ON REFINED NONVANISHING CONJECTURES BY KURIHARA AND KOLYVAGIN

FRANCESC CASTELLA AND TAKAMICHI SANO

Abstract. In this paper, we extend the results of [BCGS26] on refined conjectures by Kurihara and Kolyvagin, allowing primes of any reduction type in the case of Kurihara's conjectures, and inert primes in the underlying imaginary quadratic field in the case of Kolyvagin's. The key innovation is a new approach to the computation of the p-divisibility index of certain special elements in Galois cohomology (the bottom class of a Λ-adic Euler system twisted by a character sufficiently close to the trivial character) based on a reformulation of the Iwasawa Main Conjectures in terms of determinants of Selmer complexes.

Contents

1. Introduction

In [BCGS26], the first author with Burungale, Grossi and Skinner gave a proof of nonvanishing conjectures by Kolyvagin [Kol91b] and Kurihara [Kur14b], and their 'quantitative' refinements [Zha14a, Kim26], for elliptic curves $E/\mathbb{Q}$ at certain primes p. Building on a new approach to the descent computations in [BCGS26], in this paper we obtain an extension of the results in *op. cit.* allowing E to have any reduction type at p in the case of the refined Kurihara conjectures, and p to be any prime unramified in the underlying quadratic imaginary field K in the case of the refined Kolyvagin conjectures.

1.1. Main results.

1.1.1. *Kurihara's analytic quantities.* Let $E/\mathbb{Q}$ be an elliptic curve of conductor N without complex multiplication, and fix an odd prime p such that

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

Denote by $\mathcal{L}$ the set of primes

$$\mathcal{L} := \{\ell : \ \ell \equiv 1 \ (\mathrm{mod}\, p),\ \ell \nmid N, \text{ and } a_\ell \equiv \ell + 1 \ (\mathrm{mod}\, p)\},$$

Date: January 20, 2026.

where $a_\ell := \ell + 1 - \#\widetilde{E}(\mathbb{F}_\ell)$, and let $\mathcal{N}$ be the collection of all squarefree products of primes $\ell \in \mathcal{L}$, with the convention that $1 \in \mathcal{N}$ (corresponding to the empty product). For each $\ell \in \mathcal{L}$, let $I_\ell \subset \mathbb{Z}$ be defined by

$$I_\ell := (\ell - 1, a_\ell - \ell - 1)\mathbb{Z}_p \cap \mathbb{Z},$$

and for each $n \in \mathcal{N}$ put $I_n = \sum_{\ell | n} I_\ell$ if $n \neq 1$ and $I_n = 0$ otherwise.

Let $f \in S_2(\Gamma_0(N))$ be the newform attached to E. Let $\Omega_E^+ = \int_{E(\mathbb{R})} \omega_E \in \mathbb{R}$ be the positive Néron period of E, where ω_E is a Néron differential. Fix a modular parametrization

$$\phi : X_0(N) \to E$$

and let $c_\phi \in \mathbb{Z}$ be the associated *Manin constant*, so that $\phi^*(\omega_E) = c_\phi \cdot 2\pi i f(z) dz$. Assume that

$$p \nmid c_\phi. \tag{$p \nmid c_\phi$}$$

(For instance, if E is the strong Weil curve in the $\mathbb{Q}$-isogeny class attached to f and ϕ is the optimal quotient, then ($p \nmid c_\phi$) holds provided $p^2 \nmid N$ by [Maz78, Cor. 4.1].)

Using modular symbols, Kurihara introduced in [Kur14a] certain quantities

$$\delta_n \in \mathbb{Z}/I_n$$

shown to completely determine the structure of the p-primary Selmer group $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ under some hypotheses (see [Kur14a, Thm. B]). Specifically,

$$\delta_n := \sum_{\substack{a=1 \\ (a,n)=1}}^{n} \overline{\left[\frac{a}{n}\right]} \left(\prod_{\ell | n} \log_{\mathbb{F}_\ell}(a) \right) \in \mathbb{Z}/I_n,$$

where $\left[\frac{a}{n}\right] \in \mathbb{Q}$ is the modular symbol

$$\left[\frac{a}{n}\right] = \mathrm{Re}\left(2\pi i \int_\infty^{a/n} f(z) dz \right) / \Omega_E^+ \in \mathbb{Q},$$

which is known to be p-integral by our assumptions on p (see [Ste89, §3]), and $\overline{\left[\frac{a}{n}\right]} \in \mathbb{Z}/I_n$ denotes its reduction modulo I_n; and

$$\log_{\mathbb{F}_\ell} : \mathbb{F}_\ell^\times \cong \mathbb{Z}/(\ell - 1)\mathbb{Z} \to \mathbb{Z}/I_\ell$$

is the discrete logarithm defined by a fixed choice of primitive root $\eta_\ell \in \mathbb{F}_\ell^\times$ (so $\mathbb{F}_\ell^\times = \eta_\ell^{\mathbb{Z}}$), with the last arrow given by reduction modulo I_ℓ. In particular, for $n = 1$, δ_n reduces to the normalized L-value

$$\delta_1 = L(E, 1)/\Omega_E^+ \in \mathbb{Q}. \tag{1.1}$$

1.1.2. *Kurihara's conjectures.* Put

$$\mathrm{Tam}_E := \prod_{\ell | N} c_\ell,$$

where $c_\ell = [E(\mathbb{Q}_\ell) : E_0(\mathbb{Q}_\ell)]$ is the Tamagawa factor of E at ℓ. Let $\bar{\delta}_n \in \mathbb{F}_p$ denote the reduction of δ_n modulo p. The following conjecture was first formulated by Kurihara in [Kur14b, §1.2, Conj. 1] in the p-ordinary case, and in [Kur24, §1.2, Conj. 1.1] for supersingular p. As in [Kim26], it naturally extends to primes $p > 2$ of bad reduction as long as hypotheses (sur) and ($p \nmid c_\phi$) both hold, and below we state it in this level of generality.

Conjecture A. *Let p be an odd prime such that* (sur) *and* ($p \nmid c_\phi$) *both hold. If $p \nmid \mathrm{Tam}_E$, then there exists $n \in \mathcal{N}$ such that $\bar{\delta}_n \neq 0$.*

1.1.3. *Refined Kurihara's conjecture.* In this paper we study a strenghtening of Conjecture A motivated by the aforementioned structure theorem by Kurihara [Kur14a]. The same structure theorem was recently proved from a different perspective by C.-H. Kim [Kim26], whose notations we largely follow.

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

$$\mathscr{M}(n) := \max\{\mathscr{M} \geq 0 : \ \delta_n \in p^{\mathscr{M}} \mathbb{Z}/I_n\}$$

otherwise. Put $\mathscr{M}_r := \min\{\mathscr{M}(n) : \ n \in \mathcal{N},\ \nu(n) = r\}$, where $\nu(n)$ denotes the number of prime factors of n. As shown in [Kur14a, §10.5], the quantity δ_n can be obtained as a coefficient of the Mazur–Tate θ-element of conductor n [MT87], and it follows from the functional equation of the latter that $\delta_n = 0$ unless $(-1)^{\nu(n)} = \epsilon$, where $\nu(n)$ where $\epsilon \in \{\pm 1\}$ is the root number of E.

Putting $\mathscr{M}_r := \min\{\mathscr{M}(n) : \nu(n) = r\}$, then one can show that $\mathscr{M}_r \geq \mathscr{M}_{r+2} \geq 0$ for all $r \geq 0$, and we put

$$\mathscr{M}_\infty(\boldsymbol{\delta}) := \lim_{\substack{r\to\infty \\ (-1)^r=\epsilon}} \mathscr{M}_r,$$

where $\boldsymbol{\delta}$ denotes the collection $\{\delta_n\}_{n\in\mathcal{N}}$. Thus $\mathscr{M}_\infty(\boldsymbol{\delta}) < \infty$ if and only if $\boldsymbol{\delta} \neq \{0\}$. Suppose this is the case, and let ϱ be the 'order of vanishing' of $\boldsymbol{\delta}$:

$$\varrho := \min\{r \geq 0 : \ \delta_n \neq 0 \ \text{ and } \ \nu(n) = r\}.$$

Then [Kim26, Thm. 1.8], as originally proved by Kurihara [Kur14a, Thm. B] under some hypotheses and from a different perspective, yields the following exact formula for $Ш_{\mathrm{BK}}(E[p^\infty]/\mathbb{Q}) := \mathrm{Sel}_{p^\infty}(E/\mathbb{Q})/\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})_{\mathrm{div}}$, where the subscript 'div' denotes the maximal divisible submodule:

$$\mathrm{ord}_p\big(\#Ш_{\mathrm{BK}}(E[p^\infty]/\mathbb{Q})\big) = \mathscr{M}_\varrho - \mathscr{M}_\infty(\boldsymbol{\delta}).$$

In particular, if $L(E,1) \neq 0$, then $\varrho = 0$ and Kato's work [Kat04] implies that $Ш_{\mathrm{BK}}(E[p^\infty]/\mathbb{Q})$ is the same as the p-primary part $Ш(E/\mathbb{Q})[p^\infty]$ of the Tate–Shafarevich group of E, so combined with (1.1) the above exact formula reduces to

$$\mathrm{ord}_p\big(\#Ш(E/\mathbb{Q})[p^\infty]\big) = \mathrm{ord}_p\left(\frac{L(E,1)}{\Omega_E^+}\right) - \mathscr{M}_\infty(\boldsymbol{\delta}).$$

Together with the Birch–Swinnerton-Dyer formula, this motivates the following conjecture (in arbitrary rank) formulated in [Kim26, Conj. 1.9].

Conjecture B (Refined Kurihara's conjecture)**.** *Let $p > 3$ be a prime such that* (sur) *and* ($p \nmid c_\phi$) *both hold. Then*

$$\mathscr{M}_\infty(\boldsymbol{\delta}) = \mathrm{ord}_p(\mathrm{Tam}_E).$$

1.1.4. *Results.* Our main result towards the refined Kurihara's conjecture is the following. Let $\mathbb{Q}_\infty/\mathbb{Q}$ denote the cyclotomic $\mathbb{Z}_p$-extension.

Theorem A. *Let $p > 3$ be a prime such that* (sur) *and* ($p \nmid c_\phi$) *both hold. Then the following are equivalent:*

(i) $\mathscr{M}_\infty(\boldsymbol{\delta}) = \mathrm{ord}_p(\mathrm{Tam}_E)$*, and hence Conjecture B holds.*
(ii) *The Iwasawa Main Conjecture 2.2.2 for $\mathbb{Q}_\infty/\mathbb{Q}$ holds.*

In particular, in the case where $p \nmid \mathrm{Tam}_E$ we deduce:

Corollary A. *Let $p > 3$ be a prime such that* (sur) *and* ($p \nmid c_\phi$) *both hold. If $p \nmid \mathrm{Tam}_E$, then the following are equivalent:*

(i) *There exists $n \in \mathcal{N}$ such that $\bar{\delta}_n \neq 0$, and hence Conjecture A holds.*
(ii) *The Iwasawa Main Conjecture 2.2.2 for $\mathbb{Q}_\infty/\mathbb{Q}$ holds.*

Proof. This is clear from Theorem A, noting that $\mathscr{M}_\infty(\boldsymbol{\delta}) = 0$ if and only if there exists $n \in \mathcal{N}$ such that δ_n is p-indivisible. □

The Iwasawa Main Conjecture 2.2.2 for $\mathbb{Q}_\infty/\mathbb{Q}$ in the above results is a reformulation of [Kat04, Conj. 12.10] in terms of determinants of arithmetic complexes. Thus combined with known results on the latter, we obtain a proof of Kurihara's conjecture and its refinement in many cases.

Theorem B (Refined Kurihara's conjecture)**.** *Let $p > 3$ be a prime such that* (sur) *and* ($p \nmid c_\phi$) *both hold. Then Conjecture B (and hence also Conjecture A) holds in each of the following cases:*

- *p is good ordinary for E.*
- *p is good supersingular for E and N is squarefree.*

Proof. In the ordinary (resp. supersingular) case, the Iwasawa Main Conjecture for $\mathbb{Q}_\infty/\mathbb{Q}$ in the formulation of Mazur–Swinnerton-Dyer [Maz72, MSD74] (resp. Kobayashi [Kob03]) is proved in [Wan15, BCS25] (resp. [CLW22, BSTW24]). Each of these main conjectures is known to be equivalent to [Kat04, Conj. 12.10] and hence to the Iwasawa Main Conjecture 2.2.2 for $\mathbb{Q}_\infty/\mathbb{Q}$, so the result follows from Theorem A. □

1.1.5. *Kolyvagin conjectures.* In the second part of this paper, we prove an analogue of Theorem A for W. Zhang's refinement in [Zha14a] of Kolyvagin's conjecture.

For the statements, let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and let K satisfying the *Heegner hypothesis*:

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

and with discriminant $-D_K < 0$ such that

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

Let p be an odd prime such that (sur) and ($p \nmid c_\phi$) holds. By [Gro91, Lem. 4.3], it follows that $E(K[n])[p] = 0$ for all $n \geq 1$, where $K[n]$ denotes the ring class field of K of conductor n.

Denote by $\mathcal{L}_{\mathrm{Heeg}}$ the set of primes

$$\mathcal{L}_{\mathrm{Heeg}} := \{\ell : \ \ell \text{ is inert in } K, \ \ell \nmid N, \ \text{ and } \ a_\ell \equiv \ell + 1 \equiv 0 \ (\mathrm{mod}\, p)\},$$

and let $\mathcal{N}_{\mathrm{Heeg}}$ be the collection of all squarefree products of primes $\ell \in \mathcal{L}_{\mathrm{Heeg}}$, with $1 \in \mathcal{N}_{\mathrm{Heeg}}$ by convention. For each prime $\ell \in \mathcal{L}_{\mathrm{Heeg}}$, let $I_\ell \subset \mathbb{Z}$ be defined by

$$I_\ell := (\ell + 1, a_\ell)\mathbb{Z}_p \cap \mathbb{Z},$$

and for each $n \in \mathcal{N}_{\mathrm{Heeg}}$ put $I_n = \sum_{\ell \mid n} I_\ell$ if $n > 1$ and $I_n = 0$ otherwise.

Let $T = T_p E$ denote the p-adic Tate module of E. For each $n \in \mathcal{N}_{\mathrm{Heeg}}$, from the Kummer images of Heegner points on E of conductor n associated to a fixed modular parametrization $\phi : X_0(N) \to E$, the Kolyvagin derivative process yields a construction of classes

$$\kappa_n^{\mathrm{Heeg}} \in \mathrm{H}^1(K, T/I_n T)$$

forming a *Kolyvagin system* $\boldsymbol{\kappa}^{\mathrm{Heeg}} = \{\kappa_n^{\mathrm{Heeg}}\}_n \in \mathbf{KS}(T, \mathcal{F}, \mathcal{L}_{\mathrm{Heeg}})$ in the sense of [How04] for the Selmer structure $\mathcal{F}$ of Theorem 1.6.5 in *op. cit.* (see also [How04, §1.7]). In particular, $\kappa_1 \in \mathrm{H}^1_{\mathcal{F}}(K, T) = \varprojlim_m \mathrm{Sel}_{p^m}(E/K)$ is the Kummer image of the Heegner point $y_K \in E(K)$ in the Gross–Zagier formula [GZ86].

The classes κ_n^{Heeg} land in the *n-transverse Selmer group* $\mathrm{H}^1_{\mathcal{F}(n)}(K, T/I_n T) \subset \mathrm{H}^1(K, T/I_n T)$ (see [How04, Lem. 1.7.3] and §1.1.5 below for a review), and setting $\mathscr{M}(n)$ to be ∞ if $\kappa_n^{\mathrm{Heeg}} = 0$ and the maximum $\mathscr{M} \geq 0$ such that $\kappa_n^{\mathrm{Heeg}} \in p^{\mathscr{M}} \mathrm{H}^1_{\mathcal{F}(n)}(K, T/I_n T)$ otherwise, one defines $\mathscr{M}_r := \min\{\mathscr{M}(n) : \ \nu(n) = r\}$. In this case, Kolyvagin showed $\mathscr{M}_r \geq \mathscr{M}_{r+1}$ for all $r \geq 0$, and we put

$$\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Heeg}}) := \lim_{r \to \infty} \mathscr{M}_r \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$$

similarly as in §1.1.2.

In [Kol91b], Kolyvagin conjectured that $\boldsymbol{\kappa}^{\mathrm{Heeg}} \neq \{0\}$ (equivalently, $\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Heeg}}) < \infty$). The refined version of this conjecture by W. Zhang [Zha14a] further predicts an exact formula for $\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Heeg}})$ in terms of arithmetic invariants of E. As explained in [*op. cit.*, §4.4] (see also [Jet08, §1]), this is motivated by combining in the case that $\mathrm{ord}_{s=1} L(E/K, s) = 1$:

- The Gross–Zagier formula for $y_K \in E(K)$, whereby the Birch–Swinnerton-Dyer formula for $L'(E/K, 1)$ yields the prediction

$$2 \cdot \mathrm{ord}_p\big([E(K) : \mathbb{Z} y_K]\big) \stackrel{?}{=} \mathrm{ord}_p\big(\#Ш(E/K)[p^\infty]\big) + 2 \cdot \mathrm{ord}_p\big(\mathrm{Tam}_E\big).$$

- Kolyvagin's structure theorem [Kol91b], which in the case $\mathrm{ord}_{s=1} L(E/K, s) = 1$ implies

$$\mathrm{ord}_p\big(\#Ш(E/K)[p^\infty]\big) = 2 \cdot \big(\mathrm{ord}_p([E(K) : \mathbb{Z} y_K]) - \mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Heeg}})\big).$$

The following is [Zha14a, Conj. 4.5], which allows $\mathrm{ord}_{s=1} L(E/K, s) > 1$.

Conjecture C (Refined Kolyvagin's conjecture)**.** *Let p be an odd prime such that* (sur) *and* ($p \nmid c_\phi$) *both hold. Then*

$$\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Heeg}}) = \mathrm{ord}_p(\mathrm{Tam}_E).$$

1.1.6. *Results.* Our main result toward the refined Kolyvagin conjecture is the following.

Theorem C (Refined Kolyvagin's conjecture)**.** *Let $p > 3$ be a prime such that* (sur) *and* ($p \nmid c_\phi$) *both hold. If E has good ordinary reduction at p and is unramified in K, then the following are equivalent:*

(i) $\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Heeg}}) = \mathrm{ord}_p(\mathrm{Tam}_E)$.
(ii) *The anticyclotomic Iwasawa Main Conjecture 3.2.2 holds.*

In particular, if p splits in K, then Conjecture C holds.

1.2. **Outline of the proofs.** The proofs of Theorem A and Theorem C go along the same lines as the proofs of related results [BCGS26]; our novelty here is in the approach to the descent computations in *op. cit.*.

We shall first explain the proof of Theorem A. Letting $\Lambda = \mathbb{Z}_p[[\Gamma]]$ be the cyclotomic Iwasawa algebra over $\mathbb{Q}$, the proof of Theorem A relies on a study of the Λ-adic Kolyvagin system

$$\boldsymbol{\kappa}_{\Lambda}^{\mathrm{Kato}} = \{\kappa_{n,\Lambda}^{\mathrm{Kato}} \in \mathrm{H}^1(\mathbb{Q}, \mathbf{T}/I_n\mathbf{T}) \,:\, n \in \mathcal{N}\}$$

derived from Kato's Euler system, where $\mathbf{T} = T \otimes_{\mathbb{Z}_p} \Lambda$ is the cyclotomic deformation of T. By Kato's explicit reciprocity law [Kat04] and Rohrlich's nonvanishing results [Roh84], $\kappa_{1,\Lambda}^{\mathrm{Kato}} \in \mathrm{H}^1(\mathbb{Q}, \mathbf{T})$ is not Λ-torsion, and so letting $\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha) \in \mathrm{H}^1(\mathbb{Q}, T(\alpha))$ denote the specialization of $\kappa_{1,\Lambda}^{\mathrm{Kato}}$ at a non-trivial character $\alpha : \Gamma \to \mathbb{Z}_p^\times$ with $\alpha \equiv 1 \pmod{p^m}$, it follows that $\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha)$ is nonzero for $m \gg 0$. Towards the proof of (ii) $\Rightarrow$ (i) in Theorem A, we make use of:

(A) An exact formula, for $m \gg 0$, for the divisibility index

$$\mathrm{ind}_p\big(\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha)\big) := \max\{\mathscr{M} \geq 0 \,:\, \kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha) \in p^{\mathscr{M}}\mathrm{H}^1(\mathbb{Q}, T(\alpha))\}$$

deduced from the Iwasawa Main Conjecture 2.2.2. The Tamagawa factors for the Cartier dual $T(\alpha)^* = \mathrm{Hom}(T(\alpha), \mu_{p^\infty})$ appear here. (See Corollary 2.3.2.)

(B) An exact formula for the $\mathbb{Z}_p$-length of the *strict Selmer group* $\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T(\alpha)^*)$ (which for $m \gg 0$ such that $\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha) \neq 0$ can be shown to be finite) in terms of the difference

$$\mathrm{ind}_p\big(\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha)\big) - \mathscr{M}_\infty(\boldsymbol{\kappa}_{\Lambda}^{\mathrm{Kato}}(\alpha))$$

deduced from Mazur–Rubin's structure theorem in [MR04]. (See Theorem 2.1.4.)

For m with $p^m \in I_n$, the classes $\kappa_{n,\Lambda}^{\mathrm{Kato}}(\alpha)$ can be compared to the classes $\kappa_n^{\mathrm{Kato}} \in \mathrm{H}^1(\mathbb{Q}, T/I_nT)$ arising directly from Kato's Euler system (i.e., without going up the cyclotomic tower), and building on (A) and (B) we show that the Iwasawa Main Conjecture 2.2.2 implies, for $m \gg 0$, the equalities

$$\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Kato}}) = \mathscr{M}_\infty(\boldsymbol{\kappa}_{\Lambda}^{\mathrm{Kato}}(\alpha)) = \mathrm{ord}_p(\mathrm{Tam}_E) + t,$$

where $t = \mathrm{ord}_p(\#E(\mathbb{Q}_p)[p^\infty])$. Together with the 'derived' version of Kato's explicit reciprocity law obtained in [Kim26] extending Kato's relation between κ_n^{Kato} and δ_n for $n = 1$ via the dual exponential map to $n > 1$ (see Theorem 2.1.3), we thus arrive at the implication (ii) $\Rightarrow$ (i) in Theorem A. The proof of the converse is similar: The computations that go into the proof of (A) show that the formula for $\mathrm{ind}_p(\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha))$ obtained in Corollary 2.3.2 for $m \gg 0$ is equivalent to the Iwasawa Main Conjecture 2.2.2 specialized at α, which together with the divisibility coming from an Euler system argument applied to the non-trivial $\boldsymbol{\kappa}_{\Lambda}^{\mathrm{Kato}}(\alpha)$ yields a proof of the main conjecture.

The proof of the equivalence in Theorem C is similar: (A) and (B) then correspond to Corollary 3.3.4 and Theorem 3.1.2, respectively.

Most of the work in the paper goes into the proof of (A) and its analogue for Heegner classes. For this, the new idea in this paper is to build on a reformulation of the Iwasawa Main Conjecture in terms of determinants of Selmer complexes introduced in [KS24], dispensing with the use of p-adic L-functions and control theorems in the style of [Gre99] in the approach of [BCGS26]. The key descent computations are Proposition 2.3.1 and Proposition 3.3.2.

1.3. **Comparison to previous works.**

1.3.1. *On the refined Kurihara's conjecture.* For ordinary primes p, and subject to the 'non-anomalous' condition

$$E(\mathbb{Q}_p)[p] = 0, \tag{nonanom}$$

Corollary A was first proved by Kurihara assuming the non-degeneracy of the cyclotomic p-adic height pairing (see [Kur14a, Thm. 10.8]), and more recently by Sakamoto and C.-H. Kim independently (see [Sak22, Thm. 1.2] and [Kim26, Thm. 1.10]). Also in the non-anomalous p-ordinary case, Theorem A (and hence also Corollary A) was essentially proved in [BCGS26] (see [BCGS26, Rem. 3.3.5]).

On the other hand, for non-ordinary (and possibly bad reduction) primes p, Theorem A was independently proved by C.-H. Kim assuming $p \nmid \mathrm{Tam}_E$ (see [Kim26, Thm. 1.10]), but the case $\mathrm{ord}_p(\mathrm{Tam}_E) > 0$ of Theorem A was wide open[1].

[1]See also forthcoming work by Kurihara–Sakamoto [KS26] for an independent approach to related results.

1.3.2. *On the refined Kolyvagin's conjecture.* Under certain ramification hypotheses that imply $p \nmid \mathrm{ord}_p(\mathrm{Tam}_E)$, Conjecture C was first proved by W. Zhang [Zha14b].

Restricting to the case p split in K, Theorem C was first proved in [BCGS26] through a study of the p-adic L-function of Bertolini–Darmon–Prasanna [BDP13], its relation with y_∞ via an explicit reciprocity law [CH18], and its associated Iwasawa–Greenberg Main Conjecture (see Theorem B and Remark 2.2.5 in [BCGS26]). Our approach does not require the use of p-adic L-functions, and applies also in the p inert case.

1.4. **Acknowledgements.** We heartily thank Masato Kurihara for several enlightening conversations related to the topics of this paper, and his comments and corrections on an earlier draft. We also thank Chan-Ho Kim for helpful comments. At different stages during the preparation of this paper, the first author was supported by the NSF grant DMS-2401321, the 2014-2015 AMS Centennial Research Fellowship, and a JSPS short-term Invitational Fellowship for Research in Japan. The second author was supported by JSPS KAKENHI Grant Number 22K13896.

2. Kurihara conjectures

2.1. **Preliminaries.** As in Introduction, let $E/\mathbb{Q}$ be an elliptic curve of conductor N without CM, and fix an odd prime p such that (sur) and ($p \nmid c_\phi$) both hold.

2.1.1. *Kato's Kolyvagin systems.* As in [Kim26, §2.3], we consider Kato's Euler system

$$\big\{z_{np^k} \in \mathrm{H}^1(\mathbb{Q}(\mu_{np^k}), T) \,:\, (n, Np) = 1,\ k \geq 0\big\} \tag{2.1}$$

following the normalization in [Kat21, Thm. 6.1]. In particular, by Kato's explicit reciprocity law [Kat04] the natural image of $\mathrm{res}_p(z_1)$ under the dual exponential map $\exp^*_{\omega_E} : \mathrm{H}^1(\mathbb{Q}_p, T) \to \mathbb{Q}_p$ is given by

$$\exp^*_{\omega_E}(\mathrm{res}_p(z_1)) = \frac{L^{\{p\}}(E, 1)}{\Omega^+_E}, \tag{2.2}$$

where $L^{\{p\}}(E, s)$ is the L-function of E with the Euler factor at p removed.

By [MR04, Thm. 3.2.4 and §6.2], (see also [*op. cit.*, §6.2]), by the Kolyvagin derivative process, from (2.1) we obtain a *Kolyvagin system*

$$\boldsymbol{\kappa}^{\mathrm{Kato}} = \big\{\kappa^{\mathrm{Kato}}_n \in \mathrm{H}^1_{\mathcal{F}_{\mathrm{rel}}(n)}(\mathbb{Q}, T/I_nT) \,:\, n \in \mathcal{N}\big\}$$

in the sense of [MR04, §3.1] for the triple $(T, \mathcal{F}_{\mathrm{rel}}, \mathcal{L})$, where $\mathcal{F}_{\mathrm{rel}}$ is the 'canonical' Selmer structure of [*op. cit.*, Def. 3.2.1], and $\mathcal{F}_{\mathrm{rel}}(n)$ denotes the modification of $\mathcal{F}_{\mathrm{rel}}$ given by

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{rel}}(n)}(\mathbb{Q}_\ell, T/I_nT) = \begin{cases} \mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T/I_nT) := \mathrm{H}^1(\mathbb{Q}_\ell(\mu_\ell)/\mathbb{Q}_\ell, \mathrm{H}^0(\mathbb{Q}_\ell(\mu_\ell), T/I_nT)) & \text{if } \ell \mid n, \\ \mathrm{H}^1_{\mathcal{F}_{\mathrm{rel}}}(\mathbb{Q}_\ell, T/I_nT) & \text{if } \ell \nmid n. \end{cases} \tag{2.3}$$

In particular, the construction gives

$$\kappa^{\mathrm{Kato}}_1 = z_1 \in \mathrm{H}^1_{\mathcal{F}_{\mathrm{rel}}}(\mathbb{Q}, T),$$

where

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{rel}}}(\mathbb{Q}, T) := \ker\left\{\mathrm{H}^1(\mathbb{Q}, T) \to \bigoplus_{\ell \neq p} \frac{\mathrm{H}^1(\mathbb{Q}_\ell, T)}{\mathrm{H}^1_f(\mathbb{Q}_\ell, T)}\right\}$$

with $\mathrm{H}^1_f(\mathbb{Q}_\ell, T) := \ker\{\mathrm{H}^1(\mathbb{Q}_\ell, T) \to \mathrm{H}^1(\mathbb{Q}^{\mathrm{ur}}_\ell, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)\}$.

Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, with k-th layer $\mathbb{Q}_k$, and put $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ and $\Lambda = \mathbb{Z}_p[[\Gamma]]$. For varying $k \geq 0$, the classes z_{np^k} are compatible under the corestriction maps, and hence for every $n \geq 1$ we can let $z_{n,\Lambda} \in \mathrm{H}^1(\mathbb{Q}(\mu_n), \mathbf{T})$ be the class defined by the image of $\varprojlim_k z_{np^k}$ under the composite map

$$\varprojlim_k \mathrm{H}^1(\mathbb{Q}(\mu_{np^k}), T) \to \varprojlim_k \mathrm{H}^1(\mathbb{Q}(\mu_n)\mathbb{Q}_k, T) \cong \mathrm{H}^1(\mathbb{Q}(\mu_n), \mathbf{T}),$$

where $\mathbf{T} = T \otimes_{\mathbb{Z}_p} \Lambda$, with the $G_{\mathbb{Q}}$-action on Λ is given by the inverse of the character $G_{\mathbb{Q}} \twoheadrightarrow \Gamma \hookrightarrow \Lambda^\times$, and the last isomorphism is given by Shapiro's lemma. By [MR04, Thm. 5.3.3] (see also [*op. cit.*, §6.2]), the Kolyvagin derivative process applied to $\{z_{n,\Lambda}\}_n$ leads to the construction of a Λ-*adic Kolyvagin system*

$$\boldsymbol{\kappa}^{\mathrm{Kato}}_\Lambda = \big\{\kappa^{\mathrm{Kato}}_{n,\Lambda} \in \mathrm{H}^1_{\mathcal{F}_\Lambda(n)}(\mathbb{Q}, \mathbf{T}/I_n\mathbf{T}) \,:\, n \in \mathcal{N}\big\} \tag{2.4}$$

in the sense of [MR04, §3.1] for the triple $(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{L}_E)$, where $\mathcal{F}_\Lambda$ is the Selmer structure of [MR04, Def. 5.3.2] (and $\mathcal{F}_\Lambda(n)$ is the modification of $\mathcal{F}_\Lambda$ analogous to (3.1)). Moreover, by construction

$$\kappa_{1,\Lambda}^{\mathrm{Kato}} = z_\infty := z_{1,\Lambda} \in \mathrm{H}^1_{\mathcal{F}_\Lambda}(\mathbb{Q}, \mathbf{T}). \tag{2.5}$$

For any character $\alpha : \Gamma \to \mathbb{Z}_p^\times$, let $\kappa_{n,\Lambda}^{\mathrm{Kato}}(\alpha) \in \mathrm{H}^1(\mathbb{Q}, T(\alpha)/I_n T(\alpha))$ denote the α-specialization of $\kappa_{n,\Lambda}^{\mathrm{Kato}}$.

Lemma 2.1.1. *Suppose $\alpha : \Gamma \to \mathbb{Z}_p^\times$ is such that $\alpha \equiv 1 \pmod{p^m}$ for some $m \geq 1$. Then for all $n \in \mathcal{N}$ with $p^m \in I_n$ the classes $\kappa_{n,\Lambda}^{\mathrm{Kato}}(\alpha)$ and κ_n^{Kato} have the same image in $\mathrm{H}^1(\mathbb{Q}, T(\alpha)/p^m T(\alpha)) \cong \mathrm{H}^1(\mathbb{Q}, T/p^m T)$:*

$$\kappa_{n,\Lambda}^{\mathrm{Kato}}(\alpha) \equiv \kappa_n^{\mathrm{Kato}} \pmod{p^m}.$$

Proof. This is clear from the construction of the Kolyvagin systems in [MR04, App. A]. □

As in [BCGS26], the specialized Kolyvagin system

$$\boldsymbol{\kappa}_\Lambda^{\mathrm{Kato}}(\alpha) = \{\kappa_{n,\Lambda}^{\mathrm{Kato}}(\alpha)\}_n \in \mathbf{KS}(T(\alpha), \mathcal{F}_{\mathrm{rel}}, \mathcal{L}) \tag{2.6}$$

(see [MR04, Cor. 5.3.15] for the last inclusion) will be of use because of the following fundamental result.

Theorem 2.1.2. *Suppose $\alpha : \Gamma \to \mathbb{Z}_p^\times$ is a non-trivial character with $\alpha \equiv 1 \pmod{p^m}$ for some $m \geq 1$. Then*

$$\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha) \neq 0 \text{ for } m \gg 0.$$

In other words, for $m \gg 0$ the Kolyvagin system $\boldsymbol{\kappa}_\Lambda^{\mathrm{Kato}}(\alpha)$ is non-trivial.

Proof. In light of (2.5), the result follows from Kato's explicit reciprocity law [Kat04, Thm. 16.6] and Rohrlich's nonvanishing results [Roh84]. □

2.1.2. *Link with Kurihara's δ_n.* The bridge allowing us to translate our results on Kato's derived cohomology classes κ_n^{Kato} to statements about Kurihara's analytic quantities δ_n is the following extension of Kato's explicit reciprocity law (2.2).

Theorem 2.1.3. *Suppose $p > 3$ is a prime such that (sur) and ($p \nmid c_\phi$) both hold. Reducing the dual exponential map $\exp_{\omega_E^*} : \mathrm{H}^1(\mathbb{Q}_p, T) \to \mathbb{Z}_p$ modulo I_n, for $n > 1$, induces a well-defined map*

$$\overline{\exp^*_{\omega_E}} : \mathrm{H}^1(\mathbb{Q}_p, T/I_n T) \to \mathbb{Z}_p/I_n\mathbb{Z}_p$$

with the property that

$$\overline{\exp^*_{\omega_E}}\big(\mathrm{res}_p(\kappa_n^{\mathrm{Kato}})\big) = u \cdot p^t \cdot \delta_n,$$

where $u \in (\mathbb{Z}_p/I_n\mathbb{Z}_p)^\times$ and $p^t = \#E(\mathbb{Q}_p)[p^\infty]$.

Proof. This is shown in [Kim26, Thm. 3.11] building on computations in [KKS20, §§6-7]. □

2.1.3. *Exact formula for the strict Selmer group.* We shall need the following consequence of Mazur–Rubin's extension of Kolyvagin's structure theorem for Selmer groups [Kol91b] to the context of [MR04].

Let

$$T(\alpha)^* := \mathrm{Hom}(T(\alpha), \mu_{p^\infty}) = T(\alpha)^\vee(1)$$

denote the dual of $T(\alpha)$ (where $(-)^\vee$ denotes the Pontryagin dual) and let $\mathcal{F}_{\mathrm{str}}$ the Selmer structure *dual* to $\mathcal{F}_{\mathrm{rel}}$ in the sense of [MR04, §2.3]. In the statement below, the divisibility index $\mathscr{M}_\infty(\boldsymbol{\kappa}_\Lambda^{\mathrm{Kato}}(\alpha)) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ is defined just as $\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Heeg}})$ in §1.1.5 (see also [MR04, Def. 5.2.11], where the notation $\partial^{(\infty)}(\boldsymbol{\kappa}^{\mathrm{Kato}})$ is used).

Theorem 2.1.4. *Suppose $p > 3$ is a prime such that (sur) holds, and $\alpha : \Gamma \to \mathbb{Z}_p^\times$ is a character with $\alpha \equiv 1 \pmod{p^m}$ for some $m \geq 1$ such that $\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha) \neq 0$. Then $\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(K, T(\alpha)^*)$ is finite, with*

$$\mathrm{length}_{\mathbb{Z}_p}\big(\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(K, T(\alpha)^*)\big) = \mathrm{ind}_p(\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha)) - \mathscr{M}_\infty(\boldsymbol{\kappa}_\Lambda^{\mathrm{Kato}}(\alpha)).$$

Proof. This follows from [MR04, Thm. 5.2.12]. □

2.1.4. *Rigidity.* We conclude this section with a technical result showing a certain 'rigidity' property for the divisibility index $\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Kato}})$. As in the proof of the analogous result in [BCGS26, Prop. 2.2.1] for the Heegner point Kolyvagin system, the argument essentially goes back to Kolyvagin (cf. [McC91, Prop. 5.2]).

For every $m \geq 1$, let $\mathcal{L}^{(m)} \subset \mathcal{L}$ consist of the primes $\ell \in \mathcal{L}$ with $p^m \in I_n$, and write $\mathcal{N}^{(m)}$ for the set of all squarefree products of primes $\ell \in \mathcal{L}^{(m)}$ (with $1 \in \mathcal{N}^{(m)}$ as usual), so clearly we have the chain of inclusions

$$\mathcal{N} = \mathcal{N}^{(1)} \supset \cdots \supset \mathcal{N}^{(m)} \supset \mathcal{N}^{(m+1)} \supset \cdots . \tag{2.7}$$

Let $\boldsymbol{\kappa} = \{\kappa_n\}_{n\in\mathcal{N}}$ denote either $\boldsymbol{\kappa}^{\mathrm{Kato}}$ or $\boldsymbol{\kappa}^{\mathrm{Kato}}_\Lambda(\alpha)$ for some $\alpha : \Gamma \to \mathbb{Z}_p^\times$, and define $\mathscr{M}_\infty^{(m)}(\boldsymbol{\kappa}) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ in the same manner as $\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Kato}})$ and $\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Kato}}_\Lambda(\alpha))$, with $\mathcal{N}$ replaced by $\mathcal{N}^{(m)}$.

Proposition 2.1.5. *Suppose $p > 3$ is a prime satisfying* (sur)*. Then*

$$\mathscr{M}_\infty(\boldsymbol{\kappa}) = \mathscr{M}_\infty^{(m)}(\boldsymbol{\kappa})$$

for every $m \geq 1$.

Proof. The inequality $\mathscr{M}_\infty(\boldsymbol{\kappa}) \leq \mathscr{M}_\infty^{(m)}(\boldsymbol{\kappa})$ is immediate from (2.7). Let $r \geq 0$ be such that

$$\mathscr{M}_\infty(\boldsymbol{\kappa}) = \mathscr{M}_r := \min\{\mathrm{ind}_p(\kappa_n) \,:\, n \in \mathcal{N} \text{ and } \nu(n) = r\},$$

and take $n \in \mathcal{N}$ with $\nu(n) = r$ and $\mathrm{ind}_p(\kappa_n) = \mathscr{M}_r$. If $\mathscr{M}_r = \infty$ there is nothing to show, so in the following we assume $\mathscr{M}_r < \infty$. Put

$$\mu := \mathscr{M}_r$$

for the ease of notation, and note that necessarily $n \in \mathcal{N}^{(\mu+1)}$. If $m \leq \mu + 1$ then again there is nothing to show (in view of (2.7)), so in the following we also assume $m > \mu + 1$.

Suppose there exists a prime factor $\ell \mid n$ with $\ell \notin \mathcal{L}^{(m)}$. We shall show that there exists $\ell' \in \mathcal{L}^{(m)}$ such that $n' := \ell' n/\ell$ satisfies $\mathrm{ind}_p(\kappa_{n'}) = \mu$. Repeating this process for any prime factors of n in $\mathcal{L}^{(\mu+1)} \smallsetminus \mathcal{L}^{(m)}$ we will thus arrive at $n'' \in \mathcal{N}^{(m)}$ with $\mathrm{ind}_p(\kappa_{n''}) = \mu$; this will show $\mathscr{M}_\infty^{(m)}(\boldsymbol{\kappa}) \leq \mu$, concluding the proof.

In the following we set $\mathcal{F} = \mathcal{F}_{\mathrm{rel}}$ to simplify notation. Letting $\kappa_n^{(\mu+1)} \in \mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T/p^{\mu+1}T)$ be the reduction of κ_n modulo $p^{\mu+1}$, by assumption $\kappa_n^{(\mu+1)} \neq 0$ and is contained in $p^\mu \mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T/p^{\mu+1}T)$. Hence via the natural identification

$$p^\mu \mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T/p^{\mu+1}T) \cong \mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, \bar{T}),$$

where $\bar{T} := T/pT \cong E[p]$ (see [MR04, Lem. 3.5.4]), $\kappa_n^{(\mu+1)}$ defines a nonzero class $\bar{\kappa} \in \mathrm{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, \bar{T})$. By [MR04, Prop. 3.6.1], there exists $\ell' \in \mathcal{L}^{(m)}$ with $\ell' \nmid n$ such that $\mathrm{loc}_{\ell'}(\bar{\kappa}) \in \mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}_\ell, \bar{T})$ is nonzero. Since $\mathcal{L}^{(m)} \subset \mathcal{L}^{(\mu+1)}$, the class $\kappa_{n\ell'}^{(\mu+1)} \in \mathrm{H}^1_{\mathcal{F}(n\ell')}(\mathbb{Q}, T^{(\mu+1)})$ (obtained by reducing $\kappa_{n\ell'}$ modulo $p^{\mu+1}$) is defined, and the Kolyvagin system relations (see [MR04, Def. 3.1.3]) show that $\mathrm{loc}_{\ell'}(\kappa_{n\ell'}^{(\mu+1)})$ and $\mathrm{loc}_{\ell'}(\kappa_n^{(\mu+1)})$ have the same order. Since $\mathrm{loc}_{\ell'}(\bar{\kappa}) \neq 0$, it follows that the class $\bar{\kappa}_{\ell'} \in \mathrm{H}^1_{\mathcal{F}(n\ell')}(\mathbb{Q}, \bar{T})$ defined by $\kappa_{n\ell'}^{(\mu+1)}$ is also nonzero, and so $\kappa_{n\ell'}^{(\mu+1)} \notin p^{\mu+1}\mathrm{H}^1_{\mathcal{F}(n\ell')}(\mathbb{Q}, T/p^{\mu+1}T)$. Moreover, since $\nu(n\ell') = r + 1$, from the definitions we see that

$$\mathrm{ind}_p(\kappa_{n\ell'}) \geq \mathscr{M}_{r+1} = \mathscr{M}_r,$$

and so $\mathrm{ind}_p(\kappa_{n\ell'}) = \mu$; moreover, $\mathrm{loc}_{\ell'}(\bar{\kappa}_{\ell'}) \in \mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, \bar{T})$ is nonzero by the Kolyvagin system relations. Now for any place v of $\mathbb{Q}$, let

$$\langle\,,\,\rangle_v : \mathrm{H}^1(\mathbb{Q}_v, \bar{T}) \times \mathrm{H}^1(\mathbb{Q}_v, \bar{T}) \to \mathbb{F}_p$$

denote the local Tate pairing. For $v \nmid n\ell'$ (resp. $v \mid n/\ell$) the classes $\mathrm{loc}_v(\bar{\kappa})$ and $\mathrm{loc}_v(\bar{\kappa}_{\ell'})$ are orthogonal under $\langle\,,\,\rangle_v$, since they are both unramified (resp. transverse) at v, so together with the global reciprocity theorem of class field theory we see that

$$0 = \sum_v \langle \mathrm{loc}_v(\bar{\kappa}), \mathrm{loc}_v(\bar{\kappa}_{\ell'})\rangle_v = \langle \mathrm{loc}_\ell(\bar{\kappa}), \mathrm{loc}_\ell(\bar{\kappa}_{\ell'})\rangle_\ell + \langle \mathrm{loc}_{\ell'}(\bar{\kappa}), \mathrm{loc}_{\ell'}(\bar{\kappa}_{\ell'})\rangle_{\ell'}. \tag{2.8}$$

Since $\langle\,,\,\rangle_{\ell'}$ induces a non-degenerate pairing

$$\mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}_{\ell'}, \bar{T}) \times \mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_{\ell'}, \bar{T}) \to \mathbb{F}_p,$$

the above shows that $\langle \mathrm{loc}_{\ell'}(\bar{\kappa}), \mathrm{loc}_{\ell'}(\bar{\kappa}_{\ell'})\rangle_{\ell'} \neq 0$, which by (2.8) implies that $\mathrm{loc}_{\ell_0}(\bar{\kappa}_{\ell'}) \neq 0$. Put $n' := \ell' n/\ell \in \mathcal{N}^{(\mu+1)}$. By the same argument as above, we see that the nonvanishing of $\mathrm{loc}_\ell(\bar{\kappa}_{\ell'})$ implies that the reduction

$\kappa_{n'}^{(\mu+1)}$ of $\kappa_{n'}$ modulo $p^{\mu+1}$ satisfies $\kappa_{n'}^{(\mu+1)} \notin p^{\mu+1}\mathrm{H}^1_{\mathcal{F}(n')}(\mathbb{Q}, T/p^{\mu+1}T)$, and in fact $\mathrm{ind}_p(\kappa_{n'}^{(\mu+1)}) = \mu$, whence the result. □

2.2. **Determinantal Kato's Main Conjecture.** Clearly, our hypothesis (sur) implies that

$$E(\mathbb{Q})[p] = 0, \tag{$\mathrm{tor}_{\mathbb{Q}}$}$$

and we note that only the latter will be needed in this section.

Let S be the set of places of $\mathbb{Q}$ consisting of the infinite place and the primes dividing Np. We set $\mathbb{Z}_S := \mathbb{Z}[1/Np]$. As is well-known (see e.g. [FK06]), the cohomology complex $\mathbf{R}\Gamma(\mathbb{Z}_S, \mathbf{T})$ is a perfect complex of Λ-modules, acyclic outside degrees 1 and 2. By [Kat04, Thm. 12.4(1)], its second cohomology group $\mathrm{H}^2(\mathbb{Z}_S, \mathbf{T})$ is Λ-torsion, and so taking cohomology (and using that $\mathbf{R}\Gamma(\mathbb{Z}_S, \mathbf{T})$ has Euler characteristic $-\mathrm{rank}_{\mathbb{Z}_p}(T^-) = -1$, for T^- the minus part of T for complex conjugation) we obtain the canonical isomorphism

$$Q(\Lambda) \otimes_\Lambda \det_\Lambda^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, \mathbf{T}) \cong Q(\Lambda) \otimes_\Lambda \mathrm{H}^1(\mathbb{Z}_S, \mathbf{T}), \tag{2.9}$$

where $Q(\Lambda)$ denotes the fraction field of Λ.

Remark 2.2.1. Although it will not be needed in the following, we note that, as shown in [BS21, Thm. 2.18], just assuming ($\mathrm{tor}_{\mathbb{Q}}$) one can define a canonical Λ-module homomorphism

$$\det_\Lambda^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, \mathbf{T}) \to \mathrm{H}^1(\mathbb{Z}_S, \mathbf{T})$$

which is injective if and only if $\mathrm{H}^2(\mathbb{Z}_S, \mathbf{T})$ is Λ-torsion, and it induces (2.9) after extension of scalars to $Q(\Lambda)$.

As in [GV00], for any prime $\ell \neq p$ let $P_\ell(E, \ell^{-s})$, where $P_\ell(E, X) = (1 - \alpha_\ell X)(1 - \beta_\ell X)$ (with one or both of α_ℓ, β_ℓ possibly zero) be the Euler factor of $L(E, s)$ at ℓ, and put

$$\mathcal{P}_\ell := (1 - \alpha_\ell \ell^{-1}\gamma_\ell)(1 - \beta_\ell \ell^{-1}\gamma_\ell) \in \Lambda, \tag{2.10}$$

where $\gamma_\ell \in \Gamma$ denotes the Frobenius at ℓ. Define the *S-imprimitive* variant of z_∞ by

$$z_\infty^{(S)} := \mathcal{P}_N \cdot z_\infty \in \mathrm{H}^1(\mathbb{Z}_S, \mathbf{T}), \tag{2.11}$$

where $\mathcal{P}_N = \prod_{\ell | N} \mathcal{P}_\ell$. In these terms, the Iwasawa Main Conjecture, in the formulation of [KS24, Conj. 3.4], takes the following form.

Conjecture 2.2.2 (Main Conjecture for Kato's Euler system)**.** *Let p be an odd prime, and assume that* ($\mathrm{tor}_{\mathbb{Q}}$) *holds and* $\mathrm{H}^2(\mathbb{Z}_S, \mathbf{T})$ *is Λ-torsion. Then there exists a Λ-basis*

$$\mathfrak{z}_{\mathbb{Q}_\infty} \in \det_\Lambda^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, \mathbf{T})$$

that maps to $z_\infty^{(S)}$ under the canonical isomorphism (2.9)*.*

The following result shows that Conjecture 2.2.2 is equivalent to the Iwasawa Main Conjecture formulated by Kato in [Kat04, Conj. 12.10].

Proposition 2.2.3. *Conjecture 2.2.2 holds if and only if*

$$\mathrm{char}_\Lambda\big(\mathrm{H}^1(\mathbb{Z}_S, \mathbf{T})/\Lambda \cdot z_\infty^{(S)}\big) = \mathrm{char}_\Lambda\big(\mathrm{H}^2(\mathbb{Z}_S, \mathbf{T})\big) \tag{2.12}$$

as ideals in Λ.

Proof. As noted in [BKS24, Rem. 7.2], this follows from Proposition 2.1.5 in Chapter I of [Kat93]. (See also [KS24, Prop. 3.10].) □

Remark 2.2.4. In fact, one can show that the "upper bound" divisibility "$\subset$" in (2.12) amounts to the claim that the inverse image $\mathfrak{z}_{\mathbb{Q}_\infty}$ of $z_\infty^{(S)}$ under (2.9) is integral, i.e., $\Lambda \cdot \mathfrak{z}_{\mathbb{Q}_\infty} \subset \det_\Lambda^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, \mathbf{T})$.

2.3. **Descent computations.** From the Poitou–Tate duality sequence (2.13) below, we see that if the condition

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T(\alpha)^*) \text{ is finite} \tag{str-fin}$$

holds, then $\mathrm{H}^2(\mathbb{Z}_S, T(\alpha))$ is also finite and we have a canonical isomorphism

$$\vartheta : \det_{\mathbb{Q}_p}^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, V(\alpha)) \cong \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{H}^1(\mathbb{Z}_S, T(\alpha)),$$

where $V = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$.

Proposition 2.3.1. *Suppose $\alpha : \Gamma \to \mathbb{Z}_p^\times$ is such that $\alpha \equiv 1 \pmod{p^m}$ for some $m \geq 1$ and $\kappa^{\mathrm{Kato}}_{1,\Lambda}(\alpha) \neq 0$. Then $\mathrm{H}^1(\mathbb{Z}_S, T(\alpha))$ is $\mathbb{Z}_p$-free of rank one, $\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T(\alpha)^*)$ is finite, and for $m \gg 0$ we have*

$$\vartheta\big(\det_{\mathbb{Z}_p}^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, T(\alpha))\big) = \mathbb{Z}_p \cdot \left(\prod_{\ell \mid Np} \#E(\mathbb{Q}_\ell)[p^\infty]\right) \cdot \#\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T(\alpha)^*) \cdot x,$$

where x is any $\mathbb{Z}_p$-basis of $\mathrm{H}^1(\mathbb{Z}_S, T(\alpha))$.

Proof. By [MR04, Thm. 5.2.2] applied to (2.6), the nonvanishing of $\kappa^{\mathrm{Kato}}_{1,\Lambda}(\alpha)$ implies that $\mathrm{H}^1_{\mathcal{F}_{\mathrm{rel}}}(\mathbb{Q}, T(\alpha)) \cong \mathbb{Z}_p$ and $\#\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T(\alpha)^*) < \infty$. By Poitou–Tate duality we have the exact sequence

$$\begin{aligned} 0 \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{rel}}}(\mathbb{Q}, T(\alpha)) \to \mathrm{H}^1(\mathbb{Z}_S, T(\alpha)) \to \bigoplus_{\ell \mid N} \frac{\mathrm{H}^1(\mathbb{Q}_\ell, T(\alpha))}{\mathrm{H}^1_f(\mathbb{Q}_\ell, T(\alpha))} \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T(\alpha)^*)^\vee \\ \to \mathrm{H}^2(\mathbb{Z}_S, T(\alpha)) \to \bigoplus_{\ell \mid Np} \mathrm{H}^2(\mathbb{Q}_\ell, T(\alpha)) \to \mathrm{H}^0(\mathbb{Q}, T(\alpha)^*)^\vee \to 0. \end{aligned} \tag{2.13}$$

Noting that $\mathrm{H}^1_f(\mathbb{Q}_\ell, T(\alpha)) = \mathrm{H}^1(\mathbb{Q}_\ell, T(\alpha))_{\mathrm{tor}} = \mathrm{H}^1(\mathbb{Q}_\ell, T(\alpha))$ for any prime $\ell \mid N$, and that $\mathrm{H}^0(\mathbb{Q}, T(\alpha)^*) = 0$ by ($\mathrm{tor}_{\mathbb{Q}}$), we see that $\mathrm{H}^1_{\mathcal{F}_{\mathrm{rel}}}(\mathbb{Q}, T(\alpha)) = \mathrm{H}^1(\mathbb{Z}_S, T(\alpha))$, concluding all but the last claim in the statement, and we extract the short exact sequence

$$0 \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T(\alpha)^*)^\vee \to \mathrm{H}^2(\mathbb{Z}_S, T(\alpha)) \to \bigoplus_{\ell \mid Np} \mathrm{H}^2(\mathbb{Q}_\ell, T(\alpha)) \to 0.$$

Since $\mathrm{H}^2(\mathbb{Q}_\ell, T(\alpha)) \cong \mathrm{H}^0(\mathbb{Q}_\ell, T(\alpha)^*)^\vee$ by local duality, and for $m \gg 0$ we have $\#\mathrm{H}^0(\mathbb{Q}_\ell, T(\alpha)^*) = \#\mathrm{H}^0(\mathbb{Q}_\ell, T^*) = \#E(\mathbb{Q}_\ell)[p^\infty]$, we obtain a canonical isomorphism

$$\begin{aligned} \det_{\mathbb{Z}_p}^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, T(\alpha)) &\cong \det_{\mathbb{Z}_p}(\mathrm{H}^1(\mathbb{Z}_S, T(\alpha))) \otimes \det_{\mathbb{Z}_p}^{-1}(\mathrm{H}^2(\mathbb{Z}_S, T(\alpha))) \\ &\cong \left(\prod_{\ell \mid Np} \#E(\mathbb{Q}_\ell)[p^\infty]\right) \cdot \det_{\mathbb{Z}_p}^{-1}\big(\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T(\alpha)^*)^\vee\big) \otimes \det_{\mathbb{Z}_p}\big(\mathrm{H}^1(\mathbb{Z}_S, T(\alpha))\big) \\ &\cong \left(\prod_{\ell \mid Np} \#E(\mathbb{Q}_\ell)[p^\infty]\right) \cdot \#\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T(\alpha)^*) \cdot \mathrm{H}^1(\mathbb{Z}_S, T(\alpha)), \end{aligned}$$

which concludes the proof. □

Corollary 2.3.2. *Suppose $\alpha : \Gamma \to \mathbb{Z}_p^\times$ satisfies $\alpha \equiv 1 \pmod{p^m}$ for some $m \geq 1$ and is such that $\kappa^{\mathrm{Kato}}_{1,\Lambda}(\alpha) \neq 0$. If Conjecture 2.2.2 holds, then up to a p-adic unit:*

$$\#\big(\mathrm{H}^1_{\mathcal{F}_{\mathrm{rel}}}(\mathbb{Z}_S, T(\alpha))/\mathbb{Z}_p \cdot \kappa^{\mathrm{Kato}}_{1,\Lambda}(\alpha)\big) = \#E(\mathbb{Q}_p)[p^\infty] \cdot \#\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T(\alpha)^*) \cdot \mathrm{Tam}_E$$

for $m \gg 0$.

Proof. Suppose Conjecture 2.2.2 holds, and let $\mathfrak{z}_{\mathbb{Q}_\infty}(\alpha) \in \det_{\mathbb{Z}_p}^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, T(\alpha))$ be the image of $\mathfrak{z}_{\mathbb{Q}_\infty}$ under the isomorphism

$$\det_{\Lambda}^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, \mathbf{T}) \otimes_{\Lambda,\alpha} \mathbb{Z}_p \cong \det_{\mathbb{Z}_p}^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, T(\alpha)) \tag{2.14}$$

coming from [FK06, Prop. 1.6.5(3)]. Let $\mathrm{Eul}_N(\alpha) = \mathcal{P}_N(\alpha)$ denote the product of the Euler factors of $L(E, \alpha, s)$ at $s = 1$ (see (2.10)). Since $p \nmid N$, we have $\mathrm{Eul}_N(\alpha) \in \mathbb{Z}_{(p)}$ and for $m \gg 0$ we see that

$$\mathrm{ord}_p(\mathrm{Eul}_N(\alpha)) = \mathrm{ord}_p\left(\prod_{\ell \mid N} \#\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_\ell)\right). \tag{2.15}$$

Then $\mathfrak{z}_{\mathbb{Q}_\infty}(\alpha)$ is a $\mathbb{Z}_p$-basis of $\det_{\mathbb{Z}_p}^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, T(\alpha))$, and by construction its image under ϑ agrees with $\mathrm{Eul}_N(\alpha)\cdot\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha)$. As shown in the proof of Proposition 2.3.1, we have $\mathrm{H}^1_{\mathcal{F}_{\mathrm{rel}}}(\mathbb{Q}, T(\alpha)) = \mathrm{H}^1(\mathbb{Z}_S, T(\alpha))$, and from there and (2.15) we see that for $m \gg 0$ we have

$$\mathrm{ind}_p(\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha)) = \mathrm{ord}_p(\#E(\mathbb{Q}_p)[p^\infty]) + \sum_{\ell\mid N}\big(\mathrm{ord}_p(\#E(\mathbb{Q}_\ell)[p^\infty]) - \mathrm{ord}_p(\#\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_\ell))\big) + \mathrm{ord}_p(\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(\mathbb{Q}, T(\alpha)^*)),$$

which clearly implies the result. □

2.4. **Proof of Theorem A.** Choose a non-trivial character $\alpha : \Gamma \to \mathbb{Z}_p^\times$ with $\alpha \equiv 1 \pmod{p^m}$ for some $m \geq 1$, and suppose m is large enough so that $\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha) \neq 0$ (see Theorem 2.1.2).

Suppose the Iwasawa Main Conjecture 2.2.2 holds. Then from Theorem 2.1.4 and Corollary 2.3.2 we have that $\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(K, T(\alpha)^*)$ is finite, with

$$\begin{aligned}\mathrm{ord}_p(\#\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(K, T(\alpha)^*)) &= \mathrm{ind}_p(\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha)) - \mathscr{M}_\infty(\boldsymbol{\kappa}_\Lambda^{\mathrm{Kato}}(\alpha))\\ &= \mathrm{ord}_p(\#E(\mathbb{Q}_p)[p^\infty]) + \mathrm{ord}_p(\#\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(K, T(\alpha)^*)) + \mathrm{ord}_p(\mathrm{Tam}_E) - \mathscr{M}_\infty(\boldsymbol{\kappa}_\Lambda^{\mathrm{Kato}}(\alpha)),\end{aligned}$$

and so

$$\mathscr{M}_\infty(\boldsymbol{\kappa}_\Lambda^{\mathrm{Kato}}(\alpha)) = \mathrm{ord}_p(\#E(\mathbb{Q}_p)[p^\infty]) + \mathrm{ord}_p(\mathrm{Tam}_E). \tag{2.16}$$

Since the chain of equalities

$$\begin{aligned}\mathscr{M}_\infty(\boldsymbol{\kappa}_\Lambda^{\mathrm{Kato}}(\alpha)) &= \mathscr{M}_\infty^{(m)}(\boldsymbol{\kappa}_\Lambda^{\mathrm{Kato}}(\alpha))\\ &= \mathscr{M}_\infty^{(m)}(\boldsymbol{\kappa}^{\mathrm{Kato}}) = \mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Kato}}) = \mathscr{M}_\infty(\boldsymbol{\delta}) + \mathrm{ord}_p(\#E(\mathbb{Q}_p)[p^\infty])\end{aligned} \tag{2.17}$$

follows from Proposition 2.1.5, Lemma 2.1.1, Proposition 2.1.5, and Theorem 2.1.3, respectively, combining (2.16) and (2.17) this gives the implication (ii) ⇒ (i) in Theorem A.

Conversely, suppose the equality $\mathscr{M}_\infty(\boldsymbol{\delta}) = \mathrm{ord}_p(\mathrm{Tam}_E)$ holds, so from (2.17) we deduce that (2.16) holds, which together with Theorem 2.1.4 gives

$$\mathrm{ind}_p(\kappa_{1,\Lambda}^{\mathrm{Kato}}(\alpha)) = \mathrm{ord}_p(\#\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(K, T(\alpha)^*)) + \mathrm{ord}_p(\#E(\mathbb{Q}_p)[p^\infty]) + \mathrm{ord}_p(\mathrm{Tam}_E). \tag{2.18}$$

Let $\mathfrak{z}_{\mathbb{Q}_\infty} \in Q(\Lambda)\otimes_\Lambda \det_\Lambda^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, \mathbf{T})$ be the inverse image of $z_\infty^{(S)} \in \mathrm{H}^1(\mathbb{Z}_S, \mathbf{T})$ under the isomorphism (2.9). Since $z_\infty = \kappa_{1,\Lambda}^{\mathrm{Kato}}$ is non-torsion by Theorem 2.1.2, by [MR04, Thm. 5.3.10] applied to the Kolyvagin system (2.4) we deduce the divisibility

$$\mathrm{char}_\Lambda\big(\mathrm{H}^1(\mathbb{Z}_S, \mathbf{T})/\Lambda\cdot z_\infty^{(S)}\big) \subset \mathrm{char}_\Lambda\big(\mathrm{H}^2(\mathbb{Z}_S, \mathbf{T})\big), \tag{2.19}$$

and so by Remark 2.2.4 we deduce the integrality $\mathfrak{z}_{\mathbb{Q}_\infty} \in \det_\Lambda^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, \mathbf{T})$. Letting $\mathfrak{z}_{\mathbb{Q}_\infty}(\alpha)$ be the image of $\mathfrak{z}_{\mathbb{Q}_\infty}$ under the isomorphism (2.14), the computations in §2.3 show that $\mathfrak{z}_{\mathbb{Q}_\infty}(\alpha)$ is a $\mathbb{Z}_p$-basis of $\det_{\mathbb{Z}_p}^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, T(\alpha))$ if and only if (2.18) holds. Thus from (2.18), (2.19), [SU14, Lem. 3.2], and our choice of α, it follows that $\mathfrak{z}_{\mathbb{Q}_\infty}$ is a Λ-basis of $\det_{\mathbb{Z}_p}^{-1}\mathbf{R}\Gamma(\mathbb{Z}_S, \mathbf{T})$, thereby concluding the proof.

3. Kolyvagin conjectures

3.1. **Preliminaries.** Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and K a quadratic imaginary field satisfying (Heeg) and (disc). Fix an odd prime p such that (sur) and ($p \nmid c_\phi$) both hold.

3.1.1. *Heegner point Kolyvagin systems.* Keeping the notations from §1.1.5, for every integer $m = np^k$ with $k \geq 0$ and $n \in \mathcal{N}_{\mathrm{Heeg}}$, let $P[m] \in E(K[m])$ be the Heegner point of conductor m constructed in [How04, §1.7], associated with our fixed modular parametrization $\phi : X_0(N) \to E$. Let $x_m \in \mathrm{H}^1(K[m], T)$ denote the image of $P[m]$ under the Kummer map $E(K[m])\otimes_{\mathbb{Z}}\mathbb{Z}_p \to \mathrm{H}^1(K[m], T)$. By Theorem 1.7.3 in *loc. cit.*, after a slight modification the Kolyvagin derivatives of these classes give rise to a Kolyvagin system

$$\boldsymbol{\kappa}^{\mathrm{Heeg}} = \big\{\kappa_n^{\mathrm{Heeg}} \in \mathrm{H}^1_{\mathcal{F}(n)}(K, T/I_nT) \,:\, n \in \mathcal{N}_{\mathrm{Heeg}}\big\}$$

in the sense of [How04, §1.2] for the triple $(T, \mathcal{F}, \mathcal{L})$, where $\mathcal{F}$ is the Selmer structure given by the propagation (in the sense of [MR04]) of the *finite local condition*

$$\mathrm{H}^1_f(K_v, T) := \ker\{\mathrm{H}^1(K_v, T) \to \mathrm{H}^1(K_v^{\mathrm{ur}}, T\otimes\mathbb{Q}_p)\}$$

for $v \nmid p$, and of the image of the local Kummer map $E(K_v)\otimes\mathbb{Q}_p \to \mathrm{H}^1(K_v, T\otimes\mathbb{Q}_p)$ for $v \mid p$; and $\mathcal{F}(n)$ is the modification of $\mathcal{F}$ given by

$$\mathrm{H}^1_{\mathcal{F}(n)}(K_v, T/I_nT) = \begin{cases} \mathrm{H}^1_{\mathrm{tr}}(K_v, T/I_nT) := \mathrm{H}^1(K_v[\ell]/K_v, \mathrm{H}^0(K_v[\ell], T/I_nT)) & \text{if } v \mid \ell \mid n, \\ \mathrm{H}^1_{\mathcal{F}}(K_v, T/I_nT) & \text{if } v \nmid n, \end{cases} \tag{3.1}$$

where $K_v[\ell]$ denotes the maximal p-extension of K_v inside the completion of the ring class field $K[\ell]$ at any of the primes above v. In particular, the construction gives

$$\kappa_1^{\mathrm{Heeg}} = \mathrm{Cor}_K^{K[1]}(x_1) \in \mathrm{H}^1_{\mathcal{F}}(K,T) \cong \varprojlim_m \mathrm{Sel}_{p^m}(E/K).$$

Assume now that

$$E \text{ has good ordinary reduction at } p \tag{ord}$$

and

$$p \text{ is unramified in } K. \tag{unr}$$

Let $K_\infty = \cup_{k\geq 0} K_k$ be the anticyclotomic $\mathbb{Z}_p$-extension of K, and put $\Gamma^{\mathrm{ac}} = \mathrm{Gal}(K_\infty/K)$ and $\Lambda^{\mathrm{ac}} = \mathbb{Z}_p[[\Gamma^{\mathrm{ac}}]]$. Let now $\mathbf{T} = T\otimes_{\mathbb{Z}_p}\Lambda^{\mathrm{ac}}$ denote the anticyclotomic deformation of T, where the G_K-action on Λ^{ac} is given by the inverse of the character $G_K \twoheadrightarrow \Gamma^{\mathrm{ac}} \hookrightarrow (\Lambda^{\mathrm{ac}})^\times$. As shown in [How04, §2.3] and Theorem 4.1.1 in [CGLS22], from the Kummer images x_{np^k} for varying k one obtains the construction of a Λ^{ac}-adic Kolyvagin system

$$\boldsymbol{\kappa}_\Lambda^{\mathrm{Heeg}} = \left\{\kappa_{n,\Lambda}^{\mathrm{Heeg}} \in \mathrm{H}^1_{\mathcal{F}_\Lambda(n)}(K, \mathbf{T}/I_n\mathbf{T}) \,:\, n \in \mathcal{N}_{\mathrm{Heeg}}\right\}$$

for the triple $(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{L}_{\mathrm{Heeg}})$, where $\mathcal{F}_\Lambda$ is the Selmer structure given by

$$\mathrm{H}^1_{\mathcal{F}_\Lambda}(K_v, \mathbf{T}) = \begin{cases} \mathrm{H}^1_{\mathrm{ur}}(K_v, \mathbf{T}) := \mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, \mathrm{H}^0(K_v^{\mathrm{ur}}, \mathbf{T})) & \text{if } v \nmid p, \\ \mathrm{im}\{\mathrm{H}^1(K_v, \mathbf{T}_v^+) \to \mathrm{H}^1(K_v, \mathbf{T})\} & \text{if } v \mid p, \end{cases}$$

where $\mathbf{T}_v^+ := T_v^+ \otimes_{\mathbb{Z}_p} \Lambda^{\mathrm{ac}} \subset \mathbf{T}$ with $T_v^+ = \ker(T \to T_p\widetilde{E})$ the kernel of the reduction map at v. Note that we have $\mathrm{H}^1_{\mathrm{ur}}(K_v, \mathbf{T}) = \mathrm{H}^1(K_v, \mathbf{T})$ for $v \nmid p$ (see [MR04, Lem. 5.3.1(ii)]).

In particular (see [CGLS22, Rem. 4.1.3]), letting α_p be the p-adic unit root of $x^2 - a_p x + p$ and $P[p^k]_{\alpha_p} \in E(K[p^k])\otimes\mathbb{Z}_p$ be the *α_p-stabilized* Heegner point

$$P[p^k]_{\alpha_p} := \begin{cases} P[p^k] - \alpha_p^{-1}P[p^{k-1}] & \text{if } k \geq 1, \\ u_K^{-1}(1-\alpha_p^{-1}\sigma_p)(1-\alpha_p^{-1}\sigma_p^*)P[1] & \text{if } k = 0 \text{ and } p \text{ splits in } K, \\ u_K^{-1}(1-\alpha_p^{-2})P[1] & \text{if } k = 0 \text{ and } p \text{ is inert in } K, \end{cases} \tag{3.2}$$

where $u_K = \#(\mathcal{O}_K^\times/\{\pm 1\})$ (which is 1 under (disc)), and $\sigma_p, \sigma_p^* \in \mathrm{Gal}(K[1]/K)$ denote the Frobenius elements at the primes above p, the class $\kappa_{1,\Lambda}^{\mathrm{Heeg}} \in \mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ agrees up to a p-adic unit with the inverse image

$$y_\infty = \varprojlim_k y_k \in \varprojlim_k \mathrm{H}^1(K_k, T), \tag{3.3}$$

where y_k is the Kummer image of $\alpha_p^{-d(k)}\mathrm{Norm}_{K_k}^{K[p^{d(k)}]}(P[p^{d(k)}]_{\alpha_p}) \in E(K_k)\otimes\mathbb{Z}_p$, with $d(k)$ the smallest integer such that $K_k \subset K[p^{d(k)}]$. Note that (3.2) gives rise to

$$y_0 = \begin{cases} u_K^{-1}(1-\alpha_p^{-1})^2 x_1 & \text{if } p \text{ splits in } K, \\ u_K^{-1}(1-\alpha_p^{-2})x_1 & \text{if } p \text{ is inert in } K. \end{cases}$$

A similar computation directly from the construction yields the following result, where we let

$$\boldsymbol{\kappa}_\Lambda^{\mathrm{Heeg}}(\alpha) = \{\kappa_{n,\Lambda}^{\mathrm{Heeg}}(\alpha)\}_n \in \mathbf{KS}(T(\alpha), \mathcal{F}_\alpha, \mathcal{L}_{\mathrm{Heeg}}) \tag{3.4}$$

be the Kolyvagin system for $T(\alpha)$ obtained from $\boldsymbol{\kappa}_\Lambda^{\mathrm{Heeg}}$ by specialization at α, with the Selmer structure $\mathcal{F}_\alpha$ in [How04, Def. 2.1.2] given by propagating

$$\mathrm{H}^1_{\mathcal{F}_\alpha}(K_v, V(\alpha)) = \begin{cases} \mathrm{H}^1_{\mathrm{ur}}(K_v, V(\alpha)) := \mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, \mathrm{H}^0(K_v^{\mathrm{ur}}, V(\alpha))) & \text{if } v \nmid p, \\ \mathrm{im}\{\mathrm{H}^1(K_v, V_v^+(\alpha)) \to \mathrm{H}^1(K_v, V(\alpha))\} & \text{if } v \mid p, \end{cases} \tag{3.5}$$

where $V_v^+(\alpha) = T_v^+ \otimes_{\mathbb{Z}_p} \mathbb{Q}_p(\alpha) \subset V(\alpha)$ (see Remark 1.2.4 and Lemma 2.2.7 in *op. cit.* for the inclusion (3.4)).

Lemma 3.1.1. *Suppose $\alpha : \Gamma^{\mathrm{ac}} \to \mathbb{Z}_p^\times$ satisfies $\alpha \equiv 1 \pmod{p^m}$ for some $m \geq 1$. Then for all $n \in \mathcal{N}_{\mathrm{Heeg}}$ with $p^m \in I_n$ we have the congruence modulo p^m:*

$$\kappa_{n,\Lambda}^{\mathrm{Heeg}}(\alpha) \equiv \begin{cases} (\alpha_p - 1)^2(\beta_p - 1)^2\kappa_n^{\mathrm{Heeg}} & \text{if } p \text{ splits in } K, \\ ((p+1)^2 - a_p^2)\kappa_n^{\mathrm{Heeg}} & \text{if } p \text{ is inert in } K, \end{cases}$$

where α_p, β_p are the roots of $x^2 - a_p x + p$, with α_p the p-adic unit root.

Proof. See [BCGS26, Lem. 1.1.5]. □

3.1.2. *Exact formula for the p-primary Tate–Shafarevich group.* For $\alpha = 1$, the next result follows from Kolyvagin's structure theorem [Kol91a, Thm. C] for $Ш(E/\mathbb{Q})[p^\infty]$; the general case was proved in [BCGS26] building on the refinement of Kolyvagin's methods in [How04, Zan19] and [CGLS22, CGS25].

Theorem 3.1.2. *Suppose $p > 3$ is a prime such that (sur) holds, and $\alpha : \Gamma^{\mathrm{ac}} \to \mathbb{Z}_p^\times$ is a character such that $\kappa_{1,\Lambda}^{\mathrm{Heeg}}(\alpha) \neq 0$. Then $\mathrm{H}^1_{\mathcal{F}_\alpha}(K, T(\alpha))$ is $\mathbb{Z}_p$-free of rank 1 and there is a non-canonical isomorphism*

$$\mathrm{H}^1_{\mathcal{F}^*_\alpha}(K, T(\alpha)^*) \cong (\mathbb{Q}_p/\mathbb{Z}_p) \oplus S_\alpha \oplus S_\alpha$$

for a finite $\mathbb{Z}_p$-module S_α with

$$\mathrm{length}_{\mathbb{Z}_p}(S_\alpha) = \mathrm{ind}_p(\kappa_{1,\Lambda}^{\mathrm{Heeg}}(\alpha)) - \mathscr{M}_\infty(\boldsymbol{\kappa}_\Lambda^{\mathrm{Heeg}}(\alpha)).$$

Proof. This follows from [BCGS26, Thm. 2.2.2] applied to the Kolyvagin system $\boldsymbol{\kappa}_\Lambda^{\mathrm{Heeg}}(\alpha)$. □

3.2. **Determinantal Perrin-Riou's Main Conjecture.** In addition to our running hypotheses (Heeg) and (disc), only condition

$$E(K)[p] = 0, \tag{tor_K}$$

rather than the stronger (sur), is needed in this section. We also assume hypotheses (ord) and (unr).

Let S be the set of places of K consisting of the infinite place and the primes dividing Np. Put

$$A = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \cong E[p^\infty], \qquad \mathbf{A} = T \otimes_{\mathbb{Z}_p} (\Lambda^{\mathrm{ac}})^\vee \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathbf{T}, \mu_{p^\infty}),$$

where $(\Lambda^{\mathrm{ac}})^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(\Lambda^{\mathrm{ac}}, \mathbb{Q}_p/\mathbb{Z}_p)$ denotes the Pontryagin dual of Λ^{ac}.

For v a prime of K above p, we define $X_v^+ \subset X$ for $X \in \{A, \mathbf{A}\}$ using T_v^+ in the obvious manner. Recall that the *Selmer complex* $\widetilde{\mathbf{R}\Gamma}_f(X)$ for $X \in \{T, A, \mathbf{T}, \mathbf{A}\}$ is defined by the exact triangle

$$\widetilde{\mathbf{R}\Gamma}_f(X) \to \mathbf{R}\Gamma(\mathcal{O}_{K,S}, X) \to \bigoplus_{v|p} \mathbf{R}\Gamma(K_v, X/X_v^+) \oplus \bigoplus_{v \in S, v \nmid p\infty} \mathbf{R}\Gamma_{/\mathrm{ur}}(K_v, X), \tag{3.6}$$

where for the primes $v \mid N$ we put

$$\mathbf{R}\Gamma_{/\mathrm{ur}}(K_v, X) := \mathrm{Cone}\big(\mathbf{R}\Gamma(K_v^{\mathrm{ur}}/K_v, X^{I_v}) \to \mathbf{R}\Gamma(K_v, X)\big)$$

(see [Nek06, (6.1.3.2), (8.8.5)]). Put $\widetilde{\mathrm{H}}^i_f(X) := \mathrm{H}^i(\widetilde{\mathbf{R}\Gamma}_f(X))$.

For $X \in \{T, A, \mathbf{T}, \mathbf{A}\}$, we also let $\mathrm{Sel}_{\mathrm{Gr}}(X)$ denote the *strict Greenberg Selmer group*

$$\mathrm{Sel}_{\mathrm{Gr}}(X) := \ker\left\{ \mathrm{H}^1(\mathcal{O}_{K,S}, X) \to \bigoplus_{v|p} \mathrm{H}^1(K_v, X/X_v^+) \oplus \bigoplus_{v \in S, v \nmid p\infty} \mathrm{H}^1(K_v^{\mathrm{ur}}, X) \right\}, \tag{3.7}$$

and note that $\mathrm{Sel}_{\mathrm{Gr}}(\mathbf{T}) = \mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ by definition.

Theorem 3.2.1. *The module $\mathrm{Sel}_{\mathrm{Gr}}(\mathbf{T})$ is torsion-free and of Λ^{ac}-rank one.*

Proof. This is shown in [How04, Thm. B] under a certain big image hypothesis on T; just assuming (tor_K), it follows from the extension of that result in [CGLS22, Thm. 3.4.1] and [CGS25, Thm. 6.5.2]. □

As explained in [KS24, §5.2.2], using Nekovář's duality [Nek06, (8.9.6.2)] one deduces from Theorem 3.2.1 the existence of a canonical isomorphism

$$Q(\Lambda^{\mathrm{ac}}) \otimes_{\Lambda^{\mathrm{ac}}} \det^{-1}_{\Lambda^{\mathrm{ac}}} \widetilde{\mathbf{R}\Gamma}_f(\mathbf{T}) \cong Q(\Lambda^{\mathrm{ac}}) \otimes_{\Lambda^{\mathrm{ac}}} \mathrm{Sel}_{\mathrm{Gr}}(\mathbf{T}) \otimes_{\Lambda^{\mathrm{ac}}} \mathrm{Sel}_{\mathrm{Gr}}(\mathbf{T})^\iota, \tag{3.8}$$

where $\mathrm{Sel}_{\mathrm{Gr}}(\mathbf{T})^\iota := \mathrm{Sel}_{\mathrm{Gr}}(\mathbf{T}) \otimes_{\Lambda^{\mathrm{ac}}, \iota} \Lambda^{\mathrm{ac}}$ with $\iota : \Lambda^{\mathrm{ac}} \to \Lambda^{\mathrm{ac}}$ denote the involution given by $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \Gamma^{\mathrm{ac}}$. Let

$$y_\infty \otimes y_\infty \in \mathrm{Sel}_{\mathrm{Gr}}(\mathbf{T}) \otimes_{\Lambda^{\mathrm{ac}}} \mathrm{Sel}_{\mathrm{Gr}}(\mathbf{T})^\iota$$

be defined by the Λ-adic Heegner class $y_\infty \in \mathrm{Sel}_{\mathrm{Gr}}(\mathbf{T})$ in (3.3).

Conjecture 3.2.2 (Main Conjecture for Heegner points)**.** *Let*

$$\widetilde{\mathfrak{z}}_{K_\infty} \in Q(\Lambda^{\mathrm{ac}}) \otimes_{\Lambda^{\mathrm{ac}}} \det_{\Lambda^{\mathrm{ac}}}^{-1} \widetilde{\mathbf{R}\Gamma}_f(\mathbf{T})$$

be the element mapping to $y_\infty \otimes y_\infty$ under (3.8). Then $\widetilde{\mathfrak{z}}_{K_\infty}$ is a Λ^{ac}-basis of $\det_{\Lambda^{\mathrm{ac}}}^{-1} \widetilde{\mathbf{R}\Gamma}_f(\mathbf{T})$.

The following result shows that Conjecture 3.2.2 is equivalent to the Iwasawa Main Conjecture for Heegner points formulated by Perrin-Riou in [PR87]. Put $X_{\mathrm{Gr}}(\mathbf{A}) = \mathrm{Sel}_{\mathrm{Gr}}(\mathbf{A})^\vee$.

Proposition 3.2.3. *Conjecture 3.2.2 holds if and only if*

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(\mathrm{Sel}_{\mathrm{Gr}}(\mathbf{T})/\Lambda^{\mathrm{ac}} \cdot y_\infty\big) \cdot \mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(\mathrm{Sel}_{\mathrm{Gr}}(\mathbf{T})/\Lambda^{\mathrm{ac}} \cdot y_\infty\big)^\iota = \mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X_{\mathrm{Gr}}(\mathbf{A})_{\mathrm{tors}}\big) \tag{3.9}$$

as ideals in Λ^{ac}, where the subscript tors *denotes the Λ^{ac}-torsion submodule.*

Proof. In light of Theorem 3.2.1, this follows from [KS24, Prop. 5.12]. □

Remark 3.2.4. As in §2.2, one shows that the upper bound divisibility "$\subset$" in (3.9) amounts to the integrality $\Lambda^{\mathrm{ac}} \cdot \widetilde{\mathfrak{z}}_{K_\infty} \subset \det_{\Lambda^{\mathrm{ac}}}^{-1} \widetilde{\mathbf{R}\Gamma}_f(\mathbf{T})$.

3.3. **Descent computations.** Put

$$Ш_{\mathrm{BK}}(T(\alpha)^*/K) := \frac{\mathrm{H}^1_{\mathcal{F}^*_\alpha}(K, T(\alpha)^*)}{\mathrm{H}^1_{\mathcal{F}^*_\alpha}(K, T(\alpha)^*)_{\mathrm{div}}},$$

where $\mathrm{H}^1_{\mathcal{F}^*_\alpha}(K, T(\alpha)^*)_{\mathrm{div}}$ denotes the maximal divisible submodule of $\mathrm{H}^1_{\mathcal{F}^*_\alpha}(K, T(\alpha)^*)$.

Remark 3.3.1. For $\alpha = \mathbb{1}$, the Selmer condition $\mathcal{F}_\alpha$ is the same as the Selmer condition $\mathcal{F}$ in §3.1.1, and one can show (see e.g. [Fla90]) that $\mathrm{H}^1_{\mathcal{F}^*}(K, T^*)$ agrees with the *Bloch–Kato Selmer group*

$$\mathrm{Sel}_{\mathrm{BK}}(K, T^*) := \ker\left\{ \mathrm{H}^1(\mathcal{O}_{K,S}, T^*) \to \bigoplus_{v \in S} \frac{\mathrm{H}^1(K_v, T^*)}{\mathrm{H}^1_f(K_v, T^*)} \right\},$$

where the local conditions $\mathrm{H}^1_f(K_v, T^*)$ are obtained by propagating via $V \twoheadrightarrow A \cong T^*$ the *finite subspace*

$$\mathrm{H}^1_f(K_v, V) := \begin{cases} \ker\{\mathrm{H}^1(K_v, V) \to \mathrm{H}^1(K_v, V \otimes_{\mathbb{Q}_p} \mathbf{B}_{\mathrm{cris}})\} & \text{if } v \mid p, \\ \ker\{\mathrm{H}^1(K_v, V) \to \mathrm{H}^1(K_v^{\mathrm{ur}}, V)\} & \text{else.} \end{cases}$$

Thus in this case $Ш_{\mathrm{BK}}(T^*/K)$ is the same as Bloch–Kato Tate–Shafarevich group of T^* (and hence equal to the p-primary part $Ш(E/K)[p^\infty]$ of the usual Tate–Shafarevich group of E when the latter is finite). However, we note that for general α, $\mathrm{H}^1_{\mathcal{F}^*_\alpha}(K, T(\alpha)^*)$ may differ from the Bloch–Kato Selmer groups attached to $T(\alpha)^*$.

The next result is a twisted analogue of (3.4.4) in [San23], whose approach we largely follow.

Proposition 3.3.2. *Suppose $\alpha : \Gamma^{\mathrm{ac}} \to \mathbb{Z}_p^\times$ is such that $\alpha \equiv 1 \pmod{p^m}$ for some $m \geq 1$ and $\kappa^{\mathrm{Heeg}}_{1,\Lambda}(\alpha) \neq 0$. Then $\mathrm{H}^1_{\mathcal{F}_\alpha}(K, T(\alpha))$ and $\mathrm{H}^1_{\mathcal{F}_{\alpha^{-1}}}(K, T(\alpha^{-1}))$ are both $\mathbb{Z}_p$-free of rank 1, and there is a canonical isomorphism*

$$\vartheta : \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \det_{\mathbb{Z}_p}^{-1} \widetilde{\mathbf{R}\Gamma}_f(T(\alpha)) \cong \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \big(\mathrm{H}^1_{\mathcal{F}_\alpha}(K, T(\alpha)) \otimes_{\mathbb{Z}_p} \mathrm{H}^1_{\mathcal{F}_{\alpha^{-1}}}(K, T(\alpha^{-1}))\big),$$

with

$$\vartheta\big(\det_{\mathbb{Z}_p}^{-1} \widetilde{\mathbf{R}\Gamma}_f(T(\alpha))\big) = L_p^2 \cdot (\mathrm{Tam}_E)^2 \cdot \#Ш_{\mathrm{BK}}(T(\alpha)^*/K) \cdot \mathbb{Z}_p \otimes_{\mathbb{Z}_p} \big(\mathrm{H}^1_{\mathcal{F}_\alpha}(K, T(\alpha)) \otimes_{\mathbb{Z}_p} \mathrm{H}^1_{\mathcal{F}_{\alpha^{-1}}}(K, T(\alpha^{-1}))\big)$$

for $m \gg 0$, where $L_p = \prod_{v|p} \#\widetilde{E}(\mathbb{F}_v)$ with $\mathbb{F}_v$ the residue field of K at v.

Proof. By the action of complex conjugation, the nonvanishing of $\kappa^{\mathrm{Heeg}}_{1,\Lambda}(\alpha)$ implies that of $\kappa^{\mathrm{Heeg}}_{1,\Lambda}(\alpha^{-1})$, so the first claim follows from (3.4) and [How04, Thm. 1.6.1].

For $X \in \{T(\alpha), T(\alpha)^*\}$, the exact triangle (3.6) gives rise to the exact sequence

$$0 \to \bigoplus_{v|p} \mathrm{H}^0(K_v, X/X_v^+) \to \widetilde{\mathrm{H}}^1_f(K, X) \to \mathrm{Sel}_{\mathrm{Gr}}(K, X) \to 0,$$

where, similarly as in (3.7), $\mathrm{Sel}_{\mathrm{Gr}}(K,X)$ is the *strict Greenberg Selmer group* defined by

$$\mathrm{Sel}_{\mathrm{Gr}}(K,X) := \ker\left\{ \mathrm{H}^1(\mathcal{O}_{K,S},X) \to \bigoplus_{v\mid p} \frac{\mathrm{H}^1(K_v,X)}{\mathrm{H}^1(K_v,X_v^+)} \oplus \bigoplus_{v\mid N} \frac{\mathrm{H}^1(K_v,X)}{\mathrm{H}^1_{\mathrm{ur}}(K_v,X)} \right\}.$$

In particular, since $\mathrm{H}^0(K_v, A(\alpha)/A_v^+(\alpha))$ is finite for all $v \mid p$, it follows that

$$\widetilde{\mathrm{H}}^1_f(K,T(\alpha)) = \mathrm{Sel}_{\mathrm{Gr}}(K,T(\alpha)), \tag{3.10}$$

and together with the duality $\widetilde{\mathrm{H}}^2_f(K,T(\alpha)) \cong \widetilde{\mathrm{H}}^1_f(K,T(\alpha)^*)^\vee$ from [Nek06, Prop. 9.7.2(i)], that $\widetilde{\mathrm{H}}^2_f(K,T(\alpha))$ fits into the short exact sequence

$$0 \to \mathrm{Sel}_{\mathrm{Gr}}(K,T(\alpha)^*)^\vee \to \widetilde{\mathrm{H}}^2_f(K,T(\alpha)) \to \bigoplus_{v\mid p} \mathrm{H}^0(K_v, A(\alpha^{-1})/A_v^+(\alpha^{-1}))^\vee \to 0, \tag{3.11}$$

where we used that $T(\alpha)^* \cong A(\alpha^{-1})$ in writing the last term. Putting

$$A_v^-(\alpha^{-1}) := A(\alpha^{-1})/A_v^+(\alpha^{-1})$$

for the ease of notation, from (3.10) and (3.11) we thus obtain a canonical isomorphism

$$\begin{aligned} &\det_{\mathbb{Z}_p}^{-1}\widetilde{\mathbf{R}\Gamma}_f(K,T(\alpha)) \\ &\quad\cong \left(\prod_{v\mid p} \#\mathrm{H}^0(K_v, A_v^-(\alpha^{-1}))\right) \cdot \det_{\mathbb{Z}_p}(\mathrm{Sel}_{\mathrm{Gr}}(K,T(\alpha))) \otimes_{\mathbb{Z}_p} \det_{\mathbb{Z}_p}^{-1}(\mathrm{Sel}_{\mathrm{Gr}}(K,T(\alpha)^*)^\vee). \end{aligned} \tag{3.12}$$

On the other hand, from Poitou–Tate duality we have the exact sequence

$$\begin{aligned} 0 \to \mathrm{Sel}_{\mathrm{Gr}}(K,T(\alpha)) \to \mathrm{H}^1_{\mathcal{F}_\alpha}(K,T(\alpha)) \to \bigoplus_{v\mid p} \frac{\mathrm{H}^1_{\mathcal{F}_\alpha}(K_v,T(\alpha))}{\mathrm{H}^1(K_v,T_v^+(\alpha))} \oplus \bigoplus_{v\mid N} \frac{\mathrm{H}^1_{\mathcal{F}_\alpha}(K_v,T(\alpha))}{\mathrm{H}^1_{\mathrm{ur}}(K_v,T(\alpha))} \\ \to \mathrm{Sel}_{\mathrm{Gr}}(K,T(\alpha)^*)^\vee \to \mathrm{H}^1_{\mathcal{F}^*_\alpha}(K,T(\alpha)^*)^\vee \to 0. \end{aligned} \tag{3.13}$$

For $v \mid N$, we have $\mathrm{H}^1_{\mathrm{ur}}(K_v,T(\alpha)) \subset \mathrm{H}^1_{\mathcal{F}_\alpha}(K_v,T(\alpha))$ and by definition (see [BF96, (1.38)], for example)

$$\mathrm{Tam}(T(\alpha)^*/K_v)\cdot\mathbb{Z}_p = \#\left(\frac{\mathrm{H}^1_{\mathcal{F}_\alpha}(K_v,T(\alpha))}{\mathrm{H}^1_{\mathrm{ur}}(K_v,T(\alpha))}\right)\cdot\mathbb{Z}_p. \tag{3.14}$$

Taking determinants in the exact sequence (3.13), and using (3.14) and the short exact sequence

$$0 \to Ш_{\mathrm{BK}}(T(\alpha)^*/K)^\vee \to \mathrm{H}^1_{\mathcal{F}^*_\alpha}(K,T(\alpha)^*)^\vee \to \left(\mathrm{H}^1_{\mathcal{F}^*_\alpha}(K,T(\alpha)^*)_{\mathrm{div}}\right)^\vee \to 0,$$

we obtain a canonical isomorphism

$$\begin{aligned} &\det_{\mathbb{Z}_p}(\mathrm{Sel}_{\mathrm{Gr}}(K,T(\alpha))) \otimes_{\mathbb{Z}_p} \det_{\mathbb{Z}_p}^{-1}(\mathrm{Sel}_{\mathrm{Gr}}(K,T(\alpha)^*)^\vee) \\ &\qquad\cong \#Ш_{\mathrm{BK}}(T(\alpha)^*/K)\cdot\left(\prod_{v\mid N}\mathrm{Tam}(T(\alpha)^*/K_v)\right)\cdot\left(\prod_{v\mid p}\#\left(\frac{\mathrm{H}^1_{\mathcal{F}_\alpha}(K_v,T(\alpha))}{\mathrm{H}^1(K_v,T_v^+(\alpha))}\right)\right)\cdot\mathbb{Z}_p \\ &\qquad\otimes_{\mathbb{Z}_p} \det_{\mathbb{Z}_p}(\mathrm{H}^1_{\mathcal{F}_\alpha}(K,T(\alpha))) \otimes_{\mathbb{Z}_p} \det_{\mathbb{Z}_p}^{-1}((\mathrm{H}^1_{\mathcal{F}^*_\alpha}(K,T(\alpha)^*)_{\mathrm{div}})^\vee). \end{aligned} \tag{3.15}$$

Noting that $(\mathrm{H}^1_{\mathcal{F}^*_\alpha}(K,T(\alpha)^*)_{\mathrm{div}})^\vee \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{H}^1_{\mathcal{F}_{\alpha^{-1}}}(K,T(\alpha^{-1})),\mathbb{Z}_p)$, combining (3.12) and (3.15) this shows the existence of a canonical isomorphism ϑ as in the statement, and using that

$$\left(\prod_{v\mid N}\mathrm{Tam}(T(\alpha)^*/K_v)\right)\cdot\mathbb{Z}_p = (\mathrm{Tam}_E)^2\cdot\mathbb{Z}_p$$

for $m \gg 0$ (see [BCGS26, Rem. 1.2.9]) and Lemma 3.3.3 below, the result follows. □

The next result is a twisted analogue of [Gre99, Prop. 2.5].

Lemma 3.3.3. *Suppose $\alpha : \Gamma^{\mathrm{ac}} \to \mathbb{Z}_p^\times$ satisfies $\alpha \equiv 1 \pmod{p^m}$ for some $m \gg 0$. Then for every prime v of K above p we have*

$$\#\mathrm{H}^0(K_v, A_v^-(\alpha^{\pm 1})) \cdot \mathbb{Z}_p = \#\left(\frac{\mathrm{H}^1_{\mathcal{F}_\alpha}(K_v, T(\alpha^{\pm 1}))}{\mathrm{H}^1(K_v, T_v^+(\alpha^{\pm 1}))}\right) \cdot \mathbb{Z}_p = \#\widetilde{E}(\mathbb{F}_v) \cdot \mathbb{Z}_p$$

for $m \gg 0$.

Proof. Let v be a prime of K above p. Since $\mathrm{H}^1_{\mathcal{F}_\alpha}(K_v, A(\alpha))$ is the image of $\mathrm{H}^1_{\mathcal{F}_\alpha}(K_v, V(\alpha))$ in (3.5) under the natural map induced by $V(\alpha) \twoheadrightarrow A(\alpha)$, we see that

$$\mathrm{H}^1_{\mathcal{F}_\alpha}(K_v, A(\alpha)) = \mathrm{H}^1(K_v, A_v^+(\alpha))_{\mathrm{div}}. \tag{3.16}$$

From the short exact sequence $0 \to T_v^+(\alpha) \to V_v^+(\alpha) \to A_v^+(\alpha) \to 0$ we obtain

$$\frac{\mathrm{H}^1(K_v, A_v^+(\alpha))}{\mathrm{H}^1(K_v, A_v^+(\alpha))_{\mathrm{div}}} \cong \mathrm{H}^2(K_v, T_v^+(\alpha)),$$

which together with (3.16) and local Tate duality amounts to

$$\frac{\mathrm{H}^1_{\mathcal{F}_\alpha}(K_v, T(\alpha^{-1}))}{\mathrm{H}^1(K_v, T_v^+(\alpha^{-1}))} \cong \mathrm{H}^0(K_v, A_v^-(\alpha^{-1})),$$

whence the first equality in the statement. The second equality is immediate from the fact that $A(\alpha^{\pm 1})[p^m] \cong A[p^m]$ as G_K-modules, and so $\mathrm{H}^0(K_v, A_v^-(\alpha^{\pm 1})) \cong \mathrm{H}^0(K_v, A_v^-) \cong \widetilde{E}(\mathbb{F}_v)[p^\infty]$. □

Thus we arrive at the following result.

Corollary 3.3.4. *Suppose $\alpha : \Gamma^{\mathrm{ac}} \to \mathbb{Z}_p^\times$ is such that $\alpha \equiv 1 \pmod{p^m}$ for some $m \geq 1$ and $\kappa_{1,\Lambda}^{\mathrm{Heeg}}(\alpha) \neq 0$. If Conjecture 3.2.2 holds, then up to a p-adic unit:*

$$\#\big(\mathrm{H}^1_{\mathcal{F}_\alpha}(K, T(\alpha))/\mathbb{Z}_p \cdot \kappa_{1,\Lambda}^{\mathrm{Heeg}}(\alpha)\big)^2 = \left(\prod_{v|p} \#\widetilde{E}(\mathbb{F}_v)\right)^2 \cdot \big(\mathrm{Tam}_E\big)^2 \cdot \#Ш_{\mathrm{BK}}(T(\alpha)^*/K)$$

for $m \gg 0$.

Proof. Assume Conjecture 3.2.2, let $\widetilde{\mathfrak{z}}_{K_\infty}$ be the Λ^{ac}-basis of $\det^{-1}_{\Lambda^{\mathrm{ac}}} \widetilde{\mathbf{R}\Gamma}_f(\mathbf{T})$ corresponding to $y_\infty \otimes y_\infty$ under the isomorphism (3.8), and let $\widetilde{\mathfrak{z}}_{K_\infty}(\alpha)$ denote its image under the surjection

$$\det^{-1}_{\Lambda^{\mathrm{ac}}} \widetilde{\mathbf{R}\Gamma}_f(\mathbf{T}) \twoheadrightarrow \det^{-1}_{\mathbb{Z}_p} \widetilde{\mathbf{R}\Gamma}_f(T(\alpha))$$

induced by the 'perfect control' isomorphism

$$\widetilde{\mathbf{R}\Gamma}_f(\mathbf{T}) \otimes^{\mathbf{L}}_{\Lambda^{\mathrm{ac}},\alpha} \mathbb{Z}_p \cong \widetilde{\mathbf{R}\Gamma}_f(T(\alpha)) \tag{3.17}$$

of [Nek06, Prop. 8.10.1]. Then $\widetilde{\mathfrak{z}}_{K_\infty}(\alpha)$ is a $\mathbb{Z}_p$-basis of $\det^{-1}_{\mathbb{Z}_p} \widetilde{\mathbf{R}\Gamma}_f(T(\alpha))$ and its image under the isomorphism ϑ of Proposition 3.3.2 is given by $\kappa_{1,\Lambda}^{\mathrm{Heeg}}(\alpha) \otimes \kappa_{1,\Lambda}^{\mathrm{Heeg}}(\alpha^{-1})$ up to a p-adic unit. Noting that

$$\#\big(\mathrm{H}^1_{\mathcal{F}_\alpha}(K, T(\alpha))/\mathbb{Z}_p \cdot \kappa_{1,\Lambda}^{\mathrm{Heeg}}(\alpha)\big) = \#\big(\mathrm{H}^1_{\mathcal{F}_{\alpha^{-1}}}(K, T(\alpha^{-1}))/\mathbb{Z}_p \cdot \kappa_{1,\Lambda}^{\mathrm{Heeg}}(\alpha^{-1})\big)$$

by the action of complex conjugation, the result thus follows from Proposition 3.3.2. □

Remark 3.3.5. For p split in K, Corollary 3.3.4 was proved in [BCGS26, Cor. 1.2.11] based on a study of the p-adic L-function of [BDP13]. It is unclear whether the method in [BCGS26] can be extended to the nonsplit case.

3.4. **Proof of Theorem C.** With the results in the preceding sections in hand, the proof now follows similarly as in the case of Theorem A, so we shall be rather brief.

Choose a non-trivial $\alpha : \Gamma^{\mathrm{ac}} \to \mathbb{Z}_p^\times$ with $\alpha \equiv 1 \pmod{p^m}$ for some $m \geq 1$, and assume m is large enough so that $\kappa_{1,\Lambda}^{\mathrm{Heeg}}(\alpha) \neq 0$ (as is possible by the nonvanishing results of Cornut–Vatsal [Cor02, Vat03]).

If the anticyclotomic Iwasawa Main Conjecture 3.2.2 holds, then Theorem 3.1.2 and Corollary 3.3.4 give

$$\mathscr{M}_\infty(\boldsymbol{\kappa}_\Lambda^{\mathrm{Heeg}}(\alpha)) = \sum_{v|p} \mathrm{ord}_p(\#\widetilde{E}(\mathbb{F}_v)) + \mathrm{ord}_p(\mathrm{Tam}_E). \tag{3.18}$$

With notations as in Lemma 3.1.1, we note that

$$\left(\prod_{v|p} \#\widetilde{E}(\mathbb{F}_v)\right) \cdot \mathbb{Z}_p = \begin{cases} (\alpha_p - 1)^2(\beta_p - 1)^2 \cdot \mathbb{Z}_p & \text{if } p \text{ splits in } K, \\ ((p+1)^2 - a_p^2) \cdot \mathbb{Z}_p & \text{if } p \text{ is inert in } K. \end{cases}$$

Thus from [BCGS26, Prop. 2.2.1] (the analogue of Proposition 2.1.5 in the present setting), Lemma 3.1.1, and (3.18) we arrive at

$$\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Heeg}}) = \mathrm{ord}_p(\mathrm{Tam}_E),$$

concluding the proof of the implication (ii) ⇒ (i) in Theorem C. The proof of (i) ⇒ (ii) follows similarly as in the case of Theorem A, combining:

(1) the divisibility $\Lambda^{\mathrm{ac}} \cdot \widetilde{\mathfrak{z}}_{K_\infty} \subset \det_{\Lambda^{\mathrm{ac}}}^{-1} \widetilde{\mathbf{R}\Gamma}_f(\mathbf{T})$ (see Remark 3.2.4) deduced from [How04, Thm. 2.2.10] and the nonvanishing of $\kappa_{1,\Lambda}^{\mathrm{Heeg}}$;

(2) the equality $\mathbb{Z}_p \cdot \widetilde{\mathfrak{z}}_{K_\infty}(\alpha) = \det_{\mathbb{Z}_p}^{-1} \widetilde{\mathbf{R}\Gamma}_f(T(\alpha))$ coming from the assumption $\mathscr{M}_\infty(\boldsymbol{\kappa}^{\mathrm{Heeg}}) = \mathrm{ord}_p(\mathrm{Tam}_E)$ in (i) and the calculations in §3.3,

and invoking [SU14, Lem. 3.2] to conclude.

References

[BCGS26] Ashay Burunagle, Francesc Castella, Giada Grossi, and Christopher Skinner. Non-vanishing of Kolyvagin systems and Iwasawa theory. *Cambridge J. Math., to appear*, 2026.

[BCS25] Ashay Burungale, Francesc Castella, and Christopher Skinner. Base change and Iwasawa main conjectures for GL_2. *Int. Math. Res. Not. IMRN*, (8):Paper No. rnaf082, 15, 2025.

[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.

[BF96] D. Burns and M. Flach. Motivic L-functions and Galois module structures. *Math. Ann.*, 305(1):65–102, 1996.

[BKS24] David Burns, Masato Kurihara, and Takamichi Sano. On derivatives of Kato's Euler system for elliptic curves. *J. Math. Soc. Japan*, 76(3):855–919, 2024.

[BS21] David Burns and Takamichi Sano. On the theory of higher rank Euler, Kolyvagin and Stark systems. *Int. Math. Res. Not. IMRN*, (13):10118–10206, 2021.

[BSTW24] Ashay Burunagle, Christopher Skinner, Ye Tian, and Xin Wan. Zeta elements for elliptic curves and applications. 2024. preprint, arXiv:2409.01350.

[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.

[CGS25] Francesc Castella, Giada Grossi, and Christopher Skinner. Mazur's main conjecture at Eisenstein primes. *Math. Ann.*, 393(2):2451–2506, 2025.

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

[CLW22] Francesc Castella, Zheng Liu, and Xin Wan. Iwasawa-Greenberg main conjecture for nonordinary modular forms and Eisenstein congruences on GU(3,1). *Forum Math. Sigma*, 10:Paper No. e110, 90, 2022.

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

[FK06] Takako Fukaya and Kazuya Kato. A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory. In *Proceedings of the St. Petersburg Mathematical Society. Vol. XII*, volume 219 of *Amer. Math. Soc. Transl. Ser. 2*, pages 1–85. Amer. Math. Soc., Providence, RI, 2006.

[Fla90] Matthias Flach. A generalisation of the Cassels-Tate pairing. *J. Reine Angew. Math.*, 412:113–127, 1990.

[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.

[Gro91] Benedict H. Gross. Kolyvagin's work on modular elliptic curves. In *L-functions and arithmetic (Durham, 1989)*, volume 153 of *London Math. Soc. Lecture Note Ser.*, pages 235–256. Cambridge Univ. Press, Cambridge, 1991.

[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.

[How04] Benjamin Howard. The Heegner point Kolyvagin system. *Compos. Math.*, 140(6):1439–1472, 2004.

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

[Kat93] Kazuya Kato. Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}. I. In *Arithmetic algebraic geometry (Trento, 1991)*, volume 1553 of *Lecture Notes in Math.*, pages 50–163. Springer, Berlin, 1993.
[Kat04] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.
[Kat21] Takenori Kataoka. Equivariant Iwasawa theory for elliptic curves. *Math. Z.*, 298(3-4):1653–1725, 2021.
[Kim26] Chan-Ho Kim. The structure of Selmer groups and the Iwasawa main conjecture for elliptic curves. *Amer. J. Math., to appear*, 2026.
[KKS20] Chan-Ho Kim, Myoungil Kim, and Hae-Sang Sun. On the indivisibility of derived Kato's Euler systems and the main conjecture for modular forms. *Selecta Math. (N.S.)*, 26(2):Paper No. 31, 47, 2020.
[Kob03] Shin-ichi Kobayashi. Iwasawa theory for elliptic curves at supersingular primes. *Invent. Math.*, 152(1):1–36, 2003.
[Kol91a] V. A. Kolyvagin. On the structure of Shafarevich-Tate groups. In *Algebraic geometry (Chicago, IL, 1989)*, volume 1479 of *Lecture Notes in Math.*, pages 94–121. Springer, Berlin, 1991.
[Kol91b] Victor A. Kolyvagin. On the structure of Selmer groups. *Math. Ann.*, 291(2):253–259, 1991.
[KS24] Takenori Kataoka and Takamichi Sano. On Euler systems for motives and Heegner points. *J. Assoc. Math. Res.*, 2(2):154–208, 2024.
[KS26] Masato Kurihara and Ryotaro Sakamoto. Euler and Kolyvagin systems of rank 0 and the structure of Selmer groups. *preprint*, 2026.
[Kur14a] Masato Kurihara. Refined Iwasawa theory for p-adic representations and the structure of Selmer groups. *Münster J. Math.*, 7(1):149–223, 2014.
[Kur14b] Masato Kurihara. The structure of Selmer groups of elliptic curves and modular symbols. In *Iwasawa theory 2012*, volume 7 of *Contrib. Math. Comput. Sci.*, pages 317–356. Springer, Heidelberg, 2014.
[Kur24] Masato Kurihara. Some analytic quantities yielding arithmetic information about elliptic curves. In *Arithmetic geometry*, volume 41 of *Tata Inst. Fundam. Res. Stud. Math.*, pages 345–384. Tata Inst. Fund. Res., Mumbai, [2024] ©2024.
[Maz72] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.
[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.
[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.
[MT87] B. Mazur and J. Tate. Refined conjectures of the "Birch and Swinnerton-Dyer type". *Duke Math. J.*, 54(2):711–750, 1987.
[Nek06] Jan Nekovář. Selmer complexes. *Astérisque*, (310):viii+559, 2006.
[PR87] Bernadette Perrin-Riou. Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner. *Bull. Soc. Math. France*, 115(4):399–456, 1987.
[Roh84] David E. Rohrlich. On L-functions of elliptic curves and anticyclotomic towers. *Invent. Math.*, 75(3):383–408, 1984.
[Sak22] Ryotaro Sakamoto. p-Selmer group and modular symbols. *Doc. Math.*, 27:1891–1922, 2022.
[San23] Takamichi Sano. Derived Bockstein regulators and anticyclotomic p-adic Birch and Swinnerton-Dyer conjectures. 2023. preprint, arXiv:2308.08875.
[Ste89] Glenn Stevens. Stickelberger elements and modular parametrizations of elliptic curves. *Invent. Math.*, 98(1):75–106, 1989.
[SU14] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.
[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.
[Zan19] Murilo Zanarella. On Howard's main conjecture and the Heegner point Kolyvagin system. 2019. preprint, arXiv:1908.09197.
[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.

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

(T. Sano) Osaka Metropolitan University, Department of Mathematics, 3-3-138 Sugimoto, Sumiyoshi-ku, Osaka, 558-8585, Japan
Email address: tsano@omu.ac.jp