E/K, 1) \neq 0$.

In [Kol91] Kolyvagin conjectured that even when the analytic rank of E/K is greater than one, the *system* $\{\kappa_n^{\mathrm{Heeg}}\}_n$ is non-trivial, i.e. there exists $n \in \mathcal{N}_{\mathrm{Heeg}}$ such that

$$\kappa_n^{\mathrm{Heeg}} \neq 0.$$

The first major progress towards this conjecture was due to W. Zhang [Zha14b]: about a decade ago, he proved Kolyvagin's conjecture when $p \nmid 6N$ is a prime of good ordinary reduction for E under the assumption that

$$\bar{\rho}_E : G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{F}_p}(E[p]) \text{ is surjective} \tag{sur}$$

and $\bar{\rho}_E$ satisfies certain ramification hypotheses. More recently, some of the hypotheses have been relaxed by N. Sweeting [Swe20] using an ultrapatching method for bipartite Euler systems.

In the first part of this paper we prove Kolyvagin's conjecture in cases where (sur) is not necessarily satisfied, and we also relax the ramification hypotheses. The paper considers Eisenstein primes p as well as cases where

$$E[p] \text{ is an irreducible } G_{\mathbb{Q}}\text{-module.} \tag{irr}$$

Our method relies on anticyclotomic Iwasawa theory, recent developments towards anticyclotomic main conjectures, and ideas introduced in [CGS23]. A key ingredient is a Kolyvagin system bound with "error terms" obtained in *op. cit.* allowing us to control the size of the Tate–Shafarevich group of certain anticyclotomic twists of T by characters α with $\alpha \equiv 1 \pmod{p^m}$ for $m \gg 0$. When (sur) is satisfied, the error terms are zero and when a certain Iwasawa Main Conjecture is known, our methods also yield a proof of the *refined Kolvyagin conjecture* due to W. Zhang [Zha14a, Conj. 4.5].

We now describe the main result precisely. Let $G_{\mathbb{Q}}$ be the absolute Galois group of $\mathbb{Q}$ and $G_p \subset G_{\mathbb{Q}}$ a decomposition group at p. Denote by $\omega : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ the Teichmüller character.

Theorem A (Kolyvagin's conjecture)**.** *Let $E/\mathbb{Q}$ be an elliptic curve, and let p be an odd prime of good ordinary reduction for E. Let K be a quadratic imaginary field satisfying* (Heeg), (disc), (tor)*, and such that p splits in K. Assume that the rational anticyclotomic Main Conjecture 1.2.10 holds. Then*

$$\text{there exists } n \in \mathcal{N}_{\mathrm{Heeg}} \text{ such that } \kappa_n^{\mathrm{Heeg}} \neq 0.$$

In particular, $\{\kappa_n^{\mathrm{Heeg}}\} \neq 0$ in both of the following cases:

- *E admits a rational p-isogeny with kernel $\mathbb{F}_p(\phi) \subset E[p]$, where $\phi : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$ is a character such that $\phi|_{G_p} \neq \mathbb{1}, \omega$.*
- *$p > 3$ satisfies* (irr).

The 'In particular' part of Theorem A relies on the results of [CGS23, BCS23], respectively, on the anticyclotomic Main Conjecture.

The non-vanishing of the Kolyvagin system in combination with [Kol91, Theorem 4] leads to a link between the *order of vanishing* of the Kolyvagin system and the rank of the p^∞-Selmer group of E/K. More precisely, for any n, let $\nu(n)$ denote the number of primes factors of n, and for $n \in \mathcal{N}_{\mathrm{Heeg}}$ let

$$\mathrm{ord}(\kappa^{\mathrm{Heeg}}) := \min\{r : \text{ there exists } n \in \mathcal{N}_{\mathrm{Heeg}} \text{ with } \nu(n) = r \text{ such that } \kappa_n^{\mathrm{Heeg}} \neq 0\}.$$

The p^∞-Selmer group $\mathrm{Sel}_{p^\infty}(E/K)$ has an action of complex conjugation. Denote by $\mathrm{Sel}_{p^\infty}(E/K)^{\pm}$ the $\pm$-eigenspaces with respect to this action and let

$$r(E/K)^{\pm} = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/K)^{\pm}.$$

Corollary A. *For E, p and K as in Theorem A, we have*

$$\mathrm{ord}(\kappa^{\mathrm{Heeg}}) = \max\{r(E/K)^+, r(E/K)^-\} - 1.$$

Remark. The corollary applies for arbitrary values of $r(E/K)^{\pm}$. In the rank one case it yields a p-converse to the Gross–Zagier and Kolyvagin theorem:

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/K) = 1 \implies \mathrm{ord}_{s=1} L(E/K, s) = 1$$

as the Birch and Swinnerton-Dyer conjecture predicts (cf. [Zha14b, Theorem 1.3]). One can also deduce the p-parity conjecture for $E/\mathbb{Q}$ (cf. [Zha14b, Theorem 1.2, Remark 1]).

Refined Kolyvagin's conjecture. As formulated by W. Zhang [Zha14b], a natural refinement of Kolyvagin's conjecture predicts a formula for the divisibility index of the Heegner point Kolyvagin system $\{\kappa_n^{\mathrm{Heeg}}\}$ in terms of the Tamagawa numbers

$$c_\ell = [E(\mathbb{Q}_\ell) : E^0(\mathbb{Q}_\ell)]$$

at the primes $\ell | N$.

For each $n \in \mathcal{N}_{\mathrm{Heeg}}$, define $\mathscr{M}(n) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by $\mathscr{M}(n) = \infty$ if $\kappa_n^{\mathrm{Heeg}} = 0$, and by

$$\mathscr{M}(n) = \max\{\mathscr{M} : \kappa_n^{\mathrm{Heeg}} \in p^{\mathscr{M}} \mathrm{H}^1(K, T/I_n T)\}$$

otherwise. Put $\mathscr{M}_r = \min\{\mathscr{M}(n) : \nu(n) = r\}$. We have $\mathscr{M}_r \geq \mathscr{M}_{r+1} \geq 0$ for all $r \geq 0$ (cf. [Kol91]). Put

$$\mathscr{M}_\infty = \lim_{r \to \infty} \mathscr{M}_r.$$

Note that Kolyvagin's conjecture is equivalent to the finiteness of $\mathscr{M}_\infty$. W. Zhang's refinement [Zha14b, Conj. 4.5] provides a conjectural formula for $\mathscr{M}_\infty$, which we establish:

Theorem B (Refined Kolyvagin's conjecture)**.** *Let (E, p, K) be as in Theorem A, and assume that $p > 3$ and* (sur) *holds. Assume also that the fixed modular parametrisation $\pi : X_0(N) \to E$ as in* (0.1) *is p-optimal*[1]. *Then we have*

$$\mathscr{M}_\infty = \sum_{\ell | N} \mathrm{ord}_p(c_\ell).$$

Remark. In the rank one case Theorem B implies the p-part of the conjectural Birch and Swinnerton-Dyer formula for E/K (cf. [Zha14b, Theorem 1.6]).

Our proof relies on the cases of the anticyclotomic Main Conjecture 1.2.10 established in [BCS23].

In [Jet08] Jetchev showed that $\mathscr{M}_\infty \geq \mathrm{ord}_p(c_\ell)$ for any prime $\ell | N$. The first cases of the refined Kolyvagin's conjecture were proved by W. Zhang: the ramification hypotheses in [Zha14b] imply that $p \nmid c_\ell$ for all primes $\ell | N$, and the main result of *op. cit.* shows that $\mathscr{M}_\infty = 0$.

[1]That is $\mathrm{ord}_p(\deg(\pi))$ is minimal among all modular parametrisations of all curves in the $\mathbb{Q}$-isogeny class of E.

Non-vanishing of Kato's Kolyvagin system. The strategy introduced in this paper for the proofs of Theorem A and Theorem B can be adapted to establish analogous results for the Kolyvagin system derived from Beilinson–Kato elements. The second part of the paper is devoted to the proof of these results.

In [Kat04] Kato constructed an Euler system for T (viewed as a $G_{\mathbb{Q}}$-representation) building on Siegel units on the modular curve of level N. Let $\mathcal{L}_{\mathrm{Kato}}$ be the set of primes $\ell \nmid Np$ such that

$$I_\ell := (\ell - 1, a_\ell - \ell - 1) \subset p^k \mathbb{Z}_p$$

for some $k > 0$ (in other words, $\ell \equiv 1 \pmod{p^k}$ and $a_\ell \equiv \ell + 1 \pmod{p^k}$), and let $\mathcal{N}_{\mathrm{Kato}}$ be the set of squarefree products of primes in $\mathcal{L}_{\mathrm{Kato}}$. For $n \in \mathcal{N}_{\mathrm{Kato}}$, let

$$I_n := \sum_{\ell | n} I_\ell$$

for $n > 1$, and put $I_1 := \{0\}$. By the process of Kolyvagin derivatives, from Kato's Euler system one obtains a system of cohomology classes

$$\left\{\kappa_n^{\mathrm{Kato}} \in \mathrm{H}^1(\mathbb{Q}, T/I_n T) \,:\, n \in \mathcal{N}_{\mathrm{Kato}}\right\}$$

forming a Kolyvagin system for T in the sense of Mazur–Rubin (see [MR04, Thm. 3.2.4]).

In this setting our main result is the following.

Theorem C (Non-vanishing of Kato's Kolyvagin system)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be an odd prime of good ordinary reduction for E such that $E(\mathbb{Q})[p] = 0$. Assume that the rational cyclotomic Main Conjecture 3.2.4 holds. Then*

$$\textit{there exists } n \in \mathcal{N}_{\mathrm{Kato}} \textit{ such that } \kappa_n^{\mathrm{Kato}} \neq 0.$$

In particular, $\{\kappa_n^{\mathrm{Kato}}\} \neq 0$ in both of the following cases:

- *E admits a rational p-isogeny with kernel $\mathbb{F}_p(\phi) \subset E[p]$, where $\phi : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ is a character such that $\phi|_{G_p} \neq \mathbb{1}, \omega$.*
- *$p > 3$ satisfies (irr).*

The 'In particular' part relies on the cases of Conjecture 3.2.4 established in [Kat04, CGS23] for Eisenstein p and in [Kat04, SU14, Wan15] for non-Eisenstein p.

We now describe an application of Theorem C. Similarly as in the Heegner point case, for any $n \in \mathcal{N}_{\mathrm{Kato}}$, define the order of vanishing of the Kolyvagin system κ^{Kato} by

$$\mathrm{ord}(\kappa^{\mathrm{Kato}}) := \min\{r :\ \text{there exists } n \in \mathcal{N}_{\mathrm{Kato}} \text{ with } \nu(n) = r \text{ such that } \kappa_n^{\mathrm{Kato}} \neq 0\}.$$

Let $\mathrm{H}^1_{\mathrm{str}}(\mathbb{Q}, E[p^\infty])$ denote the Selmer group for $E[p^\infty]$ obtained by imposing the strict local condition at p (see §3.1). Let

$$r_{\mathrm{str}}(E/\mathbb{Q}) = \mathrm{corank}_{\mathbb{Z}_p}\left(\mathrm{H}^1_{\mathrm{str}}(\mathbb{Q}, E[p^\infty])\right).$$

Combining the theorem above with [MR04, Theorem 5.2.12(v)], we obtain an analogue of Corollary A for Kato's Kolyvagin system.

Corollary C. *For E and p as in Theorem C, we have*

$$\mathrm{ord}(\kappa^{\mathrm{Kato}}) = r_{\mathrm{str}}(E/\mathbb{Q}).$$

The divisibility index $\mathscr{M}_\infty^{\mathrm{Kato}}$ of $\{\kappa_n^{\mathrm{Kato}}\}$ was studied by Mazur and Rubin [MR04, §6.2], who showed that if $\mathrm{ord}_p(c_\ell) > 0$ for some prime $\ell | N$, then $\mathscr{M}_\infty^{\mathrm{Kato}} > 0$. This was refined by Büyükboduk [Buy09], who showed that $\mathscr{M}_\infty^{\mathrm{Kato}} \geq \mathrm{ord}_p(c_\ell)$ for any prime $\ell | N$. Our approach to Theorem C also leads to a proof of the conjecture [Kim22b, Conj. 1.10] of Kim:

$$\mathscr{M}_\infty^{\mathrm{Kato}} = \sum_{\ell | N} \mathrm{ord}_p(c_\ell)$$

under some hypotheses (see Remark 3.3.4; these also include that π is p-optimal).

0.2. **Strategy.** Let $\Gamma = \mathrm{Gal}(K_\infty/K)$ be the Galois group of the anticyclotomic $\mathbb{Z}_p$-extension of K, and denote by $\Lambda = \mathbb{Z}_p[[\Gamma]]$ the anticyclotomic Iwasawa algebra. The key ingredients in the proof of Theorem A are:

(a) The non-vanishing of the base class $\boldsymbol{\kappa}_1^{\mathrm{Heeg}}$ of the Λ-*adic* Heegner point Kolyvagin system (i.e., the proof by Cornut and Vastal of Mazur's conjecture).

(b) Letting $\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)$ be the specialisation of $\boldsymbol{\kappa}_1^{\mathrm{Heeg}}$ at a character α of Γ with $\alpha \equiv 1 \pmod{p^m}$ for suitable $m \gg 0$ such that

$$\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha) \neq 0, \tag{0.3}$$

an estimate on the divisibility index of $\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)$ in terms of Tamagawa numbers and the Shafarevich–Tate group of the twist of E/K by α.

(c) The Kolyvagin system bound with controlled error terms obtained in [CGS23].

Most of the work in the first part of the paper goes into the proof of (b), which we deduce from the explicit reciprocity law[2] for $\boldsymbol{\kappa}_1^{\mathrm{Heeg}}$ in [CH18] and an extension of the anticyclotomic control theorem in [JSW17] allowing character twists. Together with a congruence relation between $\boldsymbol{\kappa}_n^{\mathrm{Heeg}}(\alpha)$ and κ_n^{Heeg}, the results (a)–(c) lead to a proof of Theorem A.

To approach the refined form of Kolyvagin's conjecture as in Theorem B, we replace the Kolyvagin system bound in (c) with an *exact formula* for the size of the above Tate–Shafarevich group in terms of the divisibility index of $\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)$ and the divisibility of the system $\{\boldsymbol{\kappa}_n^{\mathrm{Heeg}}(\alpha)\}_n$, generalising a consequence of the structure theorem [Kol91, Thm. 1] in the case $\alpha = 1$. We emphasize that our result applies to the twists of E by any anticyclotomic character α not necessarily p-adically close to the trivial one. Relating the index of divisibility of $\{\boldsymbol{\kappa}_n^{\mathrm{Heeg}}(\alpha)\}_n$ to that of $\{\kappa_n^{\mathrm{Heeg}}\}_n$ gives Theorem B.

The proof of Theorem C proceeds along similar lines. The analogue of (a) follows from results of Rohrlich and Kato, and we deduce the analogue of (b) from Kato's explicit reciprocity law and a twisted variant of the Euler characteristic computation originally due to Schneider and Perrin-Riou. The analogue of (c) in the setting of Kato's Euler system requires more work; we deduce it from the results developed in the last section of the paper that extend the Kolyvagin system bound of Mazur and Rubin [MR04] to a more general setting, allowing in particular for Eisenstein primes, a result that may be of independent interest.

Finally, we note that the links established in this paper between non-triviality of a Kolyvagin system (horizontal variation), and Iwasawa theory (vertical variation) of elliptic curves seem amenable to generalisations, which we plan to explore in the near future.

0.3. **Relation to previous works.**

Comparison with [Zha14b, Swe20]. The approach used by W. Zhang in his breakthrough work on Kolyvagin's conjecture is based on the principle of level-raising and rank-lowering, where rank refers to that of an associated mod p Selmer group; this was extended by N. Sweeting to mod p^m Selmer groups for large m. The approach proceeds by induction on the rank, the base case being: the triviality of the mod p Selmer group associated to a weight two elliptic newform implies the p-indivisibility of the algebraic part of the associated central L-value. This rank zero implication is a consequence of the (integral) cyclotomic Main Conjecture for the newform, as established by Skinner and Urban [SU14] under the hypotheses of [Zha14b] (by working mod p^m, some of the ramification hypotheses were removed in [Swe20]). It is precisely at this stage that Iwasawa theory enters into the approach of W. Zhang, albeit only implicitly. In contrast, the strategy in this paper is inherently Iwasawa-theoretic, based on the variation of Heegner points along the anticyclotomic $\mathbb{Z}_p$-extension. Moreover, a rational Main Conjecture suffices for its implementation. The approach of [Zha14b, Swe20] essentially excludes the Eisenstein case. However, while the results of this paper on Kolyvagin's conjecture are for p split in K, the results of [Zha14b, Swe20] apply also when p is inert in K.

Comparison with [Kim22a, Kim22b]. In the cases where (sur) holds, results similar to Theorems A and C are obtained by C.-H. Kim [Kim22a, Kim22b]: he proves that if the anticyclotomic (resp. cyclotomic) Main Conjecture holds at the trivial character, then the system $\{\kappa_n^{\mathrm{Heeg}}\}$ (resp. $\{\kappa_n^{\mathrm{Kato}}\}$) is non-trivial. To draw a parallel with our approach, while the ingredient (a) is common, his proof interestingly replaces our ingredients (b) and (c) with a structure theorem for Selmer groups in terms of divisibility indices of certain specialisations of Λ-adic classes. In contrast, under (sur) our approach also leads to a proof of the refined Kolyvagin conjecture and its cyclotomic analogue.

[2]This is a Λ-adic avatar of the Bertolini–Darmon–Prasanna formula [BDP13].

Acknowledgements. We thank Kâzim Büyükboduk, Masataka Chida, Christophe Cornut, Shinichi Kobayashi and Wei Zhang for helpful discussions. We also thank Chan-Ho Kim for his interest in our work, and his comments on an earlier draft. During the preparation of this paper, A.B. was partially supported by the NSF grants DMS-2303864 and DMS-2302064; F.C. was partially supported by the NSF grant DMS-2101458; C.S. was partially supported by the Simons Investigator Grant #376203 from the Simons Foundation and by the NSF grant DMS-1901985. This work was partially supported by the National Science Foundation under Grant No. DMS-1928930 while the authors were in residence at the Simons Laufer Mathematical Sciences Institute in Berkeley, California during the Spring 2023 semester.

1. Heegner points and anticyclotomic Iwasawa theory

1.1. The Kolyvagin system of Heegner points.

In this section we recall the construction of the classes $\kappa_n = \kappa_n^{\rm Heeg} \in {\rm H}^1(K, T/I_nT)$ and of their Iwasawa-theoretic analogues. See [How04a, §1.7,§2.3] for more details.

1.1.1. *Selmer structures.* Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, let $p \nmid 2N$ be a prime of good ordinary reduction for E, and let K be an imaginary quadratic field of discriminant D_K prime to Np. We assume that the triple (E, p, K) satisfies hypotheses (Heeg), (disc), and (tor) from the Introduction.

Let $\Gamma = {\rm Gal}(K_\infty/K)$ be the Galois group of the anticyclotomic $\mathbb{Z}_p$-extension of K and $\alpha : \Gamma \to \mathbb{Z}_p^\times$ a character. Let $\rho_E : G_\mathbb{Q} \to {\rm Aut}_{\mathbb{Z}_p}(T_pE)$ give the action of $G_\mathbb{Q}$ on the p-adic Tate module of E and consider the G_K-modules

$$T_\alpha := T_pE \otimes \mathbb{Z}_p(\alpha), \quad V_\alpha := T_\alpha \otimes \mathbb{Q}_p, \quad W_\alpha := T_\alpha \otimes \mathbb{Q}_p/\mathbb{Z}_p \simeq V_\alpha/T_\alpha,$$

where $\mathbb{Z}_p(\alpha)$ is the free $\mathbb{Z}_p$-module of rank one on which G_K acts via the projection $G_K \twoheadrightarrow \Gamma$ composed with α, and the G_K-action on T_α is via $\rho_\alpha = \rho_E \otimes \alpha$. For $k > 0$ let $T_\alpha^{(k)} = T_\alpha/p^kT_\alpha$; this is identified with $W_\alpha[p^k] = E[p^k] \otimes \mathbb{Z}_p(\alpha)$ via $T_\alpha \ni a \mapsto a \otimes \frac{1}{p^k} \in W_\alpha$.

A *Selmer structure* $\mathcal{F}$ on any of the G_K-modules $M = T_\alpha, V_\alpha, W_\alpha, T_\alpha^{(k)}$ is a finite set $\Sigma = \Sigma(\mathcal{F})$ of places of K containing ∞, the primes above p, and the primes where T_α is ramified, together with a choice of $\mathbb{Z}_p$-submodules ("local conditions") ${\rm H}^1_\mathcal{F}(K_w, M) \subset {\rm H}^1(K_w, M)$ for every $w \in \Sigma$. The associated *Selmer group* is then defined by

$${\rm H}^1_\mathcal{F}(K, M) := \ker\biggl\{{\rm H}^1(K^\Sigma/K, M) \to \prod_{w\in\Sigma} \frac{{\rm H}^1(K_w, M)}{{\rm H}^1_\mathcal{F}(K_w, M)}\biggr\},$$

where K^Σ is the maximal extension of K unramified outside Σ.

We recall the definition of the local conditions of interest in this section:

- For a finite prime $w \nmid p$, the *finite* (or *unramified*) local condition for V_α is

  $${\rm H}^1_f(K_w, V_\alpha) := \ker\bigl\{{\rm H}^1(K_w, V_\alpha) \to {\rm H}^1(K_w^{\rm ur}, V_\alpha)\bigr\};$$

  the corresponding local conditions ${\rm H}^1_f(K_w, T_\alpha)$ and ${\rm H}^1_f(K_w, W_\alpha)$ are defined to be the inverse image and the image, respectively, of ${\rm H}^1_f(K_w, V_\alpha)$ under the natural maps

  $$ {\rm H}^1(K_w, T_\alpha) \to {\rm H}^1(K_w, V_\alpha) \to {\rm H}^1(K_w, W_\alpha). \tag{1.1}$$

  Similarly, the local condition ${\rm H}^1_f(K_w, T_\alpha^{(k)})$ is the preimage of ${\rm H}^1_f(K_w, W_\alpha)$ under the natural map ${\rm H}^1(K_w, T_\alpha^{(k)}) \twoheadrightarrow {\rm H}^1(K_w, W_\alpha)[p^k]$. If T_α is not ramified at w, then all these are just the submodules of unramified classes (see also Remark 1.1.1 below).
- Denote by $\mathcal{L}_0$ the set of rational primes $\ell \neq p$ such that
  - ℓ is inert in K,
  - T_pE is unramified at ℓ,
  - $p \mid \ell + 1$.

  Letting $K[\ell]$ be the ring class field of K of conductor ℓ, define the *transverse* local condition at $\lambda|\ell \in \mathcal{L}_0$ by

  $${\rm H}^1_{\rm tr}(K_\lambda, T_\alpha^{(k)}) := \ker\bigl\{{\rm H}^1(K_\lambda, T_\alpha^{(k)}) \to {\rm H}^1(K[\ell]_{\lambda'}, T_\alpha^{(k)})\bigr\},$$

  where $K[\ell]_{\lambda'}$ is the completion of $K[\ell]$ at any prime λ' above λ and $k > 0$ is any integer such that $p^k \mid \ell + 1$.

- For w a prime of K above p, set
$$\mathrm{Fil}_w^+(T_pE) := \ker\{T_pE \to T_p\tilde{E}\},$$
where $\tilde{E}$ is the reduction of E at w, and put
$$\mathrm{Fil}_w^+(T_\alpha) := \mathrm{Fil}_w^+(T_pE) \otimes \mathbb{Z}_p(\alpha), \quad \mathrm{Fil}_w^+(V_\alpha) := \mathrm{Fil}_w^+(T_\alpha) \otimes \mathbb{Q}_p.$$
The *ordinary* local condition for V_α is defined by
$$\mathrm{H}^1_{\mathrm{ord}}(K_w, V_\alpha) := \mathrm{im}\{\mathrm{H}^1(K_w, \mathrm{Fil}_w^+(V_\alpha)) \to \mathrm{H}^1(K_w, V_\alpha)\}.$$
Similarly as before, the corresponding local conditions $\mathrm{H}^1_{\mathrm{ord}}(K_w, T_\alpha)$ and $\mathrm{H}^1_{\mathrm{ord}}(K_w, W_\alpha)$ are defined to be the inverse image and the image, respectively, of $\mathrm{H}^1_{\mathrm{ord}}(K_w, V_\alpha)$ under the natural maps (1.1), and $\mathrm{H}^1_{\mathrm{ord}}(K_w, T_\alpha^{(k)})$ is the preimage of $\mathrm{H}^1_{\mathrm{ord}}(K_w, W_\alpha)$.

Remark 1.1.1. For $w \nmid p$, it follows immediately from the definitions that $\mathrm{H}^1_f(K_w, W_\alpha)$ is contained in
$$\mathrm{H}^1_{\mathrm{ur}}(K_w, W_\alpha) := \ker\{\mathrm{H}^1(K_w, W_\alpha) \to \mathrm{H}^1(K_w^{\mathrm{ur}}, W_\alpha)\}.$$
In fact, for V_α one even has $\mathrm{H}^1_f(K_w, V_\alpha) = 0$, and therefore $\mathrm{H}^1_f(K_w, W_\alpha)$ is also trivial. Thus the p-part of the Tamagawa number of W_α is given by
$$c_w^{(p)}(W_\alpha) := [\mathrm{H}^1_{\mathrm{ur}}(K_w, W_\alpha) \colon \mathrm{H}^1_f(K_w, W_\alpha)] = \#\mathrm{H}^1_{\mathrm{ur}}(K_w, W_\alpha).$$

Definition 1.1.2. The *ordinary* Selmer structure $\mathcal{F}_{\mathrm{ord}}$ on V_α is defined by taking $\Sigma(\mathcal{F}_{\mathrm{ord}}) = \{w \mid pN\}$ and
$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K_w, V_\alpha) := \begin{cases} \mathrm{H}^1_{\mathrm{ord}}(K_w, V_\alpha) & \text{if } w \mid p, \\ \mathrm{H}^1_f(K_w, V_\alpha) & \text{else.} \end{cases}$$
Let $\mathcal{F}_{\mathrm{ord}}$ also denote the resulting Selmer structure on T_α, W_α, and $T_\alpha^{(k)}$.

Remark 1.1.3. For $\alpha = \mathbb{1}$, one knows that $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, W_\alpha) = \mathrm{Sel}_{p^\infty}(E/K)$ (see e.g. [Rub00, Prop. 1.6.8]).

Given a subset $\mathcal{L} \subset \mathcal{L}_0$, we let $\mathcal{N}(\mathcal{L})$ be the set of squarefree products of primes $\ell \in \mathcal{L}$; when the choice of $\mathcal{L}$ is irrelevant or clear from the context, we shall simply denote this by $\mathcal{N}$. Given a Selmer structure $\mathcal{F}$ on $T_\alpha^{(k)}$, and $n \in \mathcal{N}$, we define the modified Selmer structure $\mathcal{F}(n)$ by
$$\mathrm{H}^1_{\mathcal{F}(n)}(K_\lambda, T_\alpha^{(k)}) = \begin{cases} \mathrm{H}^1_{\mathrm{tr}}(K_\lambda, T_\alpha^{(k)}) & \text{if } \lambda \mid n, \\ \mathrm{H}^1_{\mathcal{F}}(K_w, T_\alpha^{(k)}) & \text{if } \lambda \nmid n. \end{cases}$$

1.1.2. *The Kolyvagin system of Heegner points.* Let $T = T_{\mathbb{1}} = T_pE$. We start by defining the derived Heegner classes $\kappa_{n,k}^{\mathrm{Heeg}} \in \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)})$, where $T^{(k)} = T/p^kT \simeq E[p^k]$ and $k \leq M(n)$.

We recall the following result.

Lemma 1.1.4 ([CGLS22, Lem. 3.3.1])**.** *For every $n \in \mathcal{N}$ and $0 < i \leq k \leq M(n)$ there are natural isomorphisms*
$$\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(i)}) = \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)}/p^iT^{(k)}) \xrightarrow{\sim} \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)}[p^i]) \xrightarrow{\sim} \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)})[p^i]$$
induced by the maps $T^{(i)} = T^{(k)}/p^iT^{(k)} \xrightarrow{p^{k-i}} T^{(k)}[p^i] \to T^{(k)}$.

We first define $\kappa_n^{\mathrm{Heeg}} = \kappa_{n,M(n)}^{\mathrm{Heeg}} \in \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(M(n))})$; the classes $\kappa_{n,k}^{\mathrm{Heeg}}$ for $k < M(n)$ are then defined to be the pre-image of $p^{M(n)-k}\kappa_n^{\mathrm{Heeg}}$ under the isomorphism $\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)}) \xrightarrow{\sim} \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(M(n))})[p^k]$ of Lemma 1.1.4 above.

Put
$$\mathcal{L}_{\mathrm{Heeg}} := \{\ell \in \mathcal{L}_0 : \ a_\ell \equiv \ell + 1 \equiv 0 \ (\mathrm{mod}\, p)\},$$
where $a_\ell = \ell + 1 - \#\tilde{E}(\mathbb{F}_\ell)$. For $\ell \in \mathcal{L}_{\mathrm{Heeg}}$ we let $G_\ell = \mathrm{Gal}(K[\ell]/K[1])$, and for $n \in \mathcal{N}_{\mathrm{Heeg}} := \mathcal{N}(\mathcal{L}_{\mathrm{Heeg}})$ we set $\mathcal{G}(n) = \mathrm{Gal}(K[n]/K)$ and $G(n) = \prod_{\ell \mid n} G_\ell$. Then for m dividing n we have the natural identification
$$\mathrm{Gal}(K[n]/K[m]) \simeq \prod_{\ell \mid (n/m)} G_\ell = G(n/m)$$

induced by the projections $\mathrm{Gal}(K[n]/K[m]) \twoheadrightarrow G_\ell$. The Kolyvagin derivative operator $D_\ell \in \mathbb{Z}_p[G_\ell)]$ is defined by

$$D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i, \tag{1.2}$$

where σ_ℓ is a fixed generator of G_ℓ. Let $D_n = \prod_{\ell \mid n} D_\ell \in \mathbb{Z}_p[G(n)]$.

Recall the Heegner points $P[n] \in E(K[n])$ in (0.2). Choosing a set S of representatives for the cosets $\mathcal{G}(n)/G(n)$, one can show the inclusion

$$\tilde{\kappa}_n := \sum_{\sigma \in S} \sigma D_n(P[n]) \in \Big(E(K[n]) \big/ p^{M(n)} E(K[n])\Big)^{\mathcal{G}(n)}$$

(see [How04a, Lem. 1.7.1]). Hence, applying the Kummer map we may consider $\tilde{\kappa}_n \in \mathrm{H}^1(K[n], T^{(M(n))})^{\mathcal{G}(n)}$. Hypothesis (tor) ensures that the restriction map

$$\mathrm{H}^1(K, T^{(M(n))}) \to \mathrm{H}^1(K[n], T^{(M(n))})^{\mathcal{G}(n)}$$

is an isomorphism, and the derived Heegner class κ_n^{Heeg} is defined to be the unique class in $\mathrm{H}^1(K, T^{(M(n))})$ which restricts to the image of $\tilde{\kappa}_n$ in $\mathrm{H}^1(K[n], T^{(M(n))})^{\mathcal{G}(n)}$.

The classes κ_n^{Heeg} land in the n-transverse Selmer group $\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(M(n))})$ (see [How04a, Lem. 1.7.3]), and after a slight modification – which we still denote by κ_n^{Heeg} – the resulting collection of classes

$$\{\kappa_n^{\mathrm{Heeg}}\}_{n \in \mathcal{N}_{\mathrm{Heeg}}}$$

forms a *Kolyvagin system* for $(T, \mathcal{F}_{\mathrm{ord}}, \mathcal{L}_E)$ in the sense of [*op. cit.*, Def. 1.2.3].

1.1.3. *The Λ-adic Kolyvagin system.* Let K_∞/K be the anticyclotomic $\mathbb{Z}_p$-extension, let $\Gamma = \mathrm{Gal}(K_\infty/K)$ and $\Lambda = \mathbb{Z}_p[[\Gamma]]$ the anticyclotomic Iwasawa algebra. Put

$$\mathbf{T} = T_pE \otimes_{\mathbb{Z}_p} \Lambda,$$

and consider the *ordinary* Selmer structure $\mathcal{F}_\Lambda$ on $\mathbf{T}$ given by

$$\mathrm{H}^1_{\mathcal{F}_\Lambda}(K_w, \mathbf{T}) = \begin{cases} \mathrm{im}\{\mathrm{H}^1(K_w, \mathrm{Fil}_w^+(T_pE) \otimes \Lambda) \to \mathrm{H}^1(K_w, \mathbf{T})\} & \text{if } w \mid p, \\ \mathrm{H}^1_{\mathrm{ur}}(K_w, \mathbf{T}) & \text{else.} \end{cases}$$

We now briefly recall the construction of the Λ-adic Heegner point Kolyvagin system, which is a collection of classes $\boldsymbol{\kappa}_n^{\mathrm{Heeg}} \in \mathrm{H}^1(K, \mathbf{T}/p^{M(n)}\mathbf{T}) = \mathrm{H}^1(K, E[p^{M(n)}] \otimes \Lambda)$.

Let K_k be the subfield of K_∞ of degree p^k over K. For each $n \in \mathcal{N}_{\mathrm{Heeg}}$ as above set

$$P_k[n] := \mathrm{Norm}_{K[np^{d(k)}]/K_k[n]}(P[np^{d(k)}]) \in E(K_k[n]),$$

where $d(k) = \min\{d \in \mathbb{Z}_{\geq 0} \colon K_k \subset K[p^{d(k)}]\}$, and $K_k[n]$ is the compositum of K_k and $K[n]$. Let $H_k[n]$ be the $\mathbb{Z}_p[\mathrm{Gal}(K_k[n]/K)]$-submodule of $E(K_k[n]) \otimes \mathbb{Z}_p$ generated by $P_j[n]$ for $j \leq k$, and consider the $\Lambda[\mathcal{G}(n)]$-module

$$\mathbf{H}[n] = \varprojlim_k H_k[n],$$

where the limit is taken with respect to the norm maps. By [How04a, Lem. 2.3.3], there is a family

$$\{Q[n] = \varprojlim_k Q_k[n] \in \mathbf{H}[n]\}_{n \in \mathcal{N}}$$

such that

$$Q_0[n] = \Phi P[n], \quad \text{where } \Phi = \begin{cases} (p - a_p\sigma_p + \sigma_p^2)(p - a_p\sigma_p^* + \sigma_p^{*2}) & p \text{ splits in } K, \\ (p+1)^2 - a_p & p \text{ inert in } K. \end{cases} \tag{1.3}$$

Here, when p splits in K, σ_p and σ_p^* are the Frobenius elements in $\mathcal{G}(n)$ of the primes above p in K.

Letting $D_n \in \mathbb{Z}_p[G(n)]$ be the Kolyvagin's derivative operators defined in (1.2), and choosing a set S of representatives for $\mathcal{G}(n)/G(n)$, the class $\boldsymbol{\kappa}_n^{\mathrm{Heeg}} \in \mathrm{H}^1(K, \mathbf{T}/I_n\mathbf{T})$ is defined as the natural image of

$$\tilde{\boldsymbol{\kappa}}_n = \sum_{\sigma \in S} \sigma D_n(Q[n]) \in \mathbf{H}[n]$$

under the composite map

$$\big(\mathbf{H}[n]/p^{M(n)}\mathbf{H}[n]\big)^{\mathcal{G}(n)} \xrightarrow{\delta(n)} \mathrm{H}^1(K[n],\mathbf{T}/p^{M(n)}\mathbf{T})^{\mathcal{G}(n)} \xleftarrow{\simeq} \mathrm{H}^1(K,\mathbf{T}/p^{M(n)}\mathbf{T}),$$

where $\delta(n)$ is induced by the limit of Kummer maps $\delta_k(n) : E(K_k[n])\otimes\mathbb{Z}_p \to \mathrm{H}^1(K_k[n],T)$, and the second arrow is given by restriction. The latter is an isomorphism since the extensions $K[n]$ and $\mathbb{Q}(E[p])$ are linearly disjoint, and $E(K_\infty)[p]=0$ by hypothesis (tor).

Finally, [How04a, Lem. 2.3.4] *et seq.* show that the classes $\boldsymbol{\kappa}_n^{\rm Heeg}$ land in $\mathrm{H}^1_{\mathcal{F}_\Lambda(n)}(K,\mathbf{T}/p^{M(n)}\mathbf{T})$ and they can be slightly modified - and still denoted $\boldsymbol{\kappa}_n^{\rm Heeg}$ - so that the result is a system $\boldsymbol{\kappa}^{\rm Hg}=\{\boldsymbol{\kappa}_n^{\rm Heeg}\}_{n\in\mathcal{N}_{\rm Heeg}}$ satisfying the Kolyvagin system relations. Here $\mathcal{F}_\Lambda(n)$ denotes the modification of the Selmer structure on $\mathbf{T}/p^{M(n)}\mathbf{T})$ induced from $\mathcal{F}_\Lambda$ that includes the obvious analog of the transverse local conditions at the primes $\ell\mid n$.

1.1.4. *Kolyvagin system for anticyclotomic twists.* We now consider a height one prime $\mathfrak{P}\subset\Lambda$ with $\mathfrak{P}\neq p\Lambda$, and denote by $R_{\mathfrak{P}}$ the integral closure of $\Lambda/\mathfrak{P}$. We let G_K act on $R_{\mathfrak{P}}$ by the character $\alpha_{\mathfrak{P}} : G_K \twoheadrightarrow \Gamma \to \Lambda \to R_{\mathfrak{P}}$, and consider

$$T_{\mathfrak{P}} = \mathbf{T}\otimes_\Lambda R_{\mathfrak{P}} = T_{\alpha_{\mathfrak{P}}}$$

with diagonal G_K-action. By Remark 1.2.4 and Lemma 2.2.7 in [How04a], the natural map induced by $\mathbf{T}\to T_{\mathfrak{P}}$ sends $\boldsymbol{\kappa}^{\rm Hg}$ to a Kolyvagin system for $T_{\mathfrak{P}}$ (for the Selmer structure $\mathcal{F}_{\rm ord}$ defined in §1.1.1), which we denote by $\{\boldsymbol{\kappa}_n^{\rm Heeg}(\alpha_{\mathfrak{P}})\}_{n\in\mathcal{N}_{\rm Heeg}}$. In general, $R_{\mathfrak{P}}$ may not be $\mathbb{Z}_p$ and the definitions in §1.1.1 have to be suitably modified. However, for the purposes of this paper we will only be interested in the case $\mathfrak{P}=(\gamma-\alpha(\gamma))$ where γ is a topological generator of Γ and $\alpha:\Gamma\to\mathbb{Z}_p^\times$ is a character. In this case $\alpha_{\mathfrak{P}}$ is just the composition of α and the projection $G_K\twoheadrightarrow\Gamma$, and we write

$$\{\boldsymbol{\kappa}_n^{\rm Heeg}(\alpha)\}_{n\in\mathcal{N}_{\rm Heeg}}$$

for the corresponding Kolyvagin system.

Lemma 1.1.5. *Suppose $\alpha\equiv 1 \pmod{p^m}$. For all $n\in\mathcal{N}_{\rm Heeg}$ with $M(n)\geq m$ we have the congruence*

$$\boldsymbol{\kappa}_n^{\rm Heeg}(\alpha) \equiv \begin{cases} (\alpha_p-1)^2(\beta_p-1)^2\kappa_n^{\rm Heeg} & p \text{ splits in } K \\ ((p+1)^2-a_p^2)\kappa_n^{\rm Heeg} & p \text{ inert in } K \end{cases} \pmod{p^m},$$

where α_p,β_p are the roots of the characteristic polynomial of the Frobenius at p, with α_p the p-adic unit root.

Proof. Let $\mathfrak{P}=(\gamma-\alpha(\gamma))$ and $\mathfrak{P}_0=(\gamma-1)$. The image of $Q[n]$ under the map on $\mathbf{H}[n]$ induced by the composition $\Lambda\to\Lambda/\mathfrak{P}\to(\Lambda/\mathfrak{P})/p^m\simeq\mathbb{Z}_p/p^m\mathbb{Z}_p$ is the same as the image induced by the composition $\Lambda\to\Lambda/\mathfrak{P}_0\to(\Lambda/\mathfrak{P}_0)/p^m\simeq\mathbb{Z}_p/p^m\mathbb{Z}_p$ (since both are given by quotienting by the ideal $(\gamma-1,p^m)$). By (1.3), the latter image is $\Phi P[n] \pmod{p^m}$ from which the result follows immediately by the constructions of $\boldsymbol{\kappa}_n^{\rm Heeg}$ and $\kappa_n^{\rm Heeg}$ and the definition of Φ. ☐

In particular, noting that $\mathrm{H}^1(K,T)$ is torsion-free as a consequence of (tor), Lemma 1.1.5 implies, combined with the Gross–Zagier formula [GZ86], that

$$\boldsymbol{\kappa}_1^{\rm Heeg}(\mathbb{1})\neq 0 \iff \mathrm{ord}_{s=1}L(E/K,s)=1.$$

More generally, without any conditions on the analytic rank of E/K, we have the following.

Theorem 1.1.6 (Cornut–Vatsal)**.** *For $m\gg 0$ and any $\alpha\equiv 1 \pmod{p^m}$, the class $\boldsymbol{\kappa}_1^{\rm Heeg}(\alpha)$ is non-zero.*

Proof. This is immediate from the main result of [Cor02] and [Vat03], showing that $\boldsymbol{\kappa}_1^{\rm Heeg}$ is not Λ-torsion. ☐

Remark 1.1.7. Based on an extension of the Bertolini–Darmon–Prasanna formula and the nonvanishing of the p-adic L-function $\mathcal{L}_p^{\rm BDP}(f/K)$ recalled in Theorem 1.2.1 below, one can give alternate proof of Theorem 1.1.6 when p splits in K (see [Bur20] and [CH18]).

1.2. **Anticyclotomic Iwasawa Main Conjecture.** We keep the hypotheses on (E, p, K) from the preceding section, and assume in addition that

$$p = v\bar{v} \text{ splits in } K, \tag{spl}$$

with v the prime of K above p induced by a fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Fix an integral ideal $\mathfrak{N} \subset \mathcal{O}_K$ with

$$\mathcal{O}_K/\mathfrak{N} \simeq \mathbb{Z}/N\mathbb{Z}.$$

In this section we show how a certain anticyclotomic Iwasawa Main Conjecture (see Conjecture 1.2.10) yields an expression for the divisibility index of the Kolyvagin systems $\{\boldsymbol{\kappa}_n^{\mathrm{Heeg}}(\alpha)\}_{n\in\mathcal{N}_{\mathrm{Heeg}}}$, for $\alpha \equiv 1 \pmod{p^m}$ as above with $m \gg 0$, in terms of the Tamagawa numbers and the Shafarevich–Tate group of (a twist of) E.

Below we shall write $a \sim_p b$ to denote that a and b have the same p-adic valuation.

1.2.1. *p-adic L-function.* Let $f \in S_2(\Gamma_0(N))$ be the newform attached to E. Recall that $\Lambda = \mathbb{Z}_p[[\Gamma]]$ denotes the anticyclotomic Iwasawa algebra of K, and put $\Lambda^{\mathrm{ur}} = \Lambda\hat{\otimes}_{\mathbb{Z}_p}\mathbb{Z}_p^{\mathrm{ur}}$, where $\mathbb{Z}_p^{\mathrm{ur}}$ is the completion of the ring of integers of the maximal unramified extension of $\mathbb{Q}_p$.

The next result refines the construction of a continuous anticyclototomic p-adic L-function due to Bertolini–Darmon–Prasanna [BDP13]. The p-adic measure underlying their construction was explicitly given in [CH18], whose formulation we follow.

Theorem 1.2.1. *There exists an element $\mathcal{L}_p^{\mathrm{BDP}}(f/K) \in \Lambda^{\mathrm{ur}}$ characterised by the following interpolation property: For every character ξ of Γ crystalline at both v and $\bar{v}$ and corresponding to a Hecke character of K of infinity type $(n, -n)$ with $n \in \mathbb{Z}_{>0}$ and $n \equiv 0 \pmod{p-1}$, we have*

$$\mathcal{L}_p^{\mathrm{BDP}}(f/K)^2(\xi) = \frac{\Omega_p^{4n}}{\Omega_\infty^{4n}} \cdot \frac{\Gamma(n)\Gamma(n+1)\xi(\mathfrak{N}^{-1})}{4(2\pi)^{2n+1}\sqrt{D_K}^{2n-1}} \cdot \left(1 - a_p\xi(\bar{v})p^{-1} + \xi(\bar{v})^2p^{-1}\right)^2 \cdot L(f/K, \xi, 1),$$

where Ω_p and Ω_∞ are CM periods attached to K as in [CH18, §2.5]*. Moreover, $\mathcal{L}_p^{\mathrm{BDP}}(f/K)$ is nonzero.*

Proof. This follows from results contained in [CH18, §3], as explained in the proof [CGLS22, Thm. 2.1.1]. □

Definition 1.2.2. A collection of characters as in Theorem 1.2.1 with n essentially arbitrary can be defined as follows. Let $u \in 1 + p\mathbb{Z}_p = 1 + p\mathcal{O}_{K_v} \subset \mathcal{O}_{K_v}^\times$ be a $\mathbb{Z}_p$-generator and let $\gamma \in \Gamma$ be a topological generator such that there exists $h > 0$ a power of p for which γ^h is the image of u under the reciprocity map of class field theory. For $n \in \mathbb{Z}$ such that $n \equiv 0 \pmod{p-1}$, let $\xi_n : \Gamma \to \mathbb{Z}_p^\times$ be the unique continuous character such $\xi_n(\gamma) = u^n$. Then the composition of ξ_n with the projection $G_K \twoheadrightarrow \Gamma$ is crystalline at v (and hence also $\bar{v}$) and the corresponding Hecke character of K has infinity type $(hn, -hn)$. For $m > 0$ we let

$$\alpha_m = \xi_{(p-1)p^{m-1}}.$$

Then $\alpha_m \equiv 1 \pmod{p^m}$.

Assume now that $E/\mathbb{Q}$ is an elliptic curve in the isogeny class attached to f having a modular parameterisation $\pi : X_0(N) \to E$ that identifies T_pE with T_f, where T_f is the quotient of $\mathrm{H}^1(Y_1(N), \mathbb{Z}_p(1))$ associated with f (cf. [Wut14, Prop. 8]); we use such a choice of π in the following. If (irr) holds, then π is p-optimal and π (and E) is uniquely determined up to a prime-to-p isogeny, and the exact choice of π has no effect on the formulas and relations below.

Let $\kappa_\infty \in \mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ be the Λ-adic class constructed in [CH18, §5.2]. As explained in [CGLS22, Remark 4.1.3], the class κ_∞ generates the same Λ-submodule of $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ as the base class $\boldsymbol{\kappa}_1^{\mathrm{Heeg}}$ of the Λ-adic Kolyvagin system $\boldsymbol{\kappa}^{\mathrm{Heeg}}$ associated to E. For any character $\alpha : \Gamma \to \mathbb{Z}_p^\times$, put $T_\alpha = T_pE \otimes \mathbb{Z}_p(\alpha)$ and denote by

$$\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha) \in \mathrm{H}^1(K, T_\alpha)$$

the image of $\boldsymbol{\kappa}_1^{\mathrm{Heeg}}$ under the specialisation map $\mathrm{H}^1(K, \mathbf{T}) \to \mathrm{H}^1(K, T_\alpha)$.

As recalled in [CH18], there exists a Λ-module map $\mathscr{L}_{T^+} : \mathrm{H}^1(K_v, \mathrm{Fil}_v^+T \otimes_{\mathbb{Z}_p} \Lambda) \to \Lambda^{\mathrm{ur}}$ (a 'big logarithm' map) such that

$$\mathscr{L}_{T^+}(\mathrm{loc}_v(\boldsymbol{\kappa}_1^{\mathrm{Heeg}})) = \mathcal{L}_p^{\mathrm{BDP}}(f/K).$$

In the setting of this paper, $\mathscr{L}_{T^+}$ induces an isomorphism $\mathrm{H}^1(K_v, \mathrm{Fil}_v^+T \otimes_{\mathbb{Z}_p} \Lambda) \otimes_\Lambda \Lambda^{\mathrm{ur}} \xrightarrow{\sim} \Lambda^{\mathrm{ur}}$. From this we deduce the following.

Lemma 1.2.3. *Assume $E/\mathbb{Q}$ is as above. Let $\alpha : \Gamma \to \mathbb{Z}_p^\times$ be an anticyclotomic character as in Theorem 1.2.1 with $n \geq 0$ and such that $\mathcal{L}_p^{\mathrm{BDP}}(f/K)(\alpha^{-1}) \neq 0$. If $\alpha \equiv 1 \pmod{p^m}$ with $m \gg 0$, then*

$$p^{t_\alpha} \cdot \#\mathrm{H}^0(\mathbb{Q}_p, E[p^\infty]) = \#\big(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha)/\mathbb{Z}_p \cdot \boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)\big) \cdot \#\mathrm{coker}(\mathrm{loc}_v),$$

where

$$t_\alpha = \mathrm{length}_{\mathbb{Z}_p^{\mathrm{ur}}}\big(\mathbb{Z}_p^{\mathrm{ur}}/\mathcal{L}_p^{\mathrm{BDP}}(f/K)(\alpha^{-1})\big)$$

and $\mathrm{loc}_v : \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha) \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K_v, T_\alpha)/\mathrm{H}^1(K_v, T_\alpha)_{\mathrm{tors}} =: \mathrm{H}^1(K_v, \mathrm{Fil}_v^+ T_\alpha)_{/\mathrm{tors}}$.

Proof. The nonvanishing of $\mathcal{L}_p^{\mathrm{BDP}}(f/K)(\alpha^{-1})$ implies that $\mathrm{loc}_v(\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha))$ has nonzero image in $\mathrm{H}^1(K_v, \mathrm{Fil}_v^+ T_\alpha)$ (note that the latter is a torsion-free $\mathbb{Z}_p$-module). Furthermore the cokernel of the specialization map $\mathrm{H}^1(K_v, \mathrm{Fil}_v^+ T \otimes_{\mathbb{Z}_p} \Lambda) \to \mathrm{H}^1(K_v, \mathrm{Fil}_v^+ T_\alpha)$ is naturally isomorphic to $\mathrm{H}^2(K_v, \mathrm{Fil}_v^+ T \otimes_{\mathbb{Z}_p} \Lambda)[\gamma - \alpha(\gamma)]$, whose order is easily computed via local duality to equal $\#\mathrm{H}^0(\mathbb{Q}_p, E[p^\infty])$ if $m \gg 0$. As $\mathrm{H}^1(K_v, \mathrm{Fil}_v^+ T_\alpha)$ is a torsion-free $\mathbb{Z}_p$-module of rank one, it follows that

$$\#\big(\mathrm{H}^1(K_v, \mathrm{Fil}_v^+ T_\alpha)/\mathbb{Z}_p \, \mathrm{loc}_v(\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha))\big) = p^{t_\alpha} \cdot \#\mathrm{H}^0(\mathbb{Q}_p, E[p^\infty]).$$

On the other hand, since $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha)$ is also a torsion-free $\mathbb{Z}_p$-module of rank one, loc_v induces an injection $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha)/\mathbb{Z}_p \boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha) \hookrightarrow \mathrm{H}^1(K_v, \mathrm{Fil}_v^+ T_\alpha)/\mathbb{Z}_p \, \mathrm{loc}_v(\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha))$, from which it follows that

$$\#\big(\mathrm{H}^1(K_v, \mathrm{Fil}_v^+ T_\alpha)/\mathbb{Z}_p \, \mathrm{loc}_v(\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha))\big) = \#\big(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha)/\mathbb{Z}_p \boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)\big) \cdot \#\mathrm{coker}(\mathrm{loc}_v).$$

Combining the last two displayed equations yields the lemma. □

Remark 1.2.4. In the case that $\alpha = \mathbb{1}$, then $\kappa_1^{\mathrm{Heeg}}(\alpha) = (1-\alpha_p)^2(1-\beta_p)^2 \kappa_1^{\mathrm{Heeg}}$ and — noting that $\#(\mathbb{Z}_p/(1-\alpha_p)(1-\beta_p)) = \#(\mathbb{Z}_p/(1-\alpha_p^{-1})) = \#\mathrm{H}^0(\mathbb{Q}_p, E[p^\infty])$ — the formula in the Lemma can be rewritten as

$$\#\left(\mathbb{Z}_p/\mathcal{L}_p^{\mathrm{BDP}}(f/K)(\mathbb{1})\right) = \#\big(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha)/\mathbb{Z}_p \cdot \boldsymbol{\kappa}_1^{\mathrm{Heeg}}\big) \cdot \#\mathrm{coker}(\mathrm{loc}_v) \cdot \#\mathrm{H}^0(\mathbb{Q}_p, E[p^\infty]).$$

Lemma 1.2.3 links the specialisation of the p-adic L-function at α with the based class in the Heegner point Kolyvagin system for a specific elliptic curve (up to prime to p isogeny) associated with a specific choice of lattice, namely the curve $E_\bullet$ associated with the lattice T_f. The following lemma tells us that we can rephrase it in terms of the corresponding class attached to any elliptic curve in the isogeny class associated with f. Let $E/\mathbb{Q}$ be a such a curve. We write $\boldsymbol{\kappa}_{1,f}^{\mathrm{Heeg}}(\alpha)$ for the classes $\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)$ associate as above with the lattice T_f and $\boldsymbol{\kappa}_{1,E}^{\mathrm{Heeg}}(\alpha)$ for the ones for $T = T_pE$.

Lemma 1.2.5. *Let $E/\mathbb{Q}$ be any elliptic curve in the isogeny class associated with f, and let $T = T_pE$. Assume that $\boldsymbol{\kappa}_{1,f}^{\mathrm{Heeg}}(\alpha) \neq 0$. Consider the map*

$$\mathrm{loc}_{v,E} : \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha) \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K_v, T_\alpha)/\mathrm{H}^1(K_v, T_\alpha)_{\mathrm{tors}} =: \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K_v, T_\alpha)_{/\mathrm{tors}},$$

and let $\mathrm{loc}_{v,f}$ be the analogous map with T_f in place of T. Then

$$\#\big(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_{f,\alpha})/\mathbb{Z}_p \cdot \boldsymbol{\kappa}_{1,f}^{\mathrm{Heeg}}(\alpha)\big) \cdot \#\mathrm{coker}(\mathrm{loc}_{v,f}) = \#\big(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha)/\mathbb{Z}_p \cdot \boldsymbol{\kappa}_{1,E}^{\mathrm{Heeg}}(\alpha)\big) \cdot \#\mathrm{coker}(\mathrm{loc}_{v,E}).$$

Proof. Let $E_\bullet$ be the elliptic curve as before such that T_pE is identifified with T_f. We may assume without loss of generality that E is *closer* than $E_\bullet$ to the optimal curve, i.e. the degree of the modular parametrisation for E is smaller than the one for $E_\bullet$. Then there is an étale isogeny $\psi : E \to E_\bullet$ such that the induced injective map

$$\psi : \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha) \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_{f,\alpha})$$

satisfies $\psi(\boldsymbol{\kappa}_{1,E}^{\mathrm{Heeg}}(\alpha)) = \boldsymbol{\kappa}_{1,f}^{\mathrm{Heeg}}(\alpha)$. Let $d \in \mathbb{Z}_{\geq 0}$ be such that $[\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_{f,\alpha}) : \psi(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha))] = p^d$. Since we are assuming that $\boldsymbol{\kappa}_{1,f}^{\mathrm{Heeg}}(\alpha) \neq 0$, we also have $\boldsymbol{\kappa}_{1,E}^{\mathrm{Heeg}}(\alpha) \neq 0$, and so by [CGS23, Thm. 5.5.1] that $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_{f,\alpha})$ and $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha)$ are both free of rank one. Hence

$$\#\big(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_{f,\alpha}))/\mathbb{Z}_p \cdot \boldsymbol{\kappa}_{1,f}(\alpha)\big) = p^d \cdot \#\big(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_{E,\alpha}))/\mathbb{Z}_p \cdot \boldsymbol{\kappa}_{1,E}(\alpha)\big). \tag{1.4}$$

Furthermore, since $\mathrm{Fil}_w^+(T_\alpha) = \mathrm{Fil}_w^+(T_{f,\alpha})$, we have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_{f,\alpha}) & \xrightarrow{\mathrm{loc}_{v,f}} & \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K_v, T_{f,\alpha})_{/\mathrm{tors}} \\ \psi\uparrow & & \| \\ \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha) & \xrightarrow{\mathrm{loc}_{v,E}} & \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K_v, T_\alpha)_{/\mathrm{tors}} \end{array}$$

We thus obtain $\mathrm{coker}(\mathrm{loc}_{v,E}) = \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K_v, T_{f,\alpha})_{/\mathrm{tors}}/\psi(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha)) = \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K_v, T_{f,\alpha})_{/\mathrm{tors}}/p^d\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_{f,\alpha})$, and hence the equality

$$\#\mathrm{coker}(\mathrm{loc}_{v,E}) = p^d \#\mathrm{coker}(\mathrm{loc}_{v,f}). \tag{1.5}$$

Combining (1.4) and (1.5) yields the desired result. □

1.2.2. *Anticyclotomic Selmer group.* Let Σ be a finite set of places of K containing ∞ and the primes dividing Np. We assume that all finite primes in Σ split in K. For a discrete $\mathbb{Z}_p$-module A, we let $A^\vee = \mathrm{Hom}_{\mathrm{cts}}(A, \mathbb{Q}/\mathbb{Z}_p)$ be the Pontryagin dual. Put

$$M := T_pE \otimes \Lambda^\vee,$$

where $\Lambda^\vee$ is equipped with a G_K-action via the inverse of the character $G_K \to \Lambda^\times$ arising from the projection $G_K \twoheadrightarrow \Gamma$.

Definition 1.2.6. Let $G_{K,\Sigma}$ denote the Galois group of the maximal extension of K unramified outside Σ. We define the *Greenberg Selmer group* of M as follows:

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M) = \ker\Big\{\mathrm{H}^1(G_{K,\Sigma}, M) \to \mathrm{H}^1(K_v, M) \times \prod_{w\in\Sigma, w\nmid p} \mathrm{H}^1(K_w, M)\Big\}.$$

We also put

$$\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty) := \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M)^\vee.$$

It is a standard fact that $\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty)$ is a finitely generated Λ-module. We next recall a twisted anticyclotomic variant of the Euler characteristic calculation for Selmer groups [Gre99, §4]. Here $E/\mathbb{Q}$ is any elliptic curve in the isogeny class associated with f, and we let $T = T_pE$.

Theorem 1.2.7 (Anticyclotomic control theorem at α)**.** *Let $\alpha : \Gamma \to \mathbb{Z}_p^\times$ be an anticyclotomic character as in Theorem 1.2.1 such that $\mathcal{L}_p^{\mathrm{BDP}}(f/K)(\alpha^{-1}) \neq 0$ and $\alpha \equiv 1 \pmod{p^m}$ with $m \gg 0$. Then $\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty)$ is Λ-torsion, and if $\mathcal{F}_E \in \Lambda$ generates $\mathrm{char}_\Lambda(\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty))$, we have*

$$\#\big(\mathbb{Z}_p/\mathcal{F}_E(\alpha^{-1})\big) = \#Ш(W_{\alpha^{-1}}/K) \cdot \#\mathrm{coker}(\mathrm{loc}_v)^2 \cdot \prod_{w|N} c_w^{(p)}(\alpha^{-1}) \cdot \#\mathrm{H}^0(\mathbb{Q}_p, E[p^\infty])^2,$$

where:

- $c_w^{(p)}(\alpha^{-1}) = \#\mathrm{H}^1_{\mathrm{ur}}(K_w, W_{\alpha^{-1}})$ *is the p-part of the Tamagawa number,*
- $Ш(W_{\alpha^{-1}}/K) = \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, W_{\alpha^{-1}})/\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, W_{\alpha^{-1}})_{\mathrm{div}}$ *is the Bloch–Kato Shafarevich–Tate group,*
- $\mathrm{loc}_v : \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha) \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K_v, T_\alpha)_{/\mathrm{tors}}$ *is the restriction map at v composed with the projection.*

Proof. This follows from α-twisted analogues of [JSW17, Prop. 3.2.1] and [JSW17, Thm. 3.3.1]. More precisely, we begin by verifying the following properties (i)–(iii):

(i) $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, W_{\alpha^{-1}})_{\mathrm{div}} \simeq \mathbb{Q}_p/\mathbb{Z}_p$,
(ii) $\mathrm{H}^1_{\mathrm{ord}}(K_v, W_{\alpha^{-1}}) \simeq \mathbb{Q}_p/\mathbb{Z}_p$,
(iii) $\mathrm{loc}_v : \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, W_{\alpha^{-1}})_{\mathrm{div}} \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K_v, W_{\alpha^{-1}})$ is surjective.

By Lemma 1.2.3, the nonvanishing of $\mathcal{L}_p^{\mathrm{BDP}}(f/K)(\alpha^{-1})$ implies the nonvanishing of $\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)$; the proof of (i) thus follows from [CGS23, Thm. 5.1.1] (Theorem 1.3.1 below). For (ii), since $\mathrm{H}^1_{\mathrm{ord}}(K_w, W_{\alpha^{-1}})$ is divisible by definition, it suffices to show that it has $\mathbb{Z}_p$-corank one. But this is immediate from local Tate duality and Tate's local Euler characteristic formula, noting that because p is a prime of good reduction and χ is pure of weight 0, the invariant subspaces $\mathrm{H}^0(K_v, \mathrm{Fil}_w^+W_{\alpha^{-1}})$ and $\mathrm{H}^0(K_v, (\mathrm{Fil}_w^+W_{\alpha^{-1}})^\vee(1))$ are both finite. Finally, as in the proof of Lemma 1.2.3, the nonvanishing of $\mathcal{L}_p^{\mathrm{BDP}}(f/K)(\alpha^{-1})$ implies that the map $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha) \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K_v, T_\alpha)_{/\mathrm{tors}}$ is nonzero, from which (iii) follows.

The same proof as [JSW17, Prop. 3.2.1] thus yields that $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, W_{\alpha^{-1}})$ is finite, with

$$\#\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, W_{\alpha^{-1}}) = \#\text{Ш}(W_{\alpha^{-1}}/K) \cdot \#\mathrm{coker}(\mathrm{loc}_v)^2. \tag{1.6}$$

Now put $M_{\alpha^{-1}} = M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\alpha^{-1})$ and $\mathfrak{X}_{\mathrm{Gr}}(E(\alpha^{-1})/K_\infty) = \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_{\alpha^{-1}})^\vee$, and denote by $\mathrm{Tw}_{\alpha^{-1}} : \Lambda \to \Lambda$ the $\mathbb{Z}_p$-linear isomorphism given by $\gamma \mapsto \alpha^{-1}(\gamma)\gamma$ for $\gamma \in \Gamma$. In view of (i)–(iii), the hypotheses in Theorem 3.3.1 of [JSW17] are satisfied by $V_{\alpha^{-1}}$, from which we conclude (taking $\Sigma = \emptyset$ in *loc. cit.*) that $\mathfrak{X}_{\mathrm{Gr}}(E(\alpha^{-1})/K_\infty)$ is Λ-torsion, and letting $\mathcal{F}_{E(\alpha^{-1})} \in \Lambda$ be a generator of $\mathrm{char}_\Lambda(\mathfrak{X}_{\mathrm{Gr}}(E(\alpha^{-1})/K_\infty))$ we have

$$\#\big(\mathbb{Z}_p/\mathcal{F}_{E(\alpha^{-1})}(0)\big) = \#\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, W_{\alpha^{-1}}) \cdot \prod_{w|N} c_w^{(p)}(\alpha^{-1}) \cdot \#\mathrm{H}^0(K_v, W_{\alpha^{-1}}) \cdot \#\mathrm{H}^0(K_{\bar{v}}, W_{\alpha^{-1}}). \tag{1.7}$$

Since clearly $\mathrm{Tw}_{\alpha^{-1}}(\mathcal{F}_E)$ gives a generator of $\mathrm{char}_\Lambda(\mathfrak{X}_{\mathrm{Gr}}(E(\alpha^{-1})/K_\infty)$ and $\mathrm{H}^0(\mathbb{Q}_p, W_{\alpha^{-1}}) = \mathrm{H}^0(\mathbb{Q}_p, E[p^\infty])$ for α sufficiently close to 1, the combination of (1.6) and (1.7) yields the equality in the theorem. □

As in Theorem 1.2.7, denote by $c_w^{(p)}(\alpha)$ the p-part of the Tagamawa number of W_α at w, and similarly put $c_w^{(p)} = \#\mathrm{H}^1_{\mathrm{ur}}(K_w, W)$ (see also Remark 1.1.1).

Lemma 1.2.8. *Assume that $\alpha : \Gamma \to \mathbb{Z}_p^\times$ is an anticyclotomic character, and $w \nmid p$ is a finite prime of K. If $\alpha \equiv 1 \pmod{p^m}$, then $c_w^{(p)}(\alpha) \equiv c_w^{(p)} \pmod{p^m}$.*

Proof. By definition, we have

$$\mathrm{H}^1_{\mathrm{ur}}(K_w, W_\alpha) = \mathrm{H}^1(\mathbb{F}_w, (W_\alpha)^{I_w}) \simeq (W_\alpha)^{I_w}/(\mathrm{Fr}_w - 1)(W_\alpha)^{I_w},$$

where $\mathbb{F}_w$ is the residue field of K_w and $I_w \subset G_{K_w}$ is the inertia subgroup at w. Since α is unramified at w, we have $(W_\alpha)^{I_w} = W^{I_w}$, and using that $\alpha \equiv 1 \pmod{p^m}$, we obtain

$$\mathrm{H}^1_{\mathrm{ur}}(K_w, W_\alpha)/p^m\mathrm{H}^1_{\mathrm{ur}}(K_w, W_\alpha) \simeq \mathrm{H}^1_{\mathrm{ur}}(K_w, W)/p^m\mathrm{H}^1_{\mathrm{ur}}(K_w, W),$$

from which the desired result follows. □

Remark 1.2.9. If $\alpha : \Gamma \to \mathbb{Z}_p^\times$ satisfies $\alpha \equiv 1 \pmod{p^m}$ with $m > \sum_{w|N} \mathrm{ord}_p(c_w^{(p)})$, Lemma 1.2.8 implies the equality

$$\prod_{w|N} c_w^{(p)}(\alpha) = \prod_{w|N} c_w^{(p)}.$$

1.2.3. *The Main Conjecture.* We recall the statement of the anticyclotomic Main Conjecture for $\mathcal{L}_p^{\mathrm{BDP}}(f/K)^2$. Note that this can be seen as a special case of the Iwasawa Main Conjecture for p-adic deformations of motives formulated by Greenberg [Gre94].

Conjecture 1.2.10. *Suppose K satisfies (Heeg), (disc), and (spl). Then $\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty)$ is Λ-torsion, and*

$$\mathrm{char}_\Lambda(\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty))\Lambda^{\mathrm{ur}} = (\mathcal{L}_p^{\mathrm{BDP}}(f/K)^2)$$

as ideals in Λ^{ur}.

In the following, we shall refer to the statement of Conjecture 1.2.10 with Λ^{ur} replaced by $\Lambda^{\mathrm{ur}} \otimes \mathbb{Q}_p$ as the *rational anticyclotomic Main Conjecture.*

Combining the results of Lemma 1.2.3 and Theorem 1.2.7 we arrive at the main result of this section.

Corollary 1.2.11. *Let $\alpha : \Gamma \to \mathbb{Z}_p^\times$ be an anticyclotomic character as in Definition 1.2.2 with $\mathcal{L}_p^{\mathrm{BDP}}(f/K)(\alpha^{-1}) \neq 0$ and $\alpha \equiv 1 \pmod{p^m}$ with $m \gg 0$. If Conjecture 1.2.10 holds, then*

$$\#(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_\alpha)/\mathbb{Z}_p \cdot \boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha))^2 = \#\text{Ш}(W_{\alpha^{-1}}/K) \cdot \prod_{w|N} c_w^{(p)}(\alpha^{-1}) \cdot \#(\mathrm{H}^0(\mathbb{Q}_p, E[p^\infty]))^4.$$

We conclude this section by recording some results on Conjecture 1.2.10. The first cases of the conjecture were proved by X. Wan [Wan21], assuming that the G_K-action on T_pE is surjective and some mild ramification hypotheses on $E[p]$. More recently, we have the following.

Theorem 1.2.12. *Suppose K satisfies (Heeg), (disc), and (spl).*

(i) *If $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ as $G_{\mathbb{Q}}$-modules with $\phi|_{G_p} \neq \mathbb{1}, \omega$, then Conjecture 1.2.10 holds.*
(ii) *If $p > 3$ satisfies (irr), then the rational anticyclotomic Main Conjecture holds.*
(iii) *If $p > 3$ satisfies (sur), then Conjecture 1.2.10 holds.*

Proof. This is shown in [CGS23] in situation (i), and in [BCS23] in situations (ii) and (iii). □

1.3. **The Kolyvagin system bound with error term.** For a positive integer e put

$$\mathcal{L}_e = \{\ell \in \mathcal{L}_0 \,:\, a_\ell \equiv \ell + 1 \equiv 0 \pmod{p^e}\}.$$

We shall need the following mild extension of [CGS23, Thm. 5.1.1].

Theorem 1.3.1. *Suppose $\mathcal{L} \subset \mathcal{L}^{\rm Heeg}$ satisfies $\mathcal{L}_e \subset \mathcal{L}$ for $e \gg 0$. Let $\alpha : \Gamma \to \mathbb{Z}_p^\times$ be an anticyclotomic character such that $\alpha \equiv 1 \pmod{p^m}$. Suppose that there is a collection of cohomology classes*

$$\{\tilde{\kappa}_n \in {\rm H}^1(K, T_\alpha/I_nT_\alpha) \,:\, n \in \mathcal{N}(\mathcal{L})\}$$

with $\tilde{\kappa}_1 \neq 0$ and that there is an integer $t \geq 0$, independent of n, such that $\{p^t\tilde{\kappa}_n\}_{n\in\mathcal{N}(\mathcal{L})}$ is a Kolyvagin system for T_α and the Selmer structure $\mathcal{F}_{\rm ord}$. Then there exist non-negative integers $\mathcal{M}$ and $\mathcal{E}$, depending only on T_pE, such that if $m \geq \mathcal{M}$ then ${\rm H}^1_{\mathcal{F}_{\rm ord}}(K, T_\alpha)$ has $\mathbb{Z}_p$-rank one, and there is a finite $\mathbb{Z}_p$-module M such that

$${\rm H}^1_{\mathcal{F}_{\rm ord}}(K, W_{\alpha^{-1}}) \simeq \mathbb{Q}_p/\mathbb{Z}_p \oplus M \oplus M$$

with

$${\rm length}_{\mathbb{Z}_p}(M) \leq {\rm ind}(\tilde{\kappa}_1) + \mathcal{E},$$

where ${\rm ind}(\tilde{\kappa}_1) = {\rm length}_{\mathbb{Z}_p}\big({\rm H}^1_{\mathcal{F}_{\rm ord}}(K, T_\alpha)/\mathbb{Z}_p \cdot \tilde{\kappa}_1\big)$. Moreover, if (sur) holds, then $\mathcal{E} = 0$.

Proof. Take $e \gg 0$ so that $\tilde{\kappa}_1 \not\equiv 0 \pmod{p^e}$ and such that $\tilde{\mathcal{L}} := \mathcal{L}_{e+t}$ is contained in $\mathcal{L}$, and put $\tilde{\mathcal{N}} = \mathcal{N}(\tilde{\mathcal{L}})$. As in the proof of [How04b, Thm. 2.2.2], the collection of classes $\{\tilde{\kappa}_n\}_{n\in\tilde{\mathcal{N}}}$ gives a (non-trivial) Kolyvagin system for $(T/p^eT, \mathcal{F}_{\rm ord}, \tilde{\mathcal{L}})$, and a slight modification of the argument yielding [CGS23, Thm. 5.1.1] applied to this system yields the result. The claim that $\mathcal{E} = 0$ when (sur) holds follows from [CGS23, Rem. 3.3.5]. □

2. Proofs of Theorem A and Theorem B

2.1. **Kolyvagin's conjecture.** We can now prove our main result towards Kolyvagin's original conjecture.

Proof of Theorem A. Assume that the rational anticyclotomic Main Conjecture holds. In particular, letting $\mathcal{F}_p(E/K) \in \Lambda$ be any generator of ${\rm char}_\Lambda(\mathfrak{X}_{\rm Gr}(E/K_\infty))$ we have the divisibility

$$\mathcal{F}_p(E/K) \cdot p^R = \mathcal{L}_p^{\rm BDP}(f/K)^2 \cdot h \tag{2.1}$$

for some $R \geq 0$ and $h \in \Lambda^{\rm ur}$. Let also

$$x := v_p(\#{\rm H}^0(\mathbb{Q}_p, E[p^\infty])) = v_p(1 - \alpha_p).$$

Assume for contradiction that $\kappa_n^{\rm Heeg} = 0$ for all $n \in \mathcal{N}_{\rm Heeg}$. Take $t \in \mathbb{Z}_{>0}$ such that

$$t > \tfrac{1}{2}\sum_{w|N} {\rm ord}_p(c_w^{(p)}) + R + \mathcal{E}, \tag{2.2}$$

where $\mathcal{E}$ is the error term from Theorem 1.3.1. Consider a character $\alpha = \alpha_m : \Gamma \to \mathbb{Z}_p^\times$ as in Definition 1.2.2 such that the following conditions hold:

(a) $\mathcal{L}_p^{\rm BDP}(f/K)(\alpha^{-1}) \neq 0$,
(b) $m > \mathcal{M} + 2t + 2x$,
(c) The conclusion of Corollary 1.2.11 holds.

By the last claim in Theorem 1.2.1, we can always find such α. In particular, by Corollary 1.2.3 we then have $\boldsymbol{\kappa}_1^{\rm Heeg}(\alpha) \neq 0$, and moreover

$$\prod_{w|N} c_w^{(p)}(\alpha) = \prod_{w|N} c_w^{(p)}$$

by Lemma 1.2.8 and Remark 1.2.9.

Let $\mathcal{N} = \mathcal{N}(\mathcal{L}_m)$, where $\mathcal{L}_m = \{\ell \in \mathcal{L}_0 \,:\, a_\ell \equiv \ell + 1 \equiv 0 \pmod{p^m}\}$, so $\mathscr{M}(n) \geq m$ for all $n \in \mathcal{N}$. Since we assume that all $\kappa_n^{\rm Heeg}$ vanish, by Lemma 1.1.5 and the assumption $m > t + 2x$ we find that $\boldsymbol{\kappa}_n^{\rm Heeg}(\alpha) \equiv 0 \pmod{p^{t+2x}}$ for every $n \in \mathcal{N}$. We can therefore consider a collection of cohomology classes $\{\tilde{\kappa}_{n,\alpha} \in {\rm H}^1(K, T_\alpha/I_nT_\alpha)\}_{n\in\mathcal{N}}$ such that

$$p^{t+2x} \cdot \tilde{\kappa}_{n,\alpha} = \boldsymbol{\kappa}_n^{\rm Heeg}(\alpha).$$

Note that these classes are not canonically defined, but their order (and the order of their localisations) is. Since $\mathrm{H}^1(K, T_\alpha)$ is torsion-free by hypothesis (tor), the nonvanishing of $\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)$ implies that the bottom class $\tilde{\kappa}_{1,\alpha}$ is non-zero and its index is equal to $\mathrm{ind}(\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)) - t - 2x$. Hence from Theorem 1.3.1 we get

$$\tfrac{1}{2}\,\mathrm{length}_{\mathbb{Z}_p}(\text{Ш}(W_{\alpha^{-1}}/K)) \leq \mathrm{ind}(\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)) - t - 2x + \mathcal{E}. \tag{2.3}$$

On the other hand, from the combination of Lemma 1.2.3, Lemma 1.2.5, Theorem 1.2.7, and (2.1), we obtain

$$\mathrm{ind}(\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)) \leq \tfrac{1}{2}\mathrm{length}_{\mathbb{Z}_p}(\text{Ш}(W_{\alpha^{-1}}/K)) + \tfrac{1}{2}\sum_{w|N} \mathrm{ord}_p(c_w^{(p)}) + R + 2x, \tag{2.4}$$

using $m > \sum_{w|N} \mathrm{ord}_p(c_w^{(p)})$ to apply the observation in Remark 1.2.9. Combining (2.3) and (2.4), we get

$$t \leq \tfrac{1}{2}\sum_{w|N} \mathrm{ord}_p(c_w^{(p)}) + R + \mathcal{E},$$

which contradicts (2.2), thereby proving the result. □

Remark 2.1.1. In particular, if $E[p]$ satisfies (sur), the above argument shows that $\mathscr{M}_{\infty,\mathcal{N}} \leq \frac{1}{2}\sum_{w|N} \mathrm{ord}_p(c_w^{(p)})$, where $\mathscr{M}_{\infty,\mathcal{N}} = \mathscr{M}_\infty(\{\kappa_n^{\mathrm{Heeg}}\}_n)$ is the divisibility index of $\{\kappa_n^{\mathrm{Heeg}}\}_{n\in\mathcal{N}}$ for any $\mathcal{N} \supset \mathcal{N}(\mathcal{L}_m)$.

2.2. **The refined Kolyvagin's conjecture.** Let R be the ring of integers of a finite extension of $\mathbb{Q}_p$ with maximal ideal $\mathfrak{m}$ and uniformiser $\varpi \in \mathfrak{m}$. Let $\alpha : \Gamma_K \to R^\times$ be a character such that $\alpha \equiv 1 \pmod{\mathfrak{m}^m}$, and put $T_\alpha = T_pE \otimes_{\mathbb{Z}_p} R(\alpha)$, as above. In this section, we do not assume $m \gg 0$, in particular we could also have $m = 1$.

Similarly as in the introduction, if $\boldsymbol{\kappa} = \{\kappa_n\}_{n\in\mathcal{N}}$ is a Kolyvagin system for $(T_\alpha, \mathcal{F}_{\mathrm{ord}}, \mathcal{L})$, for each $n \in \mathcal{N} = \mathcal{N}(\mathcal{L})$, define $\mathscr{M}(n) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by $\mathscr{M}(n) = \infty$ if $\kappa_n = 0$, and by

$$\mathscr{M}(n) = \max\{\mathscr{M} \colon \kappa_n \in \mathfrak{m}^{\mathscr{M}}\mathrm{H}^1(K, T/I_nT)\} = \mathrm{ind}(\kappa_n)$$

otherwise. For any $\mathcal{N}' \subset \mathcal{N}$, put $\mathscr{M}_{r,\mathcal{N}'} = \min\{\mathscr{M}(n) \colon \nu(n) = r, n \in \mathcal{N}'\}$, where $\nu(n)$ denotes the number of prime factors of n. Firstly, one shows, similarly as in [Kol91], that $\mathscr{M}_{r,\mathcal{N}'} \geq \mathscr{M}_{r+1,\mathcal{N}'} \geq 0$ for all $r \geq 0$. Put

$$\mathscr{M}_{\infty,\mathcal{N}'}(\boldsymbol{\kappa}) = \lim_{r\to\infty} \mathscr{M}_{r,\mathcal{N}'}.$$

We let $\mathscr{M}_\infty(\boldsymbol{\kappa}) = \mathscr{M}_{\infty,\mathcal{N}}(\boldsymbol{\kappa})$. Note that $\mathscr{M}_{\infty,\mathcal{N}'}(\boldsymbol{\kappa}) \geq \mathscr{M}_\infty(\boldsymbol{\kappa})$ for every $\mathcal{N}' \subset \mathcal{N}$.

In addition to the ingredients that went into the proof of Theorem A, the proof of the refinement in Theorem B relies on the independence of the integer $\mathscr{M}_{\infty,\mathcal{N}'}$ from $\mathcal{N}' \subset \mathcal{N}$ and an exact formula for the length of $\text{Ш}(W_{\alpha^{-1}}/K)$ in the spirit of Kolyvagin's structure theorem [Kol91, Thm. 1].

Proposition 2.2.1. *Assume that $p \geq 3$ and that (sur) holds. Let $\boldsymbol{\kappa} = \{\kappa_n\}_{n\in\mathcal{N}}$ be a Kolyvagin system for $(T, \mathcal{F}, \mathcal{L})$. Let $e > 0$ be any integer such that $\mathcal{L}_e \subset \mathcal{L}$ and let $\mathcal{N}^{(e)} = \mathcal{N}(\mathcal{L}_e)$. Then*

$$\mathscr{M}_{\infty,\mathcal{N}^{(e)}}(\boldsymbol{\kappa}) = \mathscr{M}_{\infty,\mathcal{N}}(\boldsymbol{\kappa}).$$

Theorem 2.2.2. *Assume $p > 3$. Suppose $\mathcal{L} \subset \mathcal{L}_0$ and let $\boldsymbol{\kappa} = \{\kappa_n\}_{n\in\mathcal{N}}$ be a Kolyvagin system for $(T, \mathcal{F}, \mathcal{L})$ with $\kappa_1 \neq 0$. Assume further that (sur) holds. Then*

$$\mathrm{length}_{\mathbb{Z}_p}\big(\text{Ш}(W_{\alpha^{-1}}/K)\big) = 2\big(\mathscr{M}_0(\boldsymbol{\kappa}) - \mathscr{M}_\infty(\boldsymbol{\kappa})\big),$$

where $\mathscr{M}_0(\boldsymbol{\kappa}) = \mathrm{ind}(\kappa_1)$.

Remark 2.2.3. Note that this theorem applies to any anticylotomic character α of Γ, as will be clear from the proof below: the need to distinguish trivial characters sufficiently close to the trivial character in [CGS23, 5.1.1] (close with respect to [CGLS22, Thm. 3.3.8], where essentially the maximum m such that $\alpha \equiv 1 \mod \mathfrak{m}^m$ was part of the error term) disappears when (sur) holds. In particular, Theorem 2.2.2 applies for characters $\alpha : \Gamma \to \Lambda/(\mathfrak{P} + p^m)^\times$ for any height one prime ideal $\mathfrak{P}$ of Λ.

Let $\mathcal{F} = \mathcal{F}_{\mathrm{ord}}$ and $T = T_\alpha$. For any $k \geq 1$, let $R^{(k)} = R/\mathfrak{m}^k$ and $T^{(k)} = T/\mathfrak{m}^k$. Recall that, by [CGLS22, Prop. 3.3.2], there is an integer $\epsilon \in \{0, 1\}$ such that for all k and every every $n \in \mathcal{N}^{(k)}$ there is an $R^{(k)}$-module $M^{(k)}(n)$ such that

$$\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)}) \simeq (R/\mathfrak{m}^k)^\epsilon \oplus M^{(k)}(n) \oplus M^{(k)}(n). \tag{2.5}$$

Moreover, by [CGLS22, Thm. 3.3.8], if $\boldsymbol{\kappa} = \{\kappa_n\}_{n\in\mathcal{N}}$ is a Kolyvagin system for $(T, \mathcal{F}, \mathcal{L})$ with $\kappa_1 \neq 0$, then $\epsilon = 1$ and for $k \gg 0$, $\exp(M^{(k)}(1)) < k$. We also denote by $\boldsymbol{\kappa}^{(k)} = \{\kappa_n^{(k)}\}_{n\in\mathcal{N}^{(k)}}$ the Kolyvagin system for $(T^{(k)}, \mathcal{F}, \mathcal{L}^{(k)})$ obtained from $\boldsymbol{\kappa}$, where $\mathcal{L}^{(k)} = \{\ell \in \mathcal{L} : I_\ell \subset \mathfrak{m}^k\}$. In particular, if $\mathcal{L} = \mathcal{L}_{\mathrm{Heeg}}$ and $R = \mathbb{Z}_p$, then $\mathcal{L}^{(k)} = \mathcal{L}_k$.

We adopt the following notation: a finite torsion R-module X is isomorphic to a sum of cyclic R-modules: $X \simeq \oplus_{i=1}^{s(X)} R/\mathfrak{m}^{d_i(X)}$ for some uniquely-determined integers $d_i(X) \geq 0$, with $d_1(X) \geq d_2(X) \geq \cdots \geq d_{s(X)}(X)$. For any $x \in X$, let the order and index of x in X be

$$\mathrm{ord}(x) := \min\{n \geq 0 : \varpi^n \cdot x = 0\}, \quad \mathrm{ind}(x) := \max\{t \geq 0 : x \in \mathfrak{m}^t X\}.$$

For an integer $t \geq 0$ we let $\rho_t(X) = \#\{i : d_i(X) > t\}$. Assume $\alpha \equiv 1 \mod \mathfrak{m}^m$ for some $m \geq 0$. For $n \in \mathcal{N}^{(k)}$ with $k \geq m$, we let

$$\rho(n)^{\pm} := \rho_0(\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(m)})^{\pm}), \quad \rho(n) := \rho(n)^+ + \rho(n)^-,$$

that is, we are counting the summands of the $\pm$-components of $\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(m)})$, on which, since $\alpha \equiv 1 \mod \mathfrak{m}^m$, there is a well-defined action of the complex conjugation. Note that, by [CGLS22, Lem. 3.3.1], we are identifying

$$\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(m)}) \simeq \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)})[\mathfrak{m}^m]$$

and, in particular, $\rho(n)$ does not depend on k or α.

Note also that, by (2.5), if $\rho(n) = 1$, we must have $\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)}) \simeq R/\mathfrak{m}^k$, i.e. $M^{(k)}(n) = \{0\}$. If this is the case, we say that n is a *core vertex*, as in [MR04, Def. 4.1.8] (and [Zan19] in the Heegner point case).

Proof of Proposition 2.2.1. The essential idea of this proof can be found in the work of Kolyvagin. Indeed, the case $\alpha = 1$ can be easily extracted from the proof of [McC91, Prop. 5.2].

Let $r \geq 0$ be an integers such that $\mathscr{M}^{(k)}_{r,\mathcal{N}} = \mathscr{M}^{(k)}_{\infty,\mathcal{N}}$. Let $M := \mathscr{M}_{r,\mathcal{N}^{(k)}}$ and $\mathcal{N}_r := \{n \in \mathcal{N} : \nu(n) = r\}$. By definition, there exists some $n \in \mathcal{N}_r$ such that $\mathscr{M}(n) = M$. Necessarily $n \in \mathcal{N}^{(M+1)}$, so we may assume that $e > M + 1$. Suppose there exists a prime $\ell_0 \mid n$ such that $\ell_0 \notin \mathcal{L}_e$. We will show that there exists a prime $\ell \in \mathcal{L}_e$ such that $n' = \ell n/\ell_0 \in \mathcal{N}_r$ is such that $\mathscr{M}(n') = M$. Replacing n with n' and repeating as necessary, we arrive at an $n \in \mathcal{N}_r^{(e)}$ such that $\mathscr{M}(n) = M$, whence the proposition.

We have $\kappa_n^{(M+1)} \in \mathfrak{m}^M \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(M+1)})$ but $\kappa_n^{(M+1)} \notin \mathfrak{m}^{M+1} \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(M+1)})$. From the identification $\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(1)}) = \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(M+1)})[\mathfrak{m}]$, we see that $\kappa_n^{(M+1)}$ is identified with a non-zero class $0 \neq \bar{\kappa} \in \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(1)})$. Complex conjugation acts on $T^{(1)}$ and hence on $\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(1)})$ and we may fix a sign $s = \pm$ such that $\bar{\kappa}^s \neq 0$.

Let $0 \neq c \in \mathrm{H}^1_{\mathcal{F}(n/\ell_0)^{\ell_0}}(K, T^{(1)})^{-s}$. Here the superscript ℓ_0 on the $\mathcal{F}(n/\ell_0)$ means that we impose no restrictions on the classes at the prime ℓ_0. The existence of such a c follows easily from global duality and the fact that $\ell_0 \in \mathcal{L}$.

Now let $\ell \in \mathcal{L}_e$, $\ell \nmid n$, be a prime such that $\mathrm{loc}_\ell(\bar{\kappa}^s) \neq 0$ and $\mathrm{loc}_\ell(c) \neq 0$. The existence of such a prime ℓ follows from [CGS23, Prop. 5.3.1] (applied with $m = 1$ and $k = e$ in the notation of *op. cit.*) noting that the error term is zero since we are assuming (sur) holds. Then $n\ell \in \mathcal{N}_{r+1}^{(M+1)}$ and so $\kappa_{n\ell}^{(M+1)}$ is defined. By the Kolyvagin relations, $\mathrm{loc}_\ell(\kappa_{n\ell}^{(M+1)})$ has the same order as $\mathrm{loc}_\ell(\kappa_n^{(M+1)})$, and the latter equals 1 as $\mathrm{loc}_\ell(\bar{\kappa}) \neq 0$. In particular $\kappa_{n\ell}^{(M+1)} \notin p^{M+1}\mathrm{H}^1_{\mathcal{F}(n\ell)}(K, T^{(M+1)})$. On the other hand, $n\ell \in \mathcal{N}_{r+1}$, so $\mathscr{M}(n\ell) \geq \mathscr{M}_{r+1,\mathcal{N}} = \mathscr{M}_{r,\mathcal{N}} = M$ by the choice of r. It follows that $\kappa_{n\ell}^{(M+1)} \in \mathfrak{m}^M \mathrm{H}^1_{\mathcal{F}(n\ell)}(K, T^{(M+1)})$ and so defines a non-zero class $\bar{\kappa}_\ell \in \mathrm{H}^1_{\mathcal{F}(n\ell)}(K, T^{(1)})$. The Kolyvagin relations relate $\mathrm{loc}_\ell(\kappa_n)$ with $\mathrm{loc}_\ell(\kappa_{n\ell})$ via the usual finite-singular (iso)morphism. Since this morphism intertwines the eigenspaces for complex conjugation (see for example [Nek07, 5.15.1], recalling that $\ell \in \mathcal{L}_e$ and $e > M + 1$ imply that Frob_ℓ acts as complex conjugation on $T^{(M+1)}$), this shows that $\mathrm{loc}_\ell(\bar{\kappa}_\ell^{\pm}) \neq 0$ if and only if $\mathrm{loc}_\ell(\bar{\kappa}^{\mp}) \neq 0$, so $\mathrm{loc}_\ell(\bar{\kappa}_\ell^{-s}) \neq 0$.

By global duality we have

$$0 = \sum_v \langle \mathrm{loc}_v(c), \mathrm{loc}_v(\bar{\kappa}_\ell^{-s})\rangle_v = \langle \mathrm{loc}_\ell(c), \mathrm{loc}_\ell(\bar{\kappa}_\ell^{-s})\rangle_\ell + \langle \mathrm{loc}_{\ell_0}(c), \mathrm{loc}_{\ell_0}(\bar{\kappa}_\ell^{-s})\rangle_{\ell_0}.$$

As $0 \neq \mathrm{loc}_\ell(c) \in \mathrm{H}^1_{\mathrm{ur}}(K, T^{(1)})^{-s}$ and $0 \neq \mathrm{loc}_\ell(\bar{\kappa}_\ell^{-s}) \in \mathrm{H}^1_{\mathrm{tr}}(K, T^{(1)})^{-s}$, it follows that $\langle \mathrm{loc}_\ell(c), \mathrm{loc}_\ell(\bar{\kappa}_\ell^{-s})\rangle_\ell \neq 0$. This in turn implies that $\langle \mathrm{loc}_{\ell_0}(c), \mathrm{loc}_{\ell_0}(\bar{\kappa}_\ell^{-s})\rangle_{\ell_0} \neq 0$, which means that $\mathrm{loc}_{\ell_0}(\bar{\kappa}_\ell^{-s}) \neq 0$. So the order of

$\mathrm{loc}_{\ell_0}(\kappa_{n\ell}^{(M+1)})$ is 1. But then the Kolyvagin relations imply that $\mathrm{loc}_\ell(\kappa_{n\ell/\ell_0}^{(M+1)})$ has order 1, and so $\mathscr{M}(n\ell/\ell_0) = M$ by the same reasoning that showed that $\mathscr{M}(n\ell) = M$. □

For the proof of Theorem 2.2.2, we will also need the following result.

Lemma 2.2.4. *Assume $p > 3$. If $k \gg 0$ and $\langle \kappa_h^{(k)} \rangle = \mathfrak{m}^{j+\mathrm{length}_R(M^{(k)}(h))}\mathrm{H}^1_{\mathcal{F}(h)}(K, T^{(k)})$ for some $h \in \mathcal{N}$, then*

$$\langle \kappa_n^{(k)} \rangle = \mathfrak{m}^{j+\mathrm{length}_R(M^{(k)}(n))}\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)}) \text{ for every } n \in \mathcal{N}^{(2k-1)}.$$

Proof. The proof runs along the lines of [Zan19, § 2.2]. First, one shows that for every two core vertexes $n, m \in \mathcal{N}^{(k)}$, the $R^{(k)}$-module spanned by $\kappa_n^{(k)}, \kappa_m^{(k)}$ are isomorphic, i.e.,

$$\rho(n) = \rho(m) = 1 \quad \Rightarrow \quad R/\mathfrak{m}^{k-\mathrm{ind}(\kappa_n^{(k)})} \simeq \langle \kappa_n^{(k)} \rangle \simeq \langle \kappa_m^{(k)} \rangle \simeq R/\mathfrak{m}^{k-\mathrm{ind}(\kappa_m^{(k)})}.$$

This follows as in [Zan19, Cor. 2.2.13]. From this one deduces that for any k and any $n \in \mathcal{N}^{(k)}$ with $\rho(n) = 1$,

$$\langle \kappa_n^{(k)} \rangle \simeq R/\mathfrak{m}^{k-d}$$

for some d independent on k and n. One then shows that

$$\langle \kappa_n^{(k)} \rangle = \mathfrak{m}^{d+\mathrm{length}_R(M^{(k)}(n))}\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)}) \quad \text{if } n \in \mathcal{N}^{(2k-1)}. \tag{2.6}$$

Following the proof of [Zan19, Lemma 2.3.1], one proves this statement without the assumption that $\rho(n) = 1$ using [How04a, Lemma 1.6.4] and induction on $r(k, n) = k + \max\{\rho(n)^+, \rho(n)^-\}$. □

Proof of Theorem 2.2.2. As in the proof of [CGS23, Thm. 5.1.1], let $s(n) = \dim_{\mathbb{F}} \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(1)}) - 1 = 2 \cdot \dim_{\mathbb{F}} M(n)[\mathfrak{m}]$, where $\mathbb{F} = R/\mathfrak{m}$. Let $\rho = \rho_0(1)$. Note that $\rho \geq \dim_{\mathbb{F}} \mathrm{H}^1_{\mathcal{F}}(K, T^{(1)}) = s(1) + 1$. By [CGLS22, Thm 3.3.8], we can write $\mathrm{H}^1_{\mathcal{F}}(K, W_{\alpha^{-1}}) \simeq \mathrm{Frac}(R)/R \oplus M(1) \oplus M(1)$, where $M(1)$ is a finite torsion R-module. Let k be a fixed integer such that

$$k > \mathrm{length}_R(M(1)) + \mathrm{ind}(\kappa_1) + m \tag{2.7}$$

(recall that $\alpha \equiv 1 \pmod{\mathfrak{m}^m}$). In particular, $\mathrm{H}^1_{\mathcal{F}}(K, T^{(k)}) \simeq R^{(k)} \oplus M(1) \oplus M(1)$. In *op. cit.* we found a sequence of integers $1 = n_0, n_1, ..., n_\rho \in \mathcal{N}^{(k)}$ (which we can actually assume to be in $\mathcal{N}^{(2k-1)}$ applying [CGS23, Prop. 5.3.1] with a different choice of k) satisfying certain conditions (denoted by (a)-(g) in *op. cit.*), in particular, if (sur) holds, the error term e is zero and we found:

(e) $\mathrm{ind}(\kappa_{n_{i-1}}^{(k)}) \geq \mathrm{ind}(\kappa_{n_i}^{(k)})$;
(f) $\rho(n_i) \leq \rho(n_{i-1})$, and $\rho(n_i) = \rho(n_{i-1}) > 1$ only if $\rho_0(\mathrm{H}^1_{\mathcal{F}(n_i)}(K, T^{(m)})^\pm) \geq 1$;
(g) if $\rho(n_{i-2}) > 1$ then $\rho(n_i) < \rho(n_{i-2})$.

From (g), we get that $\rho(n_\rho) = 1$, implying in particular that

$$\mathrm{H}^1_{\mathcal{F}(n_\rho)}(K, T^{(k)}) \simeq R/\mathfrak{m}^k, \quad \text{i.e.} \quad M^{(k)}(n_\rho) = 0.$$

Note that we do not need to assume m to be large in this case, as the proof of (B) in [CGS23] only requires $m > \mathcal{M}$ and $\mathcal{M} = 0$ when (sur) holds. In particular, we can take $m = 1$ and work with the $\mathfrak{m}$-torsion in the case where the character α is attached to a height one prime ideal of Λ different from (p).

Moreover, by Lemma 2.2.4 and the choice (2.7), we have

$$j + \mathrm{length}_R(M(1)) = \mathrm{ind}(\kappa_1) < k - \mathrm{length}_R(M(1)) < k, \quad j = \mathrm{ind}(\kappa_{n_\rho}^{(k)}). \tag{2.8}$$

In order to prove the theorem, we need to show that $\mathrm{ind}(\kappa_{n_\rho}^{(k)}) = \mathscr{M}_\infty(\boldsymbol{\kappa})$. By (2.8), $\mathrm{ind}(\kappa_{n_\rho}^{(k)}) < k$, so

$$\mathscr{M}(n_\rho) = \mathrm{ind}(\kappa_{n_\rho}) = \mathrm{ind}(\kappa_{n_\rho}^{(k)}) = j.$$

Let $\mathcal{N}' = \mathcal{N}^{2k-1}$. Let $i \geq 0$ and let $n \in \mathcal{N}'_i$ such that $\mathscr{M}(n) = \mathscr{M}_{\rho+i,\mathcal{N}'}$. As $\mathscr{M}(n) \geq \mathrm{ind}(\kappa_n^{(k)})$ by the definition of $\mathscr{M}(n)$ and since $\mathrm{ind}(\kappa_n^{(k)}) = \min\{k, j + \mathrm{length}_R(M(n))\}$ by Lemma 2.2.4, we have

$$\mathscr{M}_{\rho+i,\mathcal{N}'} = \mathscr{M}(n) \geq \mathrm{ind}(\kappa_n^{(k)}) = \min\{k, j + \mathrm{length}_R(M(n))\} \geq j = \mathscr{M}(n_\rho) \geq \mathscr{M}_{\rho,\mathcal{N}'}.$$

Taking $i = 0$, it follows that $\mathscr{M}_{\rho,\mathcal{N}'} = \mathscr{M}(n_\rho)$. Furthermore, since $\mathscr{M}_{\rho+i,\mathcal{N}'} \leq \mathscr{M}_{\rho,\mathcal{N}'}$, it follows that $\mathscr{M}_{\rho+i,\mathcal{N}'} = \mathscr{M}_{\rho,\mathcal{N}'}$ for all $i \geq 0$. Hence $\mathscr{M}_{\infty,\mathcal{N}'} = \mathscr{M}_{\rho,\mathcal{N}'} = \mathscr{M}(n_\rho)$. It then follows from Proposition 2.2.1 that $\mathscr{M}_\infty(\boldsymbol{\kappa}) = \mathscr{M}_{\infty,\mathcal{N}'} = \mathscr{M}(n_\rho)$. □

Now are ready to prove the refined Kolyvagin's conjecture.

Proof of Theorem B. Assume (sur), $p > 3$ and Conjecture 1.2.10. By the nonvanishing of $\mathcal{L}_p^{\mathrm{BDP}}(f/K)$, we can choose a character $\alpha = \alpha_m : \Gamma \to \mathbb{Z}_p^\times$ as in §1.1.4 with $m > \sum_{w|N} \mathrm{ord}_p(c_w^{(p)}) + \mathscr{M}_\infty(\kappa^{\mathrm{Heeg}})$, and such that $\mathcal{L}_p^{\mathrm{BDP}}(f/K)(\alpha^{-1}) \neq 0$. By Corollary 1.2.11 and Remark 1.2.9 we then have

$$\mathrm{length}_{\mathbb{Z}_p}(Ш(W_{\alpha^{-1}}/K)) = 2 \cdot \mathrm{ind}(\boldsymbol{\kappa}_1^{\mathrm{Heeg}}(\alpha)) - 4x - \sum_{w|N} \mathrm{ord}_p(c_w^{(p)}), \tag{2.9}$$

where $x = v_p(\#\mathrm{H}^0(\mathbb{Q}_p, E[p^\infty])) = v_p(1-\alpha_p)$. Together with Theorem 2.2.2 for the Kolyvagin system $\boldsymbol{\kappa}(\alpha) := \{\boldsymbol{\kappa}_n^{\mathrm{Heeg}}(\alpha)\}_{n\in\mathcal{N}}$, where $\mathcal{N} = \mathcal{N}(\mathcal{L}_m)$,

$$\mathscr{M}_{\infty,\mathcal{N}}(\boldsymbol{\kappa}(\alpha)) = \tfrac{1}{2}\sum_{w|N} \mathrm{ord}_p(c_w^{(p)}) + 2x.$$

By Remark 2.1.1 we have $\mathscr{M}_{\infty,\mathcal{N}}(\kappa^{\mathrm{Heeg}}) \leq \frac{1}{2}\sum_{w|N} \mathrm{ord}_p(c_w^{(p)})$. If the inequality was strict, there would exist $n \in \mathcal{N}$ such that $\mathrm{ind}(\kappa_n^{\mathrm{Heeg}}) \lneq \frac{1}{2}\sum_{w|N} \mathrm{ord}_p(c_w^{(p)})$. By the congruence of Lemma 1.1.5, $\mathrm{ind}(\kappa_n^{\mathrm{Heeg}}) + 2x = \mathrm{ind}(\boldsymbol{\kappa}_n^{\mathrm{Heeg}}(\alpha))$, and hence by the choice of m and the definition of $\mathscr{M}_{\infty,\mathcal{N}}(\boldsymbol{\kappa}(\alpha))$, this would imply $\mathscr{M}_{\infty,\mathcal{N}}(\boldsymbol{\kappa}(\alpha)) \lneq \frac{1}{2}\sum_{w|N} \mathrm{ord}_p(c_w^{(p)}) + 2x$, giving a contradiction. Therefore we have $\mathscr{M}_{\infty,\mathcal{N}}(\kappa^{\mathrm{Heeg}}) = \frac{1}{2}\sum_{w|N} \mathrm{ord}_p(c_w^{(p)})$ and, by Proposition 2.2.1, we find

$$\mathscr{M}_{\infty,\mathcal{N}_{\mathrm{Heeg}}}(\kappa^{\mathrm{Heeg}}) = \tfrac{1}{2}\sum_{w|N} \mathrm{ord}_p(c_w^{(p)}).$$

□

Remark 2.2.5. Note that, conversely, the refined Kolyvagin conjecture together with Theorem 2.2.2 implies the "anticyclotomic Iwasawa main conjecture at α_m" for $m \gg 0$, namely:

$$\mathcal{F}_p(E/K)(\alpha_m) \sim_p \mathcal{L}_p^{\mathrm{BDP}}(f/K)^2(\alpha_m),$$

where $\mathcal{F}_p(E/K) \in \Lambda$ is any generator of $\mathrm{char}_\Lambda(\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty))$. This follows repeating the proof of Theorem B backwards and applying Lemma 1.2.3 and Theorem 1.2.7.

3. The cyclotomic analogue: the non-triviality of Kato's Kolyvagin system

In this section we work with the cyclotomic Iwasawa algebra over $\mathbb{Q}$. More precisely, let $\mathbb{Q}_\infty$ be the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$, let $\Gamma_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$, and

$$\Lambda = \Lambda_{\mathbb{Q}} = \mathbb{Z}_p[[\Gamma_{\mathbb{Q}}]].$$

3.1. The Kolyvagin system of Kato classes.

We recall the construction of the Kolyvagin system of classes $\kappa_n = \kappa_n^{\mathrm{Kato}} \in \mathrm{H}^1(\mathbb{Q}, T/I_nT)$ derived from Kato's Euler system and their Iwasawa-theoretic analogues.

3.1.1. *Selmer structures.* Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, without complex multiplication, and let $p \nmid 2N$ be a prime of good ordinary reduction for E. We assume

$$E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\phi^{-1}\omega) \implies \phi \neq 1, \omega, \tag{$\mathrm{tor}_{\mathbb{Q}}$}$$

where, of course, ω is the mod p cyclotomic character. This is equivalent to the assertion that $E'(\mathbb{Q})[p] = 0$ for all curves E' in the isogeny class of E.

For a character $\alpha : \Gamma_{\mathbb{Q}} \to R^\times$ with values in the ring of integers R of a finite extension $\Phi/\mathbb{Q}_p$, we consider the $G_{\mathbb{Q}}$-modules

$$T_\alpha := T_pE \otimes_{\mathbb{Z}_p} R(\alpha), \quad V_\alpha := T_\alpha \otimes_R \Phi, \quad W_\alpha := T_\alpha \otimes_R \Phi/R \simeq V_\alpha/T_\alpha, \tag{3.1}$$

where $R(\alpha)$ is the free R-module of rank one on which $G_{\mathbb{Q}}$ acts via the projection $G_{\mathbb{Q}} \twoheadrightarrow \Gamma_{\mathbb{Q}}$ composed with α, and the $G_{\mathbb{Q}}$-action on T_α is via $\rho_\alpha = \rho_E \otimes \alpha$. Recall that as E has ordinary reduction at p, there is a unique $G_{\mathbb{Q}_p}$-stable $\mathbb{Z}_p$-summand $\mathrm{Fil}^+(T_pE) \subset T_pE$ of rank one such that $T_pE/\mathrm{Fil}^+(T_pE)$ is unramified. We put $\mathrm{Fil}^+(T_\alpha) := \mathrm{Fil}^+(T_pE) \otimes_{\mathbb{Z}_p} R(\alpha)$, $\mathrm{Fil}^+(V_\alpha) := \mathrm{Fil}^+(T_\alpha) \otimes_R \Phi$, and $\mathrm{Fil}^+(W_\alpha) := \mathrm{Fil}^+(T_\alpha) \otimes_R \Phi/R$.

Let M denote any of the modules in (3.1) or a quotient T_α/IT_α for a non-zero ideal $I \subset R$. We define a *Selmer structure* $\mathcal{F}$ on M to be a finite set $\Sigma = \Sigma(\mathcal{F})$ of places of $\mathbb{Q}$ containing ∞, the prime p, and the primes where M is ramified, together with a choice of a submodule of *local conditions* $\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}_w, M) \subset \mathrm{H}^1(\mathbb{Q}_w, M)$ for every $w \in \Sigma$, similarly as in §1.1.1. The associated *Selmer group* is then defined by

$$\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}, M) := \ker\left\{\mathrm{H}^1(\mathbb{Q}^\Sigma/\mathbb{Q}, M) \to \prod_{w\in\Sigma} \frac{\mathrm{H}^1(\mathbb{Q}_w, M)}{\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}_w, M)}\right\},$$

where $\mathbb{Q}^\Sigma$ is the maximal extension of $\mathbb{Q}$ unramified outside Σ. The local conditions of interest in this setting are the following:

- For a finite prime $\ell \neq p$, the *finite* (or *unramified*) local condition:
$$\mathrm{H}^1_f(\mathbb{Q}_\ell, V_\alpha) := \ker\{\mathrm{H}^1(\mathbb{Q}_\ell, V_\alpha) \to \mathrm{H}^1(\mathbb{Q}_\ell^{\mathrm{ur}}, V_\alpha)\}.$$
- The *ordinary* condition at p:
$$\mathrm{H}^1_{\mathrm{ord}}(\mathbb{Q}_p, V_\alpha) := \mathrm{im}\{\mathrm{H}^1(\mathbb{Q}_p, \mathrm{Fil}^+_p(V_\alpha)) \to \mathrm{H}^1(\mathbb{Q}_p, V_\alpha)\}.$$
- The *relaxed condition* at ℓ: $\mathrm{H}^1_{\mathrm{rel}}(\mathbb{Q}_\ell, V_\alpha) = \mathrm{H}^1(\mathbb{Q}_\ell, V_\alpha)$.
- The *strict condition* at ℓ: $\mathrm{H}^1_{\mathrm{str}}(\mathbb{Q}_\ell, V_\alpha) = \mathrm{H}^1(\mathbb{Q}_\ell, V_\alpha)$.

The corresponding local conditions for $M \in \{T_\alpha, W_\alpha, T_\alpha/IT_\alpha\}$ are defined by propagation. (Thus, for example, $\mathrm{H}^1_{\mathrm{str}}(\mathbb{Q}_\ell, T_\alpha) = \mathrm{H}^1(\mathbb{Q}_\ell, T_\alpha)_{\mathrm{tor}}$ and $\mathrm{H}^1_{\mathrm{rel}}(\mathbb{Q}_\ell, W_\alpha) = \mathrm{H}^1(\mathbb{Q}_\ell, W_\alpha)_{\mathrm{div}}$.) For $M = T_\alpha/IT_\alpha$, with $I \subset R$ a non-zero ideal, we also consider:

- The *transverse* local condition at a prime $\ell \neq p$ is
$$\mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, M) := \ker\{\mathrm{H}^1(\mathbb{Q}_\ell, M) \to \mathrm{H}^1(\mathbb{Q}_\ell(\mu_\ell), M)\}.$$

For $\circ \in \{\mathrm{rel}, \mathrm{ord}, \mathrm{str}\}$ we put

$$\mathrm{H}^1_{\mathcal{F}_\circ}(\mathbb{Q}_\ell, V_\alpha) := \begin{cases} \mathrm{H}^1_\circ(\mathbb{Q}_p, V_\alpha) & \text{if } \ell = p, \\ \mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}_\ell, V_\alpha) & \text{else,} \end{cases}$$

and let $\mathcal{F}_\circ$ also denote the Selmer structures similarly defined on T_α, W_α, and T_α/IT_α.

Given a Selmer structure $\mathcal{F}$, and $n \in \mathbb{Z}$ square-free and coprime to p, we define the Selmer structure $\mathcal{F}(n)$ as follows:

$$\mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}_\ell, T_\alpha) = \begin{cases} \mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_\alpha) & \text{if } \ell \mid n, \\ \mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_\alpha) & \text{if } \ell \nmid n. \end{cases}$$

Also, for $M^*_\alpha = \mathrm{Hom}(M_\alpha, \mu_{p^\infty})$ (so $T^*_\alpha \simeq W_{\alpha^{-1}}$), we let $\mathcal{F}^*$ be the Selmer structure on M^* determined by the orthogonal complements of $\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}_\ell, M)$ under local Tate duality $\mathrm{H}^1(\mathbb{Q}_\ell, M) \times \mathrm{H}^1(\mathbb{Q}_\ell, M^*) \to \mathrm{H}^2(\mathbb{Q}_\ell, \mu_{p^\infty}) = \mathbb{Q}_p/\mathbb{Z}_p$.

We define the Bloch–Kato Selmer structure $\mathcal{F}_{\mathrm{BK}}$ to be the Selmer structure given by $\mathrm{H}^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_\ell, M) = \mathrm{H}^1_f(\mathbb{Q}_\ell, M)$ for all primes ℓ and $M \in \{T_\alpha, V_\alpha, W_\alpha, T_\alpha/IT_\alpha\}$. Note that $\mathcal{F}^*_{\mathrm{BK}}$ is just the Bloch–Kato Selmer structure for $M^* = \mathrm{Hom}(M, \mu_{p^\infty})$. From here on, we put

$$\mathcal{F} = \mathcal{F}_{\mathrm{BK,rel}}, \quad \mathcal{F}^* = \mathcal{F}_{\mathrm{BK,str}}.$$

Later on, in the proof of Proposition 3.3.1, we shall also need to consider the Selmer structure $\mathcal{F}_{\mathrm{ord}} = \mathcal{F}_{\mathrm{BK,ord}}$.

3.1.2. *Kato's Kolyvagin system for T_f.* Let $f = \sum_{n=1}^\infty a_n q^n \in S_2(\Gamma_0(N))$ be the newform attached to E, with associated p-adic Galois representation V_f constructed as the maximal quotient of $\mathrm{H}^1_{\mathrm{et}}(\overline{Y_1(N)}, \mathbb{Q}_p(1))$ on which the Hecke operators T_n act as multiplication by a_n. After possibly replacing E by an isogenous elliptic curve, we may suppose that the p-adic Tate module T_pE is isomorphic to the $\mathbb{Z}_p$-lattice $T_f \subset V_f$ generated by the image of $\mathrm{H}^1_{\mathrm{et}}(\overline{Y_1(N)}, \mathbb{Z}_p(1))$ in V_f (in other words, E is the elliptic curve denoted $E_\bullet$ in [Wut14]).

Put $T = T_pE$, and let

$$\{z_n \in \mathrm{H}^1(\mathbb{Q}(\mu_n), T)\}_n$$

be the Euler system construction by Kato [Kat04] (see esp. [*op. cit.*, Ex. 1.3.3]). Here n runs over the positive integers coprime to cdN, for a fixed pair of integers $c, d \equiv 1 \pmod N$ used in the construction of the classes z_n, and $\mathbb{Q}(\mu_n)$ denotes the cyclotomic extension of $\mathbb{Q}$ obtained by adjoining the n-th roots of unity. For varying n, the classes z_n satisfy the following *norm relations*:

$$\mathrm{cores}^{\mathbb{Q}(\mu_{n\ell})}_{\mathbb{Q}(\mu_n)}(z_{n\ell}) = \begin{cases} z_n & \ell \mid n, \\ P_\ell(\mathrm{Frob}_\ell^{-1}) z_n & \text{otherwise,} \end{cases} \tag{3.2}$$

where $P_\ell(x) = \det(1 - \mathrm{Frob}_\ell^{-1} x \,|\, T)$ is the characteristic polynomial of a geometric Frobenius at ℓ.

We outline the construction of the Kolyvagin system derived from Kato's Euler system classes. Denote by $\mathcal{L}_0$ the set of primes ℓ with $(\ell, cdpN) = 1$. Consider

$$\mathcal{L}_E := \{\ell \in \mathcal{L}_0 :\ \ell \equiv 1 \pmod p \text{ and } a_\ell \equiv \ell + 1 \pmod p\}.$$

Fix a subset $\mathcal{L} \subset \mathcal{L}_E$, and let $\mathcal{N} = \mathcal{N}(\mathcal{L})$ be the set of squarefree products of primes $\ell \in \mathcal{L}$. For $\ell \in \mathcal{L}$ define the ideal

$$I_\ell = (\ell - 1, a_\ell - \ell - 1) \subset \mathbb{Z}_p. \tag{3.3}$$

and for $n \in \mathcal{N}$, let $I_n = \sum_{\ell | n} I_\ell$. Let $G_n = \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$. The Kolyvagin derivative operator $D_n \in \mathbb{Z}[G_n]$ at $n \in \mathcal{N}$ is defined by

$$D_n = \prod_{\ell | n} \sum_{i=1}^{\ell - 2} i \sigma_\ell^i,$$

where σ_ℓ is a generator of G_ℓ. Then one easily checks that the natural image of $D_n z_n$ in $\mathrm{H}^1(\mathbb{Q}(\mu_n), T/I_nT)$ is fixed by G_n, and $\kappa_n^{\mathrm{Kato}} \in \mathrm{H}^1(\mathbb{Q}, T/I_nT)$ is defined to be its preimage under the restriction map

$$\mathrm{H}^1(\mathbb{Q}, T/I_nT) \xrightarrow{\mathrm{res}} \mathrm{H}^1(\mathbb{Q}(\mu_n), T/I_nT)^{G_n} \tag{3.4}$$

By ($\mathrm{tor}_{\mathbb{Q}}$) and our assumptions on n, the restriction map (3.4) is an isomorphism, and so κ_n^{Kato} is well-defined. One can show that after a slight modification (see [MR04, §§3.2, 6.2] and [Rub11, Thm. 4.3.1]) the resulting classes – still denoted κ_n^{Kato} – satisfy

$$\kappa_n^{\mathrm{Kato}} \in \mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T/I_nT)$$

and form a Kolyvagin system for $(T, \mathcal{F}, \mathcal{L})$ in the sense of [MR04], i.e., they satisfy the *finite-singular relations*, which in particular imply that

$$\mathrm{ord}(\mathrm{loc}_\ell(\kappa_n^{\mathrm{Kato}})) = \mathrm{ord}(\mathrm{loc}_\ell(\kappa_{n\ell}^{\mathrm{Kato}})) \quad \text{for every } n \in \mathcal{N}, \ell \in \mathcal{L} \text{ such that } \ell \nmid n. \tag{3.5}$$

Moreover, similarly as in the setting of Heegner points, one can show that reducing such a Kolyvagin system modulo p^k gives a Kolyvagin system for $E[p^k]$ (see [MR04, Prop. 5.2.9 and Prop. 6.2.2]).

3.1.3. *The Λ-adic Kolyvagin system.* The Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\Gamma_{\mathbb{Q}}]]$ is equipped with a $G_{\mathbb{Q}}$-action given by the character $\Psi : G_{\mathbb{Q}} \to \Lambda^\times$ arising from the projection $G_{\mathbb{Q}} \twoheadrightarrow \Gamma_{\mathbb{Q}}$.

Let $\mathbb{Q}(\mu_{p^\infty})$ be the extension of $\mathbb{Q}_\infty$ obtained by adjoining to $\mathbb{Q}$ all p-power roots of unity. In light of the norm relations (3.2), for every $n \in \mathcal{N}$ the classes z_{np^k} define an element

$$z_{n,\infty} := \{z_{np^k}\}_k \in \varprojlim_k \mathrm{H}^1(\mathbb{Q}(\mu_{np^k}), T) \simeq \mathrm{H}^1(\mathbb{Q}(\mu_n), T \otimes \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]),$$

where the inverse limits are with respect to the corestriction maps and the isomorphism follows from Shapiro's lemma. Writing $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \Delta \times \Gamma_{\mathbb{Q}}$ and letting $\mathbf{T} = T \otimes_{\mathbb{Z}_p} \Lambda$, we can take the projection to the component where the action of Δ is trivial, obtaining classes

$$\mathbf{z}_n \in \mathrm{H}^1(\mathbb{Q}(\mu_n), \mathbf{T}).$$

Since $\Gamma_{\mathbb{Q}}$ is a pro-p group, the assumption ($\mathrm{tor}_{\mathbb{Q}}$) implies that $E(\mathbb{Q}_\infty)[p] = 0$. Therefore the same construction as above gives classes

$$\boldsymbol{\kappa}_n^{\mathrm{Kato}} \in \mathrm{H}^1(\mathbb{Q}, \mathbf{T}/I_n\mathbf{T})$$

that form a Kolyvagin system for $(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{L})$, where $\mathcal{F}_\Lambda$ is the Selmer structure given by $\mathrm{H}^1_{\mathcal{F}_\Lambda}(\mathbb{Q}_\ell, \mathbf{T}) = \mathrm{H}^1(\mathbb{Q}_\ell, \mathbf{T})$ for all $\ell \in \Sigma$ (see [MR04, §§5.3, 6.2]).

3.1.4. *Kolyvagin system for cyclotomic twists.* We are interested in the image of this system in the cohomology of T_α for characters $\alpha : \Gamma_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ with $\alpha \equiv 1 \mod p^m$ and $m \gg 0$.

For any $\alpha : \Gamma_{\mathbb{Q}} \to \mathbb{Z}_p^\times$, $\mathfrak{P} = (\gamma - \alpha(\gamma))$ is a height one prime ideal of Λ such that the completion of $\Lambda/\mathfrak{P}$ is $\mathbb{Z}_p$. Composing $\Psi : G_{\mathbb{Q}} \to \Lambda^\times$ with the natural map $\Lambda \to \Lambda/\mathfrak{P}$ recovers the character α. By [MR04, §5.3] (see in particular Corollary 5.3.15 in *op.cit.*), the image of the Kolyvagin system $\{\boldsymbol{\kappa}_n^{\mathrm{Kato}}\}_{n \in \mathcal{N}}$ via the natural map $\mathbf{T} \to T_\alpha$ specializes to a Kolyagin system

$$\{\boldsymbol{\kappa}_n^{\mathrm{Kato}}(\alpha)\}_{n \in \mathcal{N}}$$

for $(T_{\mathfrak{P}}, \mathcal{F}, \mathcal{L})$. The following is the analogue of Lemma 1.1.5, and is proved in the same manner.

Lemma 3.1.1. *Suppose $\alpha \equiv 1 \pmod{p^m}$. For all $n \in \mathcal{N}^{(m)}$ we have $\boldsymbol{\kappa}_n^{\mathrm{Kato}}(\alpha) \equiv \kappa_n^{\mathrm{Kato}} \pmod{p^m}$.*

Finally, to conclude the parallel with §1.1.3, we recall the result on the nonvanishing of $\boldsymbol{\kappa}_1^{\mathrm{Kato}}$ and, therefore, by the previous lemma, of $\boldsymbol{\kappa}_1^{\mathrm{Kato}}(\alpha_m)$ for $m \gg 0$.

Theorem 3.1.2 (Kato–Rohrlich)**.** *For $m \gg 0$ and any $\alpha \equiv 1 \pmod{p^m}$, the class $\boldsymbol{\kappa}_1^{\mathrm{Kato}}(\alpha)$ is nonzero.*

Proof. This follows from a combination of Rohrlich's results [Roh84], implying the nonvanishing of the Mazur–Swinnerton-Dyer p-adic L-function $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$, and Kato's explicit reciprocity law [Kat04, Thm. 16.6] (which we recall in the next section) relating $\boldsymbol{\kappa}_1^{\mathrm{Kato}}$ with $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$. □

3.2. **Cyclotomic Main Conjecture and results.**

3.2.1. *The p-adic L-function.* We recall the existence of the cyclotomic p-adic L-function attached to E. Given a modular parametrisation $\pi_E : X_0(N) \to E$, we denote by $c_E \in \mathbb{Z}$ the corresponding Manin constant. Let ω_E be a minimal differential on E. Pick generators $\delta^\pm$ of $H_1(E,\mathbb{Z})^\pm$, and define the Néron periods $\Omega_E^\pm$ by

$$\Omega_E^\pm = \int_{\delta^\pm} \omega_E.$$

We normalize the $\delta^\pm$ so that $\Omega_E^+ \in \mathbb{R}_{>0}$ and $\Omega_E^- \in i\mathbb{R}_{\geq 0}$. We also let α_p be the p-adic unit root of $x^2 - a_p(f)x + p$, where $a_p(f)$ is the p-th Fourier coefficient of the modular form f attached to E.

Theorem 3.2.1 (Mazur–Swinnerton-Dyer [MSD74], Wüthrich [Wut14])**.** *There exists an element $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q}) \in \Lambda_{\mathbb{Q}}$ such that for any finite order character χ of $\Gamma_{\mathbb{Q}}$ of conductor p^r, we have*

$$\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})(\chi) = \begin{cases} \frac{p^r}{\tau(\overline{\chi})\alpha_p^r} \cdot \frac{L(E,\overline{\chi},1)}{\Omega_E^+} & \textit{if } r > 0, \\ (1-\alpha_p^{-1})^2 \cdot \frac{L(E,1)}{\Omega_E^+} & \textit{if } r = 0, \end{cases}$$

where $\tau(\overline{\chi}) = \sum_{a \bmod p^r} \overline{\chi}(a) e^{2\pi i a/p^r}$ is the usual Gauss sum.

3.2.2. *Kato's explicit reciprocity law.* Kato defines in [Kat04, §13.9] a modification $\mathbf{z}_{\gamma,0}^{(p)}$ of the class $\boldsymbol{\kappa}_1^{\mathrm{Kato}}$, with $\gamma = \delta(f,1,\xi)$ in the notations of *op. cit.*, where $\xi \in \mathrm{SL}_2(\mathbb{Z})$ is the auxiliary matrix used in the construction of Kato's Euler system. More precisely, he first defines

$$\mathbf{z}_\gamma^{(p)} \in \mathrm{H}^1(\mathbb{Q}, T \otimes \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]) \otimes \mathbb{Q}_p$$

by multiplying $\{z_{p^k}\}_k$ by some factors depending on the auxiliary integers c, d and by the Euler factors at the bad primes, and $\mathbf{z}_{\gamma,0}^{(p)} \in \mathrm{H}^1(\mathbb{Q}, \mathbf{T}) \otimes \mathbb{Q}_p$ is defined to be the projection to the trivial component for the action of Δ. Kato's explicit reciprocity law [Kat04, Thm. 16.6] then relates $\mathbf{z}_{\gamma,0}^{(p)}$ to $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$, possibly up to some power of p accounting for the different periods (which depend on the choice of ξ). In particular, Kato's result implies (see [Rub98, Cor. 7.2]) that the natural image of $\boldsymbol{\kappa}_1^{\mathrm{Kato}}$ under the Coleman map

$$\mathrm{Col}_\infty : \mathrm{H}^1_s(\mathbb{Q}_p, \mathbf{T}) \to \Lambda,$$

where $\mathrm{H}^1_s(\mathbb{Q}_p, \mathbf{T}) := \mathrm{H}^1(\mathbb{Q}_p, \mathbf{T})/\mathrm{H}^1(\mathbb{Q}_p, \mathrm{Fil}_p^+ T \otimes_{\mathbb{Z}_p} \Lambda)$, is related to an imprimitive variant of $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$. More precisely, taking c, d to be $\not\equiv 1 \pmod{p}$, there exists $t_1 \in \mathbb{Z}$ depending only on E such that

$$\mathrm{Col}_\infty(\mathrm{loc}_s(\boldsymbol{\kappa}_1^{\mathrm{Kato}})) \sim_p p^{t_1} \prod_{\ell \mid N} (1 - a_\ell \ell^{-1} \gamma_\ell^{-1}) \mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q}), \tag{3.6}$$

where γ_ℓ denotes the image of the arithmetic Frobenius at ℓ in $\Gamma_{\mathbb{Q}}$.

In particular, specialising at cyclotomic characters, we can obtain the following result.

Lemma 3.2.2. *Let $\alpha : \Gamma_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ be a crystalline character with Hodge–Tate weight $n \leq 0$ with $n \equiv 0 \pmod{p-1}$ and such that $\alpha \equiv 1 \pmod{p^m}$. Then there exist integers $\mathcal{M} \in \mathbb{Z}_{>0}$ and $h \in \mathbb{Z}$, both independent of α, such that if $m \geq \mathcal{M}$ then $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})(\alpha^{-1}) \neq 0$ and*

$$\#\left(\mathbb{Z}_p/\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})(\alpha^{-1})\right) \cdot p^h \sim_p \#\left(\mathrm{H}^1_s(\mathbb{Q}_p, T_\alpha)/\mathbb{Z}_p \cdot \mathrm{loc}_s(\boldsymbol{\kappa}_1^{\mathrm{Kato}}(\alpha))\right),$$

where $\mathrm{H}^1_s(\mathbb{Q}_p, T_\alpha) := \frac{\mathrm{H}^1(\mathbb{Q}_p, T_\alpha)}{\mathrm{H}^1_{\mathrm{ord}}(\mathbb{Q}, T_\alpha)}$ and loc_s is the composite of the localisation map $\mathrm{loc}_p : \mathrm{H}^1(\mathbb{Q}, T_\alpha) \to \mathrm{H}^1(\mathbb{Q}_p, T_\alpha)$ and the natural quotient map.

Proof. This follows from a similar argument as in Lemma 1.2.3. Indeed, the map Col_∞ is an isomorphism in our setting (see [Kat04, Prop. 17.11]), and we claim that the specialization map $\mathrm{H}^1_s(\mathbb{Q}_p,\mathbf{T})\to\mathrm{H}^1_s(\mathbb{Q}_p,T_\alpha)$ is surjective. From the definitions we have a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{H}^1_s(\mathbb{Q}_p,\mathbf{T}) & \longrightarrow & \mathrm{H}^1(\mathbb{Q}_p,\mathrm{Fil}^-\mathbf{T}) & \xrightarrow{e} & \mathrm{H}^2(\mathbb{Q}_p,\mathrm{Fil}^+\mathbf{T}) \\ & & \downarrow a & & \downarrow b & & \downarrow c \\ 0 & \longrightarrow & \mathrm{H}^1_s(\mathbb{Q}_p,T_\alpha) & \longrightarrow & \mathrm{H}^1(\mathbb{Q}_p,\mathrm{Fil}^-T_\alpha) & \xrightarrow{f} & \mathrm{H}^2(\mathbb{Q}_p,\mathrm{Fil}^+T_\alpha), \end{array}$$

where we have written $\mathrm{Fil}^\pm\mathbf{T}$ for $\mathrm{Fil}^\pm T\otimes_{\mathbb{Z}_p}\Lambda$. The vertical arrows are the natural specialization maps. By Tate's local duality, $\mathrm{H}^2(\mathbb{Q}_p,F^+\mathbf{T})$ is dual to

$$\mathrm{H}^0(\mathbb{Q}_p,\mathrm{Fil}^-T\otimes_{\mathbb{Z}_p}\Lambda^*)=\mathrm{H}^0(\mathbb{Q}_{\infty,p},\tilde{E}[p^\infty])=\tilde{E}(\mathbb{F}_p)[p^\infty],$$

using that $\mathbb{Q}_{\infty,p}/\mathbb{Q}_p$ is totally ramified for the last equality. The same argument shows that $\mathrm{H}^2(\mathbb{Q}_p,\mathrm{Fil}^+T_\alpha)$ is dual to $\tilde{E}(\mathbb{F}_p)[p^\infty]$ and it follows that c is an isomorphism. So replacing the right-most column with the images of the maps d and e yields a commutative diagram with short exact rows and columns and with the right-most arrow an injection. Applying the snake lemma to this diagram then yields $\mathrm{coker}(a)\simeq\mathrm{coker}(b)$. The latter cokernel is given by $\mathrm{H}^2(\mathbb{Q}_p,\mathrm{Fil}^-\mathbf{T})[\gamma-\alpha(\gamma)]$, which is dual to $\mathrm{H}^0(\mathbb{Q}_{\infty,p},F^+E[p^\infty])/(\gamma-\alpha(\gamma))$. Since the $\mathbb{Q}_{p,n}$-rational p-torsion in the formal group of E is trivial for all n, this shows that b is surjective and hence that a is surjective, as claimed.

Now setting $h:=t_1+t_2$ where $t_2:=\sum_{\ell\mid N}\mathrm{ord}_p(1-a_\ell\ell^{-1})$, and noting that $\sum_{\ell\mid N}\mathrm{ord}_p(1-a_\ell\ell^{-1}\alpha(\gamma_\ell^{-1}))$ is equal to t_2 for m sufficiently large, (3.6) yields the result. □

Remark 3.2.3. Note that crystalline characters satisfying the assumptions of Lemma 3.2.2 are just the characters ϵ^n, $n\geq 0$ an integer such that $n\equiv 0 \mod (p-1)$, for ϵ the p-adic cyclotomic character.

3.2.3. *Rational cyclotomic Main Conjecture.* The Pontryagin dual $\Lambda^\vee$ is equipped with a $G_\mathbb{Q}$-action via the inverse of the character $\Psi: G_\mathbb{Q}\to\Lambda^\times$ arising from the projection $G_\mathbb{Q}\twoheadrightarrow\Gamma_\mathbb{Q}$.

Let $\mathbf{M}=T_pE\otimes\Lambda^\vee$, and put

$$\mathrm{H}^1_{\mathrm{ord}}(\mathbb{Q}_p,\mathbf{M})=\mathrm{im}\{\mathrm{H}^1(\mathbb{Q}_p,\mathrm{Fil}^+(T_pE)\otimes\Lambda^\vee)\to\mathrm{H}^1(\mathbb{Q}_p,\mathbf{M})\},$$

where $\mathrm{Fil}^+(T_pE)=\ker\{T_pE\to T_p\tilde{E}\}$ is the kernel of reduction. The *ordinary Selmer group* $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(\mathbb{Q},\mathbf{M})$ is

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(\mathbb{Q},\mathbf{M}):=\ker\left\{\mathrm{H}^1(\mathbb{Q}^\Sigma/\mathbb{Q},\mathbf{M})\to\prod_{w\in\Sigma,w\nmid p}\mathrm{H}^1(\mathbb{Q}_w,\mathbf{M})\times\frac{\mathrm{H}^1(\mathbb{Q}_p,\mathbf{M})}{\mathrm{H}^1_{\mathrm{ord}}(\mathbb{Q}_p,\mathbf{M})}\right\},$$

and we write $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)$ for its Pontryagin dual.

We recall the statement of the Iwasawa Main Conjecture formulated by Mazur in [Maz72].

Conjecture 3.2.4. *The module $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)$ is Λ-torsion, with*

$$\mathrm{char}_\Lambda\left(\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)\right)=(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q}))$$

as ideals in Λ.

In the following, we shall refer to the statement of Conjecture 3.2.4 with Λ replaced by $\Lambda\otimes\mathbb{Q}_p$ as the *rational cyclotomic Main Conjecture*. It follows from the results of [Sch87, PR89] that this is invariant under isogenies.

The first cases of Conjecture 3.2.4 were proved by Rubin [Rub91] when $E/\mathbb{Q}$ has complex multiplication. In the non-CM case, the conjecture was proved in [Kat04, SU14] (residually irreducible case) and [Kat04, GV00] (residually reducible case) under mild hypotheses. More recently, we have the following.

Theorem 3.2.5. *Suppose $p>2$ is a prime of good ordinary reduction for E.*

(i) *If $E[p]^{ss}=\mathbb{F}_p(\phi)\oplus\mathbb{F}_p(\psi)$ as $G_\mathbb{Q}$-modules with $\phi|_{G_p}\neq\mathbb{1},\omega$, then Conjecture 3.2.4 holds.*
(ii) *If $E[p]$ satisfies (irr), then the rational cyclotomic Main Conjecture holds.*

Proof. This is shown in [CGS23] in case (i), and in [Wan15] in case (ii). □

3.3. **Nonvanishing of Kato's Kolyvagin system.** In this section we prove Theorem C in the Introduction. The key ingredients are:

(1) The nonvanishing of $\boldsymbol{\kappa}_1^{\rm Kato}$ (Theorem 3.1.2)
(2) For a character $\alpha:\Gamma_{\mathbb{Q}}\rightarrow R^\times$ sufficiently close to 1, an estimate on the divisibility index of $\boldsymbol{\kappa}_1^{\rm Kato}(\alpha)$ in terms the length of the dual Selmer group and the Tamagawa factors of E (Proposition 3.3.1 below).
(3) A Kolyvagin system bound with controlled error terms (Theorem 3.3.3 below).

The cyclotomic Main Conjecture[3] enters into the proof of (2). With these ingredients in hand, the proof of Theorem C proceeds along similar lines as in §2.

3.3.1. *Cyclotomic control theorem.* As above, we consider the $G_{\mathbb{Q}}$-modules

$$T_\alpha:=T_pE\otimes_{\mathbb{Z}_p}\mathbb{Z}_p(\alpha),\quad V_\alpha:=T_\alpha\otimes_{\mathbb{Z}_p}\mathbb{Q}_p,\quad W_\alpha:=T_\alpha\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/Z_p$$

for a character $\alpha:\Gamma_{\mathbb{Q}}\rightarrow\mathbb{Z}_p^\times$. Recall that we set $\mathcal{F}=\mathcal{F}_{\rm BK,rel}$ and $\mathcal{F}^*=\mathcal{F}_{\rm BK,str}$.

Proposition 3.3.1. *Let $\mathcal{M}$ be as in Lemma 3.2.2, and suppose $\alpha:\Gamma_{\mathbb{Q}}\rightarrow\mathbb{Z}_p^\times$ is such that $\alpha\equiv 1\pmod{p^m}$ for $m\geq\mathcal{M}$ (so in particular $\mathcal{L}_p^{\rm MSD}(E/\mathbb{Q})(\alpha^{-1})\neq 0$ and $\mathcal{L}_p^{\rm MSD}(E/\mathbb{Q})(\alpha)\neq 0$). If Conjecture 3.2.4 holds then*

$$\mathrm{length}_R(\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q},W_{\alpha^{-1}}))+\sum_{\ell\mid N}\mathrm{ord}_p(c_\ell(\alpha^{-1}))+2t_3+h=[\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q},T_\alpha):\mathbb{Z}_p\cdot\boldsymbol{\kappa}_1^{\rm Kato}(\alpha)],$$

where $c_\ell(\alpha^{-1})=\#\mathrm{H}^1_{\rm ur}(\mathbb{Q}_\ell,W_{\alpha^{-1}})$, $t_3=\mathrm{ord}_p(\#\mathrm{H}^0(\mathbb{Q}_p,E[p^\infty]))$, and $h=t_1+t_2$ is as in Lemma 3.2.2.

Proof. Poitou–Tate duality gives rise to the exact sequence

$$0\rightarrow\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q},W_{\alpha^{-1}})\rightarrow\mathrm{H}^1_{\mathcal{F}_{\rm ord}}(\mathbb{Q},W_{\alpha^{-1}})\xrightarrow{\mathrm{loc}_p}\mathrm{H}^1_{\rm ord}(\mathbb{Q}_p,W_{\alpha^{-1}})\xrightarrow{\beta}\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q},T_\alpha)^\vee\rightarrow\mathrm{H}^1_{\mathcal{F}_{\rm ord}}(\mathbb{Q},T_\alpha)^\vee\rightarrow 0. \tag{3.7}$$

By the cyclotomic Main Conjecture and Mazur's control theorem, the nonvanishing of $\mathcal{L}_p^{\rm MSD}(E/\mathbb{Q})(\alpha)$ and $\mathcal{L}_p^{\rm MSD}(E/\mathbb{Q})(\alpha^{-1})$ implies that $\mathrm{H}^1_{\mathcal{F}_{\rm ord}}(\mathbb{Q},W_{\alpha^{-1}})$ and $\mathrm{H}^1_{\mathcal{F}_{\rm ord}}(\mathbb{Q},T_\alpha)$ are both finite. From (3.7), it follows that $\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q},W_{\alpha^{-1}})$ is also finite, and that $\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q},T_\alpha)$ has $\mathbb{Z}_p$-rank one; since the latter is torsion-free by ($\mathrm{tor}_{\mathbb{Q}}$), we have in fact $\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q},T_\alpha)\simeq\mathbb{Z}_p$. Moreover, by local Tate duality the map β is identified with the Pontryagin dual of the natural map

$$\mathrm{loc}_s:\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q},T_\alpha)\rightarrow\mathrm{H}^1_s(\mathbb{Q}_p,T_\alpha):=\frac{\mathrm{H}^1(\mathbb{Q}_p,T_\alpha)}{\mathrm{H}^1_{\rm ord}(\mathbb{Q},T_\alpha)},$$

and from the above we see that loc_s has finite cokernel, with

$$\#\mathrm{im}(\mathrm{loc}_p)=\#\mathrm{coker}(\mathrm{loc}_s). \tag{3.8}$$

Since by Lemma 3.2.2 the class $\boldsymbol{\kappa}_1^{\rm Kato}(\alpha)\in\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q},T_\alpha)$ is nonzero and has non-torsion image in $\mathrm{H}^1_s(\mathbb{Q}_p,T_\alpha)$, we find

$$\#\mathrm{coker}(\mathrm{loc}_s)=\frac{[\mathrm{H}^1_s(\mathbb{Q}_p,T_\alpha):\mathbb{Z}_p\cdot\mathrm{loc}_s(\boldsymbol{\kappa}_1^{\rm Kato}(\alpha))]}{[\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q},T_\alpha):\mathbb{Z}_p\cdot\boldsymbol{\kappa}_1^{\rm Kato}(\alpha)]}=\frac{\#(\mathbb{Z}_p/\mathcal{L}_p^{\rm MSD}(E/\mathbb{Q})(\alpha))\cdot p^h}{[\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q},T_\alpha):\mathbb{Z}_p\cdot\boldsymbol{\kappa}_1^{\rm Kato}(\alpha)]}. \tag{3.9}$$

On the other hand, letting $\mathcal{F}_E\in\Lambda$ be a generator of $\mathrm{char}_\Lambda(\mathfrak{X}_{\rm ord}(E/\mathbb{Q}_\infty))$, by a variant of [Gre99, Thm. 4.1] incorporating the twist by α with $m\gg 0$, we have

$$\begin{aligned}\#\mathbb{Z}_p/(\mathcal{F}_E(\alpha^{-1}))&\sim_p\#\mathrm{H}^1_{\mathcal{F}_{\rm ord}}(\mathbb{Q},W_{\alpha^{-1}})\cdot\prod_{\ell\mid N}c_\ell(\alpha^{-1})\cdot(\#\mathrm{H}^0(\mathbb{Q}_p,E[p^\infty]))^2\\&\sim_p\#\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q},W_{\alpha^{-1}})\cdot\#\mathrm{coker}(\mathrm{loc}_s)\cdot\prod_{\ell\mid N}c_\ell(\alpha^{-1})\cdot(\#\mathrm{H}^0(\mathbb{Q}_p,E[p^\infty]))^2,\end{aligned} \tag{3.10}$$

using (3.7) and (3.8) for the second equality. Since Conjecture 3.2.4 implies

$$\#\mathbb{Z}_p/(\mathcal{F}_E(\alpha^{-1}))=\#\mathbb{Z}_p/(\mathcal{L}_p^{\rm MSD}(E/\mathbb{Q})(\alpha^{-1}))$$

the result now follows from (3.9) and (3.10). □

We have the following analogue of Lemma 1.2.8.

[3] In fact, as will be clear from the proof, the "lower bound" on the size the Selmer group predicted by Conjecture 3.2.4 (or its rational version) suffices for the application to nonvanishing.

Lemma 3.3.2. *Assume that $\alpha : \Gamma_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ is such that $\alpha \equiv 1 \pmod{p^m}$, and $\ell \nmid p$ is a finite prime. Then $c_\ell(\alpha) \equiv c_\ell \pmod{\varpi^m}$, where c_ℓ is the p-part of the Tamagawa factor E at ℓ.*

Proof. The proof is exactly the same as the one of Lemma 1.2.8. □

Thus taking $\alpha : \Gamma_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ as in Proposition 3.3.1 sufficiently close to 1, from Lemma 3.3.2 we arrive at

$$\mathrm{length}_R(\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, W_{\alpha^{-1}})) + \sum_{\ell \mid N} \mathrm{ord}_p(c_\ell) + h' = \mathrm{ind}(\boldsymbol{\kappa}_1^{\mathrm{Kato}}(\alpha), \mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}, T_\alpha)), \tag{3.11}$$

where $h' := t_1 + t_2 + 2t_3$.

3.3.2. *Kolyvagin system bound.* The last ingredient we need is the following extension of [MR04, Thm. 5.2.2]. For a positive integer e we put

$$\mathcal{L}_{E,e} = \{\ell \in \mathcal{L}_E \ : \ I_\ell \subset p^e\mathbb{Z}_p\},$$

where $I_\ell \subset \mathbb{Z}_p$ is as in (3.3).

Theorem 3.3.3. *Suppose $\mathcal{L} \subset \mathcal{L}_E$ satisfies $\mathcal{L}_{E,e} \subset \mathcal{L}$ for $e \gg 0$. Let $\alpha : \Gamma_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ be a cyclotomic character such that $\alpha \equiv 1 \pmod{p^m}$. Suppose that there is a collection of cohomology classes*

$$\{\tilde{\kappa}_n \in \mathrm{H}^1(\mathbb{Q}, T_\alpha/I_nT_\alpha) \ : \ n \in \mathcal{N}\}$$

with $\tilde{\kappa}_1 \neq 0$ and that there is an integer $t \geq 0$, independent of n, such that $\{p^t\tilde{\kappa}_n\}_{n\in\mathcal{N}} \in \mathbf{KS}(T_\alpha, \mathcal{F}, \mathcal{L})$. Then $\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}, T_\alpha)$ has $\mathbb{Z}_p$-rank 1, $\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, W_{\alpha^{-1}})$ is finite, and there is a non-negative integer $\mathcal{E}$ depending only on T_pE such that

$$\mathrm{length}_R(\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, W_{\alpha^{-1}})) \leq \mathrm{ind}(\tilde{\kappa}_1) + \mathcal{E},$$

where $\mathrm{ind}(\tilde{\kappa}_1) = \mathrm{length}_{\mathbb{Z}_p}(\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}, T_\alpha)/\mathbb{Z}_p \cdot \tilde{\kappa}_1)$.

Proof. By the same argument as in the proof Theorem 1.3.1, the result for $t = 0$ easily implies the result for any $t \geq 0$, so it suffices to prove the former. Under hypothesis (sur), the result is shown in [MR04, Thm. 5.2.2]; the proof in the general case is given in §3.4 (see Theorem 3.4.1). □

Granted the results in §3.4, we are now ready to conclude the proof of Theorem C.

Proof of Theorem C. Arguing by contradiction, we assume that $\kappa_n = 0$ for every $n \in \mathcal{N}$, and take t such that

$$t > \sum_{\ell \mid N} \mathrm{ord}_p(c_\ell) + \mathcal{E} + h',$$

where $\mathcal{E}$ and h' are as in Theorem 3.3.3 and (3.11), respectively. Take $\alpha : \Gamma_{\mathbb{Q}} \to \mathbb{Z}_p^\times$, $\alpha \equiv 1 \pmod{p^m}$, as in Proposition 3.3.1, with $m \geq t$ and such that (3.11) holds. Then, letting $\mathcal{N} = \mathcal{N}(\mathcal{L}_m)$, from Lemma 3.1.1 we deduce the existence of a collection of cohomology classes $\{\tilde{\kappa}_{n,\alpha} \in \mathrm{H}^1(\mathbb{Q}, T_\alpha/I_nT_\alpha)\}_{n\in\mathcal{N}}$ defined by the relation $p^t \cdot \tilde{\kappa}_{n,\alpha} = \boldsymbol{\kappa}_n^{\mathrm{Kato}}(\alpha)$. By Theorem 3.1.2 and Theorem 3.3.3 we obtain

$$\mathrm{length}_{\mathbb{Z}_p}(\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, W_{\alpha^{-1}})) \leq \mathrm{ind}(\boldsymbol{\kappa}_1^{\mathrm{Kato}}(\alpha), \mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}, T_\alpha)) - t + \mathcal{E},$$

which by our choice of t contradicts (3.11). This concludes the proof of Theorem C assuming Conjecture 3.2.4. A straightforward modification of the above argument leads to the same conclusion just assuming the rational anticyclotomic Main Conjecture. □

Remark 3.3.4. Denote by $\mathscr{M}_\infty^{\mathrm{Kato}}$ the divisibility index of $\{\kappa_n^{\mathrm{Kato}}\}$. Similarly as in the proof of Theorem B, the above argument combined with Mazur–Rubin's structure theorem for $\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, W_{\alpha^{-1}})$ in terms of $\boldsymbol{\kappa}^{\mathrm{Kato}}(\alpha)$ (see [MR04, Thm. 5.2.12]) shows that under the following hypotheses:

(i) (sur) holds (so that $\mathcal{E} = 0$ in Theorem 3.3.3),
(ii) $h = 0$ in the notations of Lemma 3.2.2,
(iii) $a_p \not\equiv 1 \pmod{p}$ (so that $E(\mathbb{Q}_p)[p^\infty] = 0$ and $t_3 = 0$ in the notation of Proposition 3.3.1),

if Conjecture 3.2.4 holds, then

$$\mathscr{M}_\infty^{\mathrm{Kato}} = \sum_{\ell \mid N} \mathrm{ord}_p(c_\ell), \tag{3.12}$$

confirming [Kim22b, Conj. 1.10]. In particular, by the cases of Conjecture 3.2.4 established in [BCS23], (3.12) holds under the following hypotheses in addition to (i)-(iii): $p > 3$ and there exists an element $\sigma \in G_{\mathbb{Q}}$ fixing $\mathbb{Q}(\mu_{p^\infty})$ such that $T/(\sigma - 1)T$ is a free $\mathbb{Z}_p$-module of rank one.

3.4. **Extension of Mazur–Rubin's Selmer group bound.** In this section we prove Theorem 3.4.1 below. The result extends [MR04, Thm. 5.2.2] and might be of independent interest.

Let R be the ring of integers of a finite extension of $\mathbb{Z}_p$ with maximal ideal $\mathfrak{m}$ and uniformiser $\varpi \in \mathfrak{m}$. Let $\alpha : \Gamma_{\mathbb{Q}} \to R^\times$ be a cyclotomic character such that $\alpha \equiv 1 \pmod{\mathfrak{m}}$, and put

$$T = T_pE \otimes_{\mathbb{Z}_p} R(\alpha).$$

As above, we put $\mathcal{F} = \mathcal{F}_{\mathrm{BK,rel}}$, $\mathcal{F}^* = \mathcal{F}_{\mathrm{BK,str}}$, and let $\mathcal{L} \subset \mathcal{L}_E$ be a set of primes with $\mathcal{L}_{E,e} \subset \mathcal{L}$ for $e \gg 0$. We also put $\mathcal{N} = \mathcal{N}(\mathcal{L})$.

Theorem 3.4.1. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication, and let p be an odd prime of good reduction for E such that $E(\mathbb{Q})[p] = 0$. Suppose that there is a Kolyvagin system $\kappa = \{\kappa_n\}_{n\in\mathcal{N}} \in \mathbf{KS}(T, \mathcal{F}, \mathcal{L})$ with $\kappa_1 \neq 0$. Then $\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}, T)$ has R-rank one, $\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)$ is finite, and there exists a non-negative integer $\mathcal{E}$ depending only on T_pE and $\mathrm{rank}_{\mathbb{Z}_p}(R)$ such that*

$$\mathrm{length}_R(\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)) \leq \mathrm{ind}(\kappa_1) + \mathcal{E},$$

where $\mathrm{ind}(\kappa_1) = \mathrm{length}_R\big(\mathrm{H}^1_{\mathcal{F}}(K, T)/R\cdot\kappa_1\big)$. Moreover, $\mathcal{E} = 0$ if (sur) holds.

As preparation for the proof of Theorem 3.4.1, we collect some preliminary results from [MR04, §4.1], whose proof applies verbatim under the assumption $E(\mathbb{Q})[p] = 0$.

Lemma 3.4.2. *Let $k > 0$ and $T^{(k)} = T/\mathfrak{m}^k$. For every $n \in \mathcal{N}$ and $0 < i \leq k$ there are natural isomorphisms*

$$\mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T^{(k)}/\mathfrak{m}^iT^{(k)}) \xrightarrow{\sim} \mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T^{(k)}[\mathfrak{m}^i]) \xrightarrow{\sim} \mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T^{(k)})[\mathfrak{m}^i]$$

and

$$\mathrm{H}^1_{\mathcal{F}(n)^*}(\mathbb{Q}, T^*[\mathfrak{m}^i]) \xrightarrow{\sim} \mathrm{H}^1_{\mathcal{F}(n)^*}(\mathbb{Q}, T^*)[\mathfrak{m}^i]$$

induced by the maps $T^{(k)}/\mathfrak{m}^iT^{(k)} \xrightarrow{\varpi^{k-i}} T^{(k)}[\mathfrak{m}^i] \hookrightarrow T^{(k)}$ and the inclusion $T^*[\mathfrak{m}^i] \hookrightarrow T^*$, respectively.

Proof. This is [MR04, Lem. 4.1.1]. □

Theorem 3.4.3. *For every $k > 0$ and $n \in \mathcal{N}$, we have*

$$\mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T/\mathfrak{m}^k) \simeq R/\mathfrak{m}^k \oplus \mathrm{H}^1_{\mathcal{F}(n)^*}(\mathbb{Q}, T^*[\mathfrak{m}^k]).$$

Proof. Since our Selmer structure $\mathcal{F}$ has *core rank* $\chi(T, \mathcal{F}) = 1$ in the sense of [MR04] (see [*op. cit.*, Prop. 6.2.2]), the result follows from [MR04, Thm. 4.1.13]. □

By assumption the elliptic curve does not have CM, so there exists $\tau \in G_{\mathbb{Q}}$ such that $V_pE/(\tau-1)V_pE \simeq \mathbb{Q}_p$ since it follows by Serre's open image theorem [Ser72] that $\left(\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right)$ is in the image of ρ_E for some $0 \neq x \in \mathbb{Z}_p$. We fix τ such that $\rho_E(\tau) = \left(\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right)$ with $t' := v_p(x) = \min_m\{m : \left(\begin{smallmatrix}1 & y\\ 0 & 1\end{smallmatrix}\right) \in \mathrm{Im}(\rho_E), v_p(y) = m\}$. In particular, we have

$$(\tau) \qquad \tau_{|\mu_{p^\infty}} = 1 \quad \text{and} \quad T_pE/(\tau-1)T_pE \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p/p^{t'}.$$

Note that, since the first condition implies $\tau_{|\mathbb{Q}_\infty} = 1$ and α is a character of $\Gamma_{\mathbb{Q}}$, we also have $T/(\tau-1)T \simeq R \oplus R/\mathfrak{m}^t$, where $t = t' \cdot \mathrm{rank}_{\mathbb{Z}_p} R$.

Let $\mathcal{L}^{(k)}$ be the set of Kolyvagin primes "mod $\mathfrak{m}^k$", that is, the primes $\ell \nmid Np$ in $\mathcal{L}$ such that

(i) $T/(\mathfrak{m}^kT + (\mathrm{Frob}_\ell - 1)T) \simeq R/\mathfrak{m}^k \oplus R/\mathfrak{m}^{\min\{k,t\}}$,
(ii) $I_\ell = (\ell - 1, \det(1 - \mathrm{Frob}_\ell |T)) \subset \mathfrak{m}^k$.

Note that we can then see the reduction modulo $\mathfrak{m}^k$ of the Kolyvagin system for T yields a Kolyvagin system for $(T/\mathfrak{m}^kT, \mathcal{F}, \mathcal{L}^{(k)})$ given by classes $\kappa_n^{(k)} \in \mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T/\mathfrak{m}^kT)$ for $n \in \mathcal{N}^{(k)} = \mathcal{N}(\mathcal{L}^{(k)})$.

3.4.1. *The Čebotarev argument.* We recall the definitions of the error terms C_1, C_2 of [CGLS22, §3.3.1]. For $U = \mathbb{Z}_p^\times \cap \mathrm{im}(\rho_E)$ let

$$C_1 := \min\{v_p(u-1) \colon u \in U\}.$$

As U is an open subgroup, $C_1 < \infty$. Recall also that $\mathrm{End}_{\mathbb{Z}_p}(T_pE)/\rho_E(\mathbb{Z}_p[G_\mathbb{Q}])$ is a torsion $\mathbb{Z}_p$-module and let

$$C_2 := \min\bigl\{n \geq 0 \colon p^n \,\mathrm{End}_{\mathbb{Z}_p}(T_pE) \subset \rho_E(\mathbb{Z}_p[G_\mathbb{Q}])\bigr\}.$$

Let $d = \mathrm{rank}_{\mathbb{Z}_p} R$ and

$$e := d(C_1 + C_2 + t') = d(C_1 + C_2) + t,$$

where t' is determined by the choice of τ in (τ). For a finitely-generated torsion R-module M and $x \in M$, let

$$\mathrm{ord}(x) := \min\{m \geq 0 : \varpi^m \cdot x = 0\}.$$

The following result is the analogue of [CGLS22, Prop. 3.3.6].

Proposition 3.4.4. *Let $k > e$ and consider two classes $c_0 \in \mathrm{H}^1(\mathbb{Q}, T^{(k)})$ and $c_1 \in \mathrm{H}^1(\mathbb{Q}, (T^{(k)})^*)$. Then there exist infinitely many primes $\ell \in \mathcal{L}^{(k)}$ such that*

$$\mathrm{ord}(\mathrm{loc}_\ell(c_i)) \geqslant \mathrm{ord}(c_i) - e, \quad i = 0, 1.$$

Proof. Let $T_E^{(k)} = T_pE \otimes R/\mathfrak{m}^k \simeq (T_E^{(k)})^*$ and let L be the fixed field of the action of $G_\mathbb{Q}$ on $T_E^{(k+2)}$. Since $\mathbb{Q}(\mu_{p^{k+2}}) \subset L$, we have that $\mathbb{Q}_{p^{k+1}} \subset L$, where $\mathbb{Q}_{p^{k+1}}$ is the subfield of $\mathbb{Q}_\infty$ such that $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_{p^{k+1}}) \simeq p^{k+1}\mathbb{Z}_p$. We claim that $\alpha|_{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_{p^{k+1}})} \equiv 1 \mod \mathfrak{m}^k$, which in turn implies

$$\alpha|_{G_L} = 1 \mod \mathfrak{m}^k. \tag{3.13}$$

The claim follows from the assumption $\alpha \equiv 1 \mod \varpi$. If γ is a topological generator of $\Gamma_\mathbb{Q}$, we need to show that $\alpha(\gamma)^{p^{k+1}} \equiv 1 \mod \varpi^k$. Since $\alpha(\gamma) = 1 + \varpi x$ for some $x \in R$, $\alpha(\gamma)^{p^{k+1}} = 1 + \sum_{i=1}^{p^{k+1}} \binom{p^{k+1}}{i}(\varpi x)^i$. Since $\mathrm{ord}_p(\binom{p^{k+1}}{i}) = k + 1 - \mathrm{ord}_p(i)$, we find $\mathrm{ord}_\varpi(\binom{p^{k+1}}{i}\varpi^i) \geq (k+1)\,\mathrm{ord}_\varpi(p) - (\mathrm{ord}_\varpi(p) - 1)(\mathrm{ord}_p\, i) \geq (k+1)\,\mathrm{ord}_\varpi(p) - (\mathrm{ord}_\varpi(p) - 1)(k+1)$. The claim follows.

We therefore have the following identifications

$$\mathrm{H}^1(L, T^{(k)}) = \mathrm{Hom}(G_L, T_E^{(k)})^{(\alpha)} \subset \mathrm{Hom}(G_L, T_E^{(k)}), \tag{3.14}$$

$$\mathrm{H}^1(L, (T^{(k)})^*) = \mathrm{Hom}(G_L, T_E^{(k)})^{(\alpha^{-1})} \subset \mathrm{Hom}(G_L, T_E^{(k)}), \tag{3.15}$$

where the superscript $(\alpha^{\pm 1})$ denotes the submodule on which $G_\mathbb{Q}$ acts via $\alpha^{\pm 1}$. It then follows from [CGS23, (5.3)] that p^{C_1} annihilates $\mathrm{H}^1(\mathrm{Gal}(L/\mathbb{Q}), T^{(k)})$ and $\mathrm{H}^1(\mathrm{Gal}(L/\mathbb{Q}), (T^{(k)})^*)$ and hence, using the identifications (3.14),(3.15), we have

$$p^{C_1} \cdot \ker\bigl(\mathrm{H}^1(\mathbb{Q}, T^{(k)}) \to \mathrm{Hom}(G_L, T_E^{(k)})\bigr) = 0, \tag{3.16}$$

$$p^{C_1} \cdot \ker\bigl(\mathrm{H}^1(\mathbb{Q}, (T^{(k)})^*) \to \mathrm{Hom}(G_L, T_E^{(k)})\bigr) = 0. \tag{3.17}$$

We now consider the images of the c_i under the following natural maps

$$\begin{array}{ccccc} \mathrm{H}^1(\mathbb{Q}, M) & \longrightarrow & \mathrm{Hom}(G_L, T_E^{(k)}) & \longrightarrow & \mathrm{Hom}(G_L, T_E^{(k)}/(\tau-1)T_E^{(k)}) \\ c_i & \longmapsto & f_i & \longmapsto & f_i, \end{array}$$

where $M = T^{(k)}$ or $(T^{(k)})^*$ for $i = 0$ or $i = 1$, respectively, and the second map is induced by the projection $T_E^{(k)} \to T_E^{(k)}/(\tau-1)T_E^{(k)}$. By the definition of C_2, the image of f_i contains $p^{C_2}\,\mathrm{End}(T_p(E)) \cdot f_i(G_L)$. Since $\mathrm{ord}(f_i) \geq \mathrm{ord}(c_i) - \mathrm{ord}_\varpi(p)C_1$ by (3.16), , it follows that, letting $d_i = \mathrm{ord}(c_i) - e$,

$$R \cdot f_i(G_L) \supset \varpi^{k-d_i} T_E^{(k)}. \tag{3.18}$$

Let $J_i = \{\gamma \in G_L : \mathrm{ord}(f_i(\gamma)) \lneq d_i)\}$. This is a subgroup of G_L. We find

$$R \cdot f_i(J_i) \subset \varpi^{k-(d_i-1)} T_E^{(k)} + (\tau - 1)T_E^{(k)} \subsetneq \varpi^{k-d_i} T_E^{(k)},$$

where the last inclusion follows from the fact that $T_E^{(k)}/(\tau-1)T_E^{(k)} \simeq R/\mathfrak{m}^k \oplus R/\mathfrak{m}^t$; it must be strict, because if not $(\tau-1)T_E^{(k)} = \varpi^{k-d_i} T_E^{(k)}$ and this implies $k = t$. Combined with (3.18), this shows that $J_i \subsetneq G_L$ with index at least p. Now consider

$$B_i = \{\gamma \in G_L : \mathrm{ord}(f_i(\gamma\tau)) \lneq d_i)\}.$$

Note that, since $\gamma \in G_L$ acts trivially on $T_E^{(k)}$, $f_i(\gamma\tau) = f_i(\gamma) + f_i(\tau)$. Therefore for any $\gamma, \gamma' \in G_L$, we have $f_i(\gamma^{-1}\gamma') = -f_i(\gamma\tau) + f_i(\gamma'\tau)$. It follows that B_i is a coset of J_i. Since both J_1 and J_2 have index at least p in G_L and $p > 2$, we have shown

$$\text{there exists } \gamma \in G_L \setminus (B_1 \cup B_2).$$

Fix a choice of such a γ. We now let $\ell \nmid Np$ be any prime such that both c_is are unramified at ℓ and the conjugacy class of Frob_ℓ in $\mathrm{Gal}(L'/\mathbb{Q})$, where L' is the compositum of the fixed fields of the kernels of c_1 and c_2 restricted to G_L. The Čebotarev density theorem implies there are infinitely many such primes. By (3.13) and the fact that G_L acts trivially on $T_E^{(k)}$, Frob_ℓ acts as τ on $T^{(k)}$, therefore by (τ), we obtain

(i) $T^{(k)}/(\mathrm{Frob}_\ell - 1)T^{(k)} \simeq R/\mathfrak{m}^k \oplus R/\mathfrak{m}^t$ and $\det(1 - \mathrm{Frob}_\ell | T) = \det(1 - \tau | T) \equiv 0 \mod \mathfrak{m}^k$;
(ii) $\ell = \chi_{cyc}(\mathrm{Frob}_\ell) = \chi_{cyc}(\gamma\tau) = \det(\rho_E)(\gamma\tau) \equiv 1 \mod \mathfrak{m}^k$.

In particular we have shown ℓ is a Kolyvagin prime for $T^{(k)}$, that is, $\ell \in \mathcal{L}_E^{(k)}$. Moreover, since c_0, c_1 are both unramified at ℓ, we have $\mathrm{loc}_\ell(c_i) \in \mathrm{H}^1_f(\mathbb{Q}, T_E^{(k)}) \simeq T_E^{(k)}/(\mathrm{Frob}_\ell - 1)T_E^{(k)} \simeq R/\mathfrak{m}^k \oplus R/\mathfrak{m}^t$, where the first isomorphism is given by evaluation at Frob_ℓ and the second one follows from (i) above. In particular, $\mathrm{ord}(\mathrm{loc}_\ell(c_i))$ equals the order of $c_i(\mathrm{Frob}_\ell) = f_i(\gamma\tau)$, which, since $\gamma \in G_L \setminus (B_1 \cup B_2)$, is at least d_i, concluding the proof. □

Remark 3.4.5. Recall that, as it can be seen from the proof of [MR04, Thm. 4.1.13], the isomorphism of Theorem 3.4.3 is not canonical. Therefore if we take c_1 to be a class generating $R/\mathfrak{m}^k$ in $\mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T^{(k)})$ and $c_2 \in \mathrm{H}^1_{\mathcal{F}^*(n)}(\mathbb{Q}, T^{(k)})$, even though we have (non-canonical) isomorphisms $\mathrm{H}^1_f(\mathbb{Q}_\ell, (T^{(k)})^*) \simeq R/\mathfrak{m}^k \oplus R/\mathfrak{m}^t \simeq \mathrm{H}^1_f(\mathbb{Q}_\ell, T^{(k)})$, with $\ell \nmid n$, the Chebotarev result does not assert some "linear independence" of the localisations of the classes.

As warm up for the proof of Theorem 3.4.1, we first prove the following weaker result.

Proposition 3.4.6. *Assume* $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}, T)) = 1$ *and let* $s_1 = \mathrm{ind}(\kappa_1, \mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}, T))$. *For* $k \gg 0$ *chosen so that* $k > m + s_1 + 2e$, $\mathfrak{m}^{s_1+2e}\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, T^*) = 0$.

Proof. Choose $k \gg s_1 + 2e$ such that the image of κ_1 in $\mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}, T^{(k)})$ is non-zero and has index s_1. Then there exists $c_0 \in \mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}, T^{(k)})$ of order exactly k such that $\varpi^{s_1} c_0 = \kappa_1$. Let us write

$$\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, (T^{(k)})^*) = \bigoplus_{i=1}^{s} R/\varpi^{d_i} \cdot c_i, \quad d_1 \geq d_2 \geq \cdots \geq d_s.$$

This is a cyclic-module decomposition with factors of the indicated lengths d_i. We apply Proposition 3.4.4 to the classes c_0, c_1 to find a prime $\ell \in \mathcal{L}^{(k)}$ such that

$$\mathrm{ord}(\mathrm{loc}_\ell(c_0)) \geq k - e, \quad \mathrm{ord}(\mathrm{loc}_\ell(c_1)) \geq d_1 - e.$$

Recall that $\mathrm{H}^1_f(\mathbb{Q}_\ell, T^{(k)})$ and $\mathrm{H}^1_f(\mathbb{Q}_\ell, (T^{(k)})^*)$ are isomorphic to $R/\mathfrak{m}^k \oplus R/\mathfrak{m}^t$. If $d_1 < 2e$, then the statement holds trivially. We assume $d_1 > 2e > t$. Then we have

$$0 \to \mathrm{H}^1_{\mathcal{F}^*_\ell}(\mathbb{Q}, (T^{(k)})^*) \to \mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, (T^{(k)})^*) \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{x'} \oplus R/\mathfrak{m}^a \to 0, \quad x' \geq d_1 - e, a \leq t,$$

$$0 \to \mathrm{H}^1_{\mathcal{F}}(\mathbb{Q}, T^{(k)}) \to \mathrm{H}^1_{\mathcal{F}^\ell}(\mathbb{Q}, T^{(k)}) \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{k-x} \oplus R/\mathfrak{m}^{a'} \to 0, \quad x \geq x', a' \leq t,$$

where the second exact sequence is obtained from the first one by global duality. Recall that $\kappa_\ell \in \mathrm{H}^1_{\mathcal{F}^\ell}(\mathbb{Q}, T^{(k)})$ and that we cannot have $\mathrm{ord}(\mathrm{loc}_\ell(\kappa_\ell)) \leq a'$, since this would contradict the assumption $k > m + s_1 + 2e$. Then by the Kolyvagin system relation (3.5) and the assumptions above, we obtain

$$k - (d_1 - e) \geq k - x \geq \mathrm{ord}(\mathrm{loc}_\ell(\kappa_\ell)) = \mathrm{ord}(\mathrm{loc}_\ell(\kappa_1)) = \mathrm{ord}(\mathrm{loc}_\ell(\varpi^{s_1} c_0)) \geq k - s_1 - e,$$

which proves $\exp(\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, (T^{(k)})^*)) = d_1 \leq s_1 + 2e$. □

3.4.2. *The proof of Theorem 3.4.1.* The proof follows the same lines of the proof of [CGLS22, Thm. 3.2.1] and [CGS23, Thm. 5.1.1]. In particular, exactly as in *op. cit.*, one reduces to proving that, for k big enough, there exists $\mathcal{E}$ depending on E and $\mathrm{rank}_{\mathbb{Z}_p} R$, but not on α or k, such that

$$s_1 + \mathcal{E} \geq \mathrm{length}_R(\mathrm{H}^1_{\mathcal{F}^*}(\mathbb{Q}, (T^{(k)})^*)). \tag{B}$$

In order to prove this, we will inductively choose Kolyvagin primes in $\mathcal{L}^{(k)}$ by repeatedly applying Proposition 3.4.4. We will abbreviate $\mathrm{H}^1_{\mathcal{F}(n)} = \mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T^{(k)})$ and $\mathrm{H}^1_{\mathcal{F}^*(n)} = \mathrm{H}^1_{\mathcal{F}^*(n)}(\mathbb{Q}, (T^{(k)})^*)$ for any $n \in \mathcal{N}^{(k)}$. We let

$$s(n) = \dim_{R/\mathfrak{m}}(\mathrm{H}^1_{\mathcal{F}^*(n)}[\mathfrak{m}])$$

and we write

$$\mathrm{H}^1_{\mathcal{F}^*(n)} = \bigoplus_{i=1}^{s(n)} R/\mathfrak{m}^{d_i(\mathrm{H}^1_{\mathcal{F}^*(n)})}, \quad \text{where } d_1(\mathrm{H}^1_{\mathcal{F}^*(n)}) \geq d_2(\mathrm{H}^1_{\mathcal{F}^*(n)}) \geq \cdots \geq d_{s(n)}(\mathrm{H}^1_{\mathcal{F}^*(n)}).$$

Let

$$s = s(1)$$

and note that this depends only on E in view of Lemma 3.4.2 and the assumption $\alpha \equiv 1 \mod \mathfrak{m}$. For any $x \geq 0$, let

$$\rho_x(n) = \#\{i : d_i(\mathrm{H}^1_{\mathcal{F}^*(n)}) \gneq x\}, \quad \rho := \rho_{3se}(1) = \#\{i : d_i(\mathrm{H}^1_{\mathcal{F}^*}) \gneq 3se\}.$$

We will find sequences of integers $1 = n_0, n_1, ..., n_\rho \in \mathcal{N}^{(k)}$ such that

(a) $s(n_{i-1}) - 2 \leq s(n_i) \leq s(n_{i-1}) + 2$;
(b) $t + d_i(\mathrm{H}^1_{\mathcal{F}^*(n_i)}) \geq d_{i+1}(\mathrm{H}^1_{\mathcal{F}^*(n_{i-1})})$ for $1 \leq i \leq \rho_t(n_{i-1}) - 1$;
(c) $\mathrm{length}_R(\mathrm{H}^1_{\mathcal{F}^*(n_i)}) \leq \mathrm{length}_R(\mathrm{H}^1_{\mathcal{F}^*(n_{i-1})}) - d_1(\mathrm{H}^1_{\mathcal{F}^*(n_{i-1})}) + 3e$;
(d) $\mathrm{ord}(\kappa_{n_i}) \geq \mathrm{ord}(\kappa_{n_{i-1}}) - e$;
(e) $\mathrm{ind}(\kappa_{n_{i-1}}) \geq \mathrm{ind}(\kappa_{n_i}) + d_1(\mathrm{H}^1_{\mathcal{F}^*(n_{i-1})}) - 3e$;
(f) $\rho_x(n_i) \geq \rho_{x+t}(n_{i-1}) - 1$, for any $x \geq 0$.

In particular, applying (e) repeatedly, we find

$$s_1 \geq \mathrm{ind}(\kappa_{n_1}) + d_1(\mathrm{H}^1_{\mathcal{F}^*}) - 3e \geq \cdots \geq \mathrm{ind}(\kappa_{n_\rho}) + \sum_{i=1}^{\rho} d_1(\mathrm{H}^1_{\mathcal{F}^*(n_{i-1})}) - 3\rho e. \tag{3.19}$$

Applying (f) repeatedly, starting with $i = j-1$ and $x = 3se - (j-1)t = 3sd(C_1 + C_2 + t) - (j-1)t$ (which is bigger than t as $j \leq s$), we find, for $1 \leq h \leq j-1$,

$$\rho_x(n_{j-1}) \geq \rho_{x+t}(n_{j-2}) - 1 \geq \cdots \geq \rho_{x+ht}(n_{j-h-1}) - h \geq \cdots \geq \rho_{x+(j-1)t}(1) - (j-1) = \rho(1) - (j-1) \geq 1.$$

In particular, $1 \leq \rho_{x+t}(n_{j-2}) - 1 \leq \rho_t(n_{j-2}) - 1$ and, more generally, for any $1 \leq h \leq j-1$, $h \leq \rho_t(n_{j-h-1}) - 1$. We can therefore apply (b) to deduce

$$\begin{aligned} d_1(\mathrm{H}^1_{\mathcal{F}^*(n_{j-1})}) &\geq d_2(\mathrm{H}^1_{\mathcal{F}^*(n_{j-2})}) - t \geq \cdots \geq d_h(\mathrm{H}^1_{\mathcal{F}^*(n_{j-h})}) - (h-1)t \geq d_{h+1}(\mathrm{H}^1_{\mathcal{F}^*(n_{j-h-1})}) - ht \geq \ldots \\ &\geq d_j(\mathrm{H}^1_{\mathcal{F}^*}) - (j-1)t. \end{aligned}$$

Combining this with (3.19), we find

$$\begin{aligned} s_1 + 3\rho e + (s-\rho)3se + t\tfrac{\rho(\rho-1)}{2} &\geq \mathrm{ind}(\kappa_{n_\rho}) + \sum_{i=1}^{\rho}(d_1(\mathrm{H}^1_{\mathcal{F}^*(n_{i-1})}) + (i-1)t) + \sum_{i=\rho+1}^{s} d_i(\mathrm{H}^1_{\mathcal{F}^*}) \\ &\geq \mathrm{ind}(\kappa_{n_\rho}) + \sum_{i=1}^{\rho} d_i(\mathrm{H}^1_{\mathcal{F}^*}) + \sum_{i=\rho+1}^{s} d_i(\mathrm{H}^1_{\mathcal{F}^*}) \geq \mathrm{length}_R(\mathrm{H}^1_{\mathcal{F}^*}). \end{aligned}$$

Since $3\rho e + (s-\rho)3se + t\frac{\rho(\rho-1)}{2}$ is bounded above by $3(s^2+s)e + ts(s-1)$, which depends only on E and $\mathrm{rank}_{\mathbb{Z}_p} R$, we have proved the desired inequality (B).

We now prove the existence of such integers by induction. Assume we have found integers n_i for $i \leq j$ satisfying (a)-(e) (note that for $n_0 = 1$ these conditions are vacuously satisfied). By Theorem 3.3.3, we can write

$$\mathrm{H}^1_{\mathcal{F}(n_j)} = R/\mathfrak{m}^k \cdot c_0 \oplus \mathrm{H}^1_{\mathcal{F}^*(n_j)}.$$

Similarly as in the proof of Proposition 3.4.6, we apply Proposition 3.4.4 to c_0 and the class c_1 generating the $R/\mathfrak{m}^{d_1(\mathrm{H}^1_{\mathcal{F}^*(n_j)})}$ summand of $\mathrm{H}^1_{\mathcal{F}^*(n_j)}$ to obtain a prime $\ell \in \mathcal{L}^{(k)}$. We obtain the following exact sequences

$$0 \to \mathrm{H}^1_{\mathcal{F}(n_j)_\ell} \to \mathrm{H}^1_{\mathcal{F}(n_j)} \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{k-a} \oplus R/\mathfrak{m}^f \to 0, \quad a \leq e, f \leq t, \tag{3.20}$$

$$0 \to \mathrm{H}^1_{\mathcal{F}^*(n_j)_\ell} \to \mathrm{H}^1_{\mathcal{F}^*(n_j)} \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{x'} \oplus R/\mathfrak{m}^{g'} \to 0, \quad x' \geq d_1(\mathrm{H}^1_{\mathcal{F}^*(n_j)}) - e, g' \leq t. \tag{3.21}$$

By global duality applied to the above exact sequences, we get respectively

$$0 \to \mathrm{H}^1_{\mathcal{F}^*(n_j)_\ell} \to \mathrm{H}^1_{\mathcal{F}^*(n_j\ell)} \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{a'} \oplus R/\mathfrak{m}^{f'} \to 0, \quad a' \leq a, f' \leq t. \tag{3.22}$$

$$0 \to \mathrm{H}^1_{\mathcal{F}(n_j)_\ell} \to \mathrm{H}^1_{\mathcal{F}(n_j\ell)} \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{k-x} \oplus R/\mathfrak{m}^{g} \to 0, \quad x \geq x', g \leq t, \tag{3.23}$$

We claim (a)-(f) are satisfied for $n_{j+1} = n_j\ell$. The proof is similar to the one in [CGLS22, §3.3.3], but it is simplified by the fact that here the image of the localisation is almost cyclic (i.e., it is cyclic after multiplication by ϖ^t, rather than being of rank two over $R/\mathfrak{m}^k$) and, moreover, the "torsion part" of $\mathrm{H}^1_{\mathcal{F}(n_j)}$ is itself a Selmer group (namely $\mathrm{H}^1_{\mathcal{F}^*(n_j)}$) thanks to Theorem 3.3.3, and hence we can control better the behavior of the localisation (compare the exact sequences (3.20),(3.21),(3.22),(3.23) to [CGLS22, (3.16),(3.17)]).

Using [CGLS22, Lem. 3.3.9] applied to (3.21) and (3.22) and the fact that $\mathrm{H}^1_{\mathcal{G}}[\mathfrak{m}] \simeq \mathrm{H}^1_{\mathcal{G}}(\mathbb{Q}, \bar{T})$ for all the Selmer groups involved (thanks to Lemma 3.4.2), we obtain (a). One easily obtains (c) combining again (3.21) and (3.22).

In order to prove (b), we note that applying [CGLS22, Lem. 3.3.9] to the first inclusion in (3.22), we find $d_i(\mathrm{H}^1_{\mathcal{F}^*(n_j)_\ell}) \leq d_i(\mathrm{H}^1_{\mathcal{F}^*(n_j\ell)})$ for $1 \leq i \leq s_i(n_j)$, where we let $d_{s_i(n_j)}(\mathrm{H}^1_{\mathcal{F}^*(n_j)_\ell}) = 0$ if the number of summands of $\mathrm{H}^1_{\mathcal{F}^*(n_j)_\ell}$ is smaller than $s(n_j)$, which happens if and only if $\mathrm{loc}_\ell(\mathrm{H}^1_{\mathcal{F}^*(n_j)}[\mathfrak{m}]) \neq 0$. From (3.21) we obtain the exact sequence

$$0 \to C := (\mathrm{H}^1_{\mathcal{F}^*(n_j)_\ell} \cap p^t\mathrm{H}^1_{\mathcal{F}^*(n_j)}) \to p^t\mathrm{H}^1_{\mathcal{F}^*(n_j)} \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{x'-t} \to 0.$$

We then let $M_0 \simeq p^t \cdot R/\mathfrak{m}^{d_{i_0}(\mathrm{H}^1_{\mathcal{F}^*(n_j)})}$ be the summand of $p^t\mathrm{H}^1_{\mathcal{F}^*(n_j)}$ surjecting into $R/\mathfrak{m}^{x'-t}$. By (3.21) we then have a surjection $C \twoheadrightarrow p^t\mathrm{H}^1_{\mathcal{F}^*(n_j)}/M_0 \simeq \oplus_{i\neq i_0}^{\rho_t(n_j)} R/\mathfrak{m}^{d_i(\mathrm{H}^1_{\mathcal{F}^*(n_j)})-t}$. Dually, we obtain an injection $\oplus_{i\neq i_0}^{\rho_t(n_j)} R/\mathfrak{m}^{d_i(\mathrm{H}^1_{\mathcal{F}^*(n_j)})-t} \hookrightarrow C \hookrightarrow \mathrm{H}^1_{\mathcal{F}^*(n_j)_\ell}$, to which we can apply [CGLS22, Lem. 3.3.9] to obtain $d_i(\mathrm{H}^1_{\mathcal{F}^*(n_j)_\ell}) \geq d_i(\mathrm{H}^1_{\mathcal{F}^*(n_j)})$ if $i \lneq i_0$ and $t + d_i(\mathrm{H}^1_{\mathcal{F}^*(n_j)_\ell}) \geq d_{i+1}(\mathrm{H}^1_{\mathcal{F}^*(n_j)})$ if $i_0 \leq i \leq \rho_t(n_j) - 1$. In particular, we obtain

$$d_i(\mathrm{H}^1_{\mathcal{F}^*(n_j\ell)}) + t \geq d_i(\mathrm{H}^1_{\mathcal{F}^*(n_j)_\ell}) \geq d_{i+1}(\mathrm{H}^1_{\mathcal{F}^*(n_j)}) \quad \text{for every } 1 \leq i \leq \rho_t(n_j) - 1,$$

which yields (b) for $i = j + 1$. This inequality for $i = \rho_{x+t}(n_j) - 1$ also yields (f).

It remains to show (d) and (e). The proof is very similar to the proof of (d) and (e) in [CGLS22, §3.3.3], and we leave the details to the reader.

References

[BCS23] Ashay Burungale, Francesc Castella, and Christopher Skinner. Base change and Iwasawa main conjectures for GL_2. *in preparation*, 2023.

[BDP13] Massimo Bertolini, Henri Darmon, and Kartik Prasanna. Generalized Heegner cycles and p-adic Rankin L-series. *Duke Math. J.*, 162(6):1033–1148, 2013. With an appendix by Brian Conrad.

[Bur20] Ashay A. Burungale. On the non-triviality of the p-adic Abel-Jacobi image of generalised Heegner cycles modulo p, I: Modular curves. *J. Algebraic Geom.*, 29(2):329–371, 2020.

[Buy09] Kâzim Buyükboduk. Tamagawa defect of Euler systems. *J. Number Theory*, 129(2):402–417, 2009.

[CGLS22] Francesc Castella, Giada Grossi, Jaehoon Lee, and Christopher Skinner. On the anticyclotomic Iwasawa theory of rational elliptic curves at Eisenstein primes. *Invent. Math.*, 227:517–580, 2022.

[CGS23] Francesc Castella, Giada Grossi, and Christopher Skinner. Mazur's main conjecture at Eisenstein primes. *preprint*, 2023.

[CH18] Francesc Castella and Ming-Lun Hsieh. Heegner cycles and p-adic L-functions. *Math. Ann.*, 370(1-2):567–628, 2018.

[Cor02] Christophe Cornut. Mazur's conjecture on higher Heegner points. *Invent. Math.*, 148(3):495–523, 2002.

[Gre94] Ralph Greenberg. Iwasawa theory and p-adic deformations of motives. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 193–223. Amer. Math. Soc., Providence, RI, 1994.

[Gre99] Ralph Greenberg. Iwasawa theory for elliptic curves. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 51–144. Springer, Berlin, 1999.

[GV00] Ralph Greenberg and Vinayak Vatsal. On the Iwasawa invariants of elliptic curves. *Invent. Math.*, 142(1):17–63, 2000.

[GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[How04a] Benjamin Howard. The Heegner point Kolyvagin system. *Compos. Math.*, 140(6):1439–1472, 2004.

[How04b] Benjamin Howard. Iwasawa theory of Heegner points on abelian varieties of GL_2 type. *Duke Mathematical Journal*, 124(1):1–45, 2004.

[Jet08] Dimitar Jetchev. Global divisibility of Heegner points and Tamagawa numbers. *Compos. Math.*, 144(4):811–826, 2008.

[JSW17] Dimitar Jetchev, Christopher Skinner, and Xin Wan. The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one. *Camb. J. Math.*, 5(3):369–434, 2017.

[Kat04] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.

[Kim22a] Chan-Ho Kim. A higher Gross-Zagier formula and the structure of Selmer groups, 2022.

[Kim22b] Chan-Ho Kim. The structure of Selmer groups and the Iwasawa main conjecture for elliptic curves, 2022.

[Kol91] Victor A. Kolyvagin. On the structure of Selmer groups. *Math. Ann.*, 291(2):253–259, 1991.

[Maz72] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.

[McC91] William G. McCallum. Kolyvagin's work on Shafarevich-Tate groups. In *L-functions and arithmetic (Durham, 1989)*, volume 153 of *London Math. Soc. Lecture Note Ser.*, pages 295–316. Cambridge Univ. Press, Cambridge, 1991.

[MR04] Barry Mazur and Karl Rubin. Kolyvagin systems. *Mem. Amer. Math. Soc.*, 168(799):viii+96, 2004.

[MSD74] Barry Mazur and Peter Swinnerton-Dyer. Arithmetic of Weil curves. *Invent. Math.*, 25:1–61, 1974.

[Nek07] Jan Nekovář. The Euler system method for CM points on Shimura curves. In *L-functions and Galois representations*, volume 320 of *London Math. Soc. Lecture Note Ser.*, pages 471–547. Cambridge Univ. Press, Cambridge, 2007.

[PR89] B. Perrin-Riou. Variation de la fonction L p-adique par isogénie. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 347–358. Academic Press, Boston, MA, 1989.

[Roh84] David E. Rohrlich. On L-functions of elliptic curves and anticyclotomic towers. *Invent. Math.*, 75(3):383–408, 1984.

[Rub91] Karl Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.

[Rub98] Karl Rubin. Euler systems and modular elliptic curves. In *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, volume 254 of *London Math. Soc. Lecture Note Ser.*, pages 351–367. Cambridge Univ. Press, Cambridge, 1998.

[Rub00] Karl Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.

[Rub11] Karl Rubin. Euler systems and Kolyvagin systems. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 449–499. Amer. Math. Soc., Providence, RI, 2011.

[Sch87] Peter Schneider. The μ-invariant of isogenies. *J. Indian Math. Soc. (N.S.)*, 52:159–170 (1988), 1987.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972.

[SU14] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[Swe20] Naomi Sweeting. Kolyvagin's Conjecture and patched Euler systems in anticyclotomic Iwasawa theory, 2020.

[Vat03] Vinayak Vatsal. Special values of anticyclotomic L-functions. *Duke Math. J.*, 116(2):219–261, 2003.

[Wan15] Xin Wan. The Iwasawa main conjecture for Hilbert modular forms. *Forum Math. Sigma*, 3:Paper No. e18, 95, 2015.

[Wan21] Xin Wan. Heegner Point Kolyvagin System and Iwasawa Main Conjecture. *Acta Math. Sin. (Engl. Ser.)*, 37(1):104–120, 2021.

[Wut14] Christian Wuthrich. On the integrality of modular symbols and Kato's Euler system for elliptic curves. *Doc. Math.*, 19:381–402, 2014.

[Zan19] Murilo Zanarella. On Howard's main conjecture and the Heegner point Kolyvagin system, 2019.

[Zha14a] Wei Zhang. The Birch–Swinnerton-Dyer conjecture and Heegner points: a survey. In *Current developments in mathematics 2013*, pages 169–203. Int. Press, Somerville, MA, 2014.

[Zha14b] Wei Zhang. Selmer groups and the indivisibility of Heegner points. *Camb. J. Math.*, 2(2):191–253, 2014.

(A. Burungale) University of Texas at Austin, USA
Email address: `ashayk@utexas.edu`

(F. Castella) University of California Santa Barbara, South Hall, Santa Barbara, CA 93106, USA
Email address: `castella@ucsb.edu`

(G. Grossi) CNRS, Institut Galilée, Université Sorbonne Paris Nord, 93430 Villetaneuse, FRANCE
Email address: `grossi@math.univ-paris13.fr`

(C. Skinner) Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544-1000, USA
Email address: `cmcls@princeton.edu`