# MAZUR'S MAIN CONJECTURE AT EISENSTEIN PRIMES

FRANCESC CASTELLA, GIADA GROSSI, AND CHRISTOPHER SKINNER

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve and let $p$ be an odd prime of good reduction for $E$. Assume that $E$ admits a rational $p$-isogeny $\varphi : E \to E'$, and let $\phi : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ be the character by which $G_{\mathbb{Q}}$ acts on $\ker(\varphi)$. In this paper, we prove the Iwasawa main conjecture for $E$, as formulated by B. Mazur in 1972, when $\phi|_{G_p} \neq 1, \omega$, where $G_p \subset G_{\mathbb{Q}}$ is a decomposition group at $p$ and $\omega$ is the Teichmüller character.

Two key innovations in our proof are a Kolyvagin system argument for the Selmer group of $E$ twisted by anticyclotomic Hecke characters arbitrarily close to the trivial character, and a congruence argument exploiting Beilinson–Flach classes and their explicit reciprocity laws.

## CONTENTS



*Date*: September 15, 2023.

## 1. Introduction

Let $E$ be an elliptic curve over $\mathbb{Q}$, and let $p$ be an odd prime of good reduction for $E$. In the early 1970s, motivated by Iwasawa's theory for the $p$-part of class groups of number fields in $\mathbb{Z}_p$-extensions, Mazur initiated a parallel study for the arithmetic of $E$ over the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$. In particular, in [Maz72] he proved a foundational "control theorem" for the $p$-primary Selmer group $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$, viewed as a module over the Iwasawa algebra $\Lambda_{\mathbb{Q}} = \mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]\!]$, and formulated an analogue of Iwasawa's main conjecture, expressing the characteristic ideal of the Pontryagin dual of $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty) = \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\vee$ in terms of the $p$-adic $L$-function attached to $E$ by the work Mazur–Swinnerton-Dyer [MSD74]:

$$\mathrm{ch}_{\Lambda_{\mathbb{Q}}}\big(\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)\big) = \big(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})\big) \tag{MC}$$

(see [*op. cit.*, Conj. 3]). By the Weierstrass preparation theorem, conjecture (MC) can be viewed as the equality between two integral $p$-adic polynomials attached to $E$, one by means of the arithmetic of $E$ (i.e., its Mordell–Weil and Tate–Shafarevich groups) over $\mathbb{Q}_\infty$ and the other by means of the modular symbols associated with $E$ (available thanks to its modularity [Wil95, TW95, BCDT01]), encoding the special values of the Hasse–Weil $L$-function of $E$ twisted by finite order characters of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$.

The main result in this paper is the proof (under a mild hypothesis) of Mazur's main conjecture (MC) when $p$ is an *Eisenstein prime* for $E$, meaning that $E$ admits a rational $p$-isogeny. In other words, we consider the case where $E[p]$ is *reducible* as a module over the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so that

$$E[p]^{ss} = \mathbb{F}(\phi) \oplus \mathbb{F}(\psi)$$

as $G_{\mathbb{Q}}$-modules, where $\phi, \psi : G_{\mathbb{Q}} \to \mathbb{F}^\times$ are characters whose product $\phi\psi = \omega$ is the mod $p$ cyclotomic character. (In the non-Eisenstein case, conjecture (MC) was proved under mild hypotheses in [Kat04, SU14, Wan15].)

**Theorem A.** *Let $E/\mathbb{Q}$ be an elliptic curve, and let $p > 2$ be a prime of good reduction for $E$. Suppose that $p$ is Eisenstein with $\phi|_{G_p} \neq 1, \omega$, where $G_p \subset G_{\mathbb{Q}}$ is a decomposition group at $p$. Then $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)$ is $\Lambda_{\mathbb{Q}}$-torsion with*

$$\mathrm{ch}_{\Lambda_{\mathbb{Q}}}\big(\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)\big) = \big(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})\big),$$

*and hence Mazur's main conjecture holds.*

In the setting of Theorem A, Kato proved [Kat04] that $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)$ is $\Lambda_{\mathbb{Q}}$-torsion and that its characteristic ideal contains $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$ after inverting $p$. This ambiguity of powers of $p$ was subsequently removed by Wüthrich [Wut14]. On the other hand, in a foundational paper [GV00], Greenberg–Vatsal proved conjecture (MC) for Eisenstein primes $p$ under the assumption that

$$\phi \text{ is either } \begin{cases} \text{unramified at } p \text{ and odd, or} \\ \text{ramified at } p \text{ and even.} \end{cases} \tag{GV}$$

Under this hypothesis, they could show that both $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)$ and $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$ have vanishing $\mu$-invariant by building on the work of Ferrero–Washington [FW79] and Mazur–Wiles [MW84], thereby reducing their result on (MC) to a delicate comparison of Iwasawa $\lambda$-invariants.

Without hypothesis (GV), the situation is known to be more complicated. Indeed, Greenberg showed that if $E[p^\infty]$ contains a $G_{\mathbb{Q}}$-invariant cyclic subgroup $\Phi$ of order $p^m$ which is ramified at $p$ and odd, then $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)$ has $\mu$-invariant $\geq m$ (see [Gre99, Prop. 5.7]). On the analytic side, a conjecture by Stevens [Ste89] predicts a similar phenomenon for $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$. The methods in this paper allow us to prove Mazur's main conjecture (MC) for Eisenstein primes regardless of the value of the $\mu$-invariant. In particular, our results include giving a new proof for the case previously handled by Greenberg–Vatsal.

### 1.1. Some ideas from the proof.

Our proof of Theorem A goes through *anticyclotomic* Iwasawa theory for $E$ over an auxiliary imaginary quadratic field $K/\mathbb{Q}$ in which $p$ splits. Roughly speaking, this is used to show that $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)$ and $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$ have the same Iwasawa invariants[1]:

$$\mu(\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)) = \mu(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})) \quad \text{and} \quad \lambda(\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)) = \lambda(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})),$$

even in situations of positive $\mu$-invariant.

[1] Strictly speaking, our results only show these equalities for *the sum* of the Iwasawa invariants of $E$ and the quadratic twist $E^K$, but this suffices for the proof of Theorem A thanks to Kato's work.

More precisely, our argument rests on the proof of an Iwasawa main conjecture for $E$ over the anticyclotomic $\mathbb{Z}_p$-extension of $K$ (see Theorem C below), and a congruence argument building on the cyclotomic Euler system of Beilinson–Flach classes of Lei–Loeffler–Zerbes [LLZ14] and Kings–Loeffler–Zerbes [KLZ17].

*Anticyclotomic main conjectures.* Denote by $N$ the conductor of $E$, and let $K$ be an imaginary quadratic field such that

(disc) $$\text{the discriminant } D_K \text{ is odd and } D_K \neq -3,$$

and such that the following *Heegner hypothesis* holds:

(Heeg) $$\text{every prime } \ell | N \text{ splits in } K.$$

Let $\Gamma_K^- = \mathrm{Gal}(K_\infty^-/K)$ be the Galois group of the anticyclotomic $\mathbb{Z}_p$-extension of $K$, and for each $n$ denote by $K_n^-$ the subfield of $K_\infty^-$ with $[K_n^- : K] = p^n$. In sharp contrast with the case of $\mathbb{Q}_\infty/\mathbb{Q}$, one can show that $\mathrm{rank}_{\mathbb{Z}} E(K_n^-)$ is unbounded as $n \to \infty$, and therefore the Pontryagin dual $\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^-)$ of the Selmer group $\mathrm{Sel}_{p^\infty}(E/K_\infty^-)$ has positive rank as a module over the anticyclotomic Iwasawa algebra $\Lambda_K^- = \mathbb{Z}_p[\![\Gamma_K^-]\!]$. This unbounded growth is accounted for by the existence of Heegner points on $E$ associated with a given modular parametrization

$$\pi : X_0(N) \to E.$$

This system of points gives rise to a $\Lambda_K^-$-adic class $\kappa_1^{\mathrm{Hg}}$ which was shown to be non-torsion by Cornut [Cor02] and Vatsal [Vat03] in their proof of "Mazur's conjecture" on higher Heegner points [Maz84]. As recalled below, a formulation of the Iwasawa main conjecture in this context was given by Perrin-Riou [PR87a]. Write

$$\mathfrak{S}_{\mathrm{ord}}(E/K_\infty^-) := \varprojlim_n \varprojlim_m \mathrm{Sel}_{p^m}(E/K_n^-),$$

which is a compact $\Lambda_K^-$-module containing $\kappa_1^{\mathrm{Hg}}$.

**Conjecture B** (Perrin-Riou)**.** *Let $E/\mathbb{Q}$ be an elliptic curve, $p > 2$ a prime of good ordinary reduction for $E$, and let $K$ be an imaginary quadratic field satisfying* (Heeg) *and* (disc)*. Then $\mathfrak{S}_{\mathrm{ord}}(E/K_\infty^-)$ and $\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^-)$ both have $\Lambda_K^-$-rank one, and*

$$\mathrm{char}_{\Lambda_K^-}\big(\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^-)_{\mathrm{tors}}\big) = \mathrm{char}_{\Lambda_K^-}\big(\mathfrak{S}_{\mathrm{ord}}(E/K_\infty^-)/(\kappa_1^{\mathrm{Hg}})\big)^2,$$

*where the subscript* tors *denotes the $\Lambda_K^-$-torsion submodule.*

The first general result towards Conjecture B for Eisenstein primes $p$ was obtained in [CGLS22]. Namely, it was shown that Perrin-Riou's main conjecture holds for Eisenstein primes $p$ under the additional hypotheses that

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

that $\phi|_{G_p} \neq 1, \omega$, and that

(Sel) $$\text{the } \mathbb{Z}_p\text{-corank of } \mathrm{Sel}_{p^\infty}(E/K) \text{ is } 1.$$

In particular, hypothesis (Sel), which obviously excludes elliptic curves with $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \geq 2$, was imposed to account for the inability of the methods in [*op. cit.*, §3] to control certain error terms appearing at height one primes of $\Lambda_K^-$ approaching the augmentation ideal $\mathfrak{P}_0 \subset \Lambda_K^-$.

A key technical innovation in this paper is the proof of a Kolyvagin system argument for the Selmer group of $E/K$ twisted by characters of $\Gamma_K^-$ arbitrarily close to 1 yielding the "upper bound" divisibility in Conjecture B after localization at height one primes of $\Lambda_K^-$ approaching $\mathfrak{P}_0$. Together with complementary results obtained in [CGLS22], this argument yields the following.

**Theorem C.** *Let $E/\mathbb{Q}$ be an elliptic curve, let $p \nmid 2N$ be an Eisenstein prime for $E$, and let $K$ be an imaginary quadratic field satisfying* (Heeg)*,* (disc)*, and* (spl)*. Suppose that $\phi|_{G_p} \neq 1, \omega$. Then Conjecture B holds.*

To go from Theorem C to Theorem A, we use a reformulation of the former in terms of $p$-adic $L$-functions. Let $\mathbb{Z}_p^{\mathrm{ur}}$ be the completion of the ring of integers of the maximal unramified extension of $\mathbb{Q}_p$, and put

$$\Lambda_K^{-,\mathrm{ur}} := \Lambda_K^- \widehat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p^{\mathrm{ur}}.$$

It follows from the explicit reciprocity law for $\kappa_1^{\mathrm{Hg}}$, that Conjecture B is equivalent to the Iwasawa–Greenberg main conjecture for the $p$-adic $L$-function $\mathcal{L}_p^{\mathrm{BDP}}(f/K)$ introduced in [BDP13]. Under the same hypotheses of Theorem C, we thus deduce that a different Greenberg Selmer group denoted $\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty^-)$ is $\Lambda_K^-$-torsion, with

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

as ideals in $\Lambda_K^{-,\mathrm{ur}}$. This equality of characterisitc ideals is the first key ingredient in the proof of Theorem A.

*Comparing Iwasawa invariants.* In [LLZ14] and [KLZ17], Lei–Loeffler–Zerbes and Kings–Loeffler–Zerbes constructed a cyclotomic Euler system (over $\mathbb{Q}$) for the Rankin–Selberg convolution of two modular forms moving in Hida families. To be able to use these classes as a bridge between the anticyclotomic $\mathbb{Z}_p$-extension $K_\infty^-/K$ and the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$ (or rather its translate by $K$), here we are led to consider a variant of their construction attached to the pair $(f,\boldsymbol{g})$, where $f$ is the weight 2 newform attached to $E$, and $\boldsymbol{g}$ is a suitable CM Hida family. Because our $\boldsymbol{g}$ specializes in weight 1 to the $p$-irregular Eisenstein series $\mathrm{Eis}_{1,\eta}$, where $\eta=\eta_{K/\mathbb{Q}}$ is the quadratic character associated to $K/\mathbb{Q}$, in fact we use a refinement of the construction in [KLZ17] studied in [BST21].

Let $\Lambda_K$ (resp. $\Lambda_K^+$) be the Iwasawa algebra for the $\mathbb{Z}_p^2$-extension of $K$ (resp. the cyclotomic $\mathbb{Z}_p$-extension $K_\infty^+/K$). In particular, from these works we obtain a two-variable Iwasawa cohomology class

$$BF \in \mathrm{H}^1_{\mathrm{Iw}}(K_\infty, T_pE_\bullet),$$

where $E_\bullet/\mathbb{Q}$ is the distinguished elliptic curve in the isogeny class of $E$ constructed by Wüthrich [Wut14]. Combined with the relations between different $p$-adic $L$-functions established in Sect. 2, we also deduce two explicit reciprocity laws:

(1) One relating $\mathrm{loc}_{\bar v}(BF)$ to a $p$-adic $L$-function $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)\in\Lambda_K$ whose image $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+$ under the natural projection $\Lambda_K\to\Lambda_K^+$ satisfies
$$\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+ = \mathcal{L}_p^{\mathrm{MSD}}(E_\bullet/\mathbb{Q})\cdot\mathcal{L}_p^{\mathrm{MSD}}(E_\bullet^K/\mathbb{Q})$$
up to a unit, where $E_\bullet^K$ is the twist of $E_\bullet$ by the quadratic field $K$.

(2) Another relating $\mathrm{loc}_v(BF)$ to a $p$-adic $L$-function $\mathcal{L}_p^{\mathrm{Gr}}(f/K)\in\Lambda_K^{\mathrm{ur}}=\Lambda_K\widehat{\otimes}\mathbb{Z}_p^{\mathrm{ur}}$ whose image $\mathcal{L}_p^{\mathrm{Gr}}(f/K)^-$ under the natural projection $\Lambda_K^{\mathrm{ur}}\to\Lambda_K^{-,\mathrm{ur}}$ satisfies
$$\mathcal{L}_p^{\mathrm{Gr}}(f/K)^- = \mathcal{L}_p^{\mathrm{BDP}}(f/K)$$
up to a unit.

The next key idea to have Theorem C to bring to bear on the proof of Theorem A is to consider the restriction of $BF$ to $\mathrm{H}^1_{\mathrm{Iw}}(K_\infty^+,T_pE_\bullet)$, and exploit the fact that the anticyclotomic and the cyclotomic $\mathbb{Z}_p$-extensions meet at the trivial character (in other words, $K_\infty^-\cap K_\infty^+=K$). When $\mathcal{L}_p^{\mathrm{BDP}}(f/K)(1)\neq 0$ (which by the main result of [BDP13] can only happen when $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q})\le 1$), the argument for the implication Theorem C⇒Theorem A is relatively simple, and to help orient the reader, this simpler case is explained in detail in Sect. 5.

To make the argument work in arbitrary rank, we take a character $\alpha$ of $\Gamma_K^-$ with

$$\alpha\equiv 1\ (\mathrm{mod}\, p^m)$$

for some $m\gg 0$ such that $\mathcal{L}_p^{\mathrm{BDP}}(f/K)(\alpha)\neq 0$ (as always possible by the nonvanishing of $\mathcal{L}_p^{\mathrm{BDP}}(f/K)$), and consider $\alpha$-twisted versions of the above Selmer groups and $p$-adic $L$-functions projected to $\Lambda_K^+$. With the aid of a cyclotomic Euler system extending the $\alpha$-twist of the class $BF$ projected to $\mathrm{H}^1_{\mathrm{Iw}}(K_\infty^+,T_pE_\bullet)$, building on Theorem C we deduce that the twisted Selmer group $\mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)$ is $\Lambda_K^+$-torsion, with

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)\big) = \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^+\big) \tag{1.1}$$

as ideals in $\Lambda_K^+$. On the other hand, Kato's divisibility [Kat04] (as refined by Wüthrich [Wut14]) applied to $E_\bullet$ and $E_\bullet^K$ implies that the untwisted Selmer group $\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)$ is $\Lambda_K^+$-torsion, with the divisibility

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)\big) \supset \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+\big) \tag{1.2}$$

as ideals in $\Lambda_K^+$. By a congruence argument using the study of the variation of both sides of (1.1) as $\alpha$ varies carried out in the earlier parts of the paper, we deduce from this equality (for $\alpha$ sufficiently close to 1) that $\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)$ and $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+$ have the same Iwasawa invariants, and so equality holds in (1.2). The proof

of Theorem A for both $E_\bullet$ and the original elliptic curve $E$, can then be deduced from Kato's work and the invariance of Mazur's main conjecture under isogenies.

1.2. **Application to the $p$-part of the Birch–Swinnerton Dyer formula.** As a standard consequence of Theorem A, we deduce most cases of the $p$-part of the Birch–Swinnerton Dyer formula for elliptic curves $E/\mathbb{Q}$ of analytic rank $\leq 1$ at Eisenstein primes $p$.

**Theorem D.** *Let $E/\mathbb{Q}$ and $p>2$ be as in Theorem A, and let $r\in\{0,1\}$. If $\mathrm{ord}_{s=1}L(E,s)=r$, then*

$$\mathrm{ord}_p\left(\frac{L^{(r)}(E,1)}{\mathrm{Reg}(E/\mathbb{Q})\cdot\Omega_E}\right)=\mathrm{ord}_p\left(\#Ш(E/\mathbb{Q})\prod_{\ell\nmid\infty}c_\ell(E/\mathbb{Q})\right),$$

*where*

- $\mathrm{Reg}(E/\mathbb{Q})$ *is the regulator of* $E(\mathbb{Q})$,
- $\Omega_E=\int_{E(\mathbb{R})}|\omega_E|$ *is the Néron period associated to the Néron differential* $\omega_E$, *and*
- $c_\ell(E/\mathbb{Q})$ *is the Tamagawa number of* $E$ *at the prime* $\ell$.

*In other words, the $p$-part of the Birch–Swinnerton-Dyer formula for $E$ holds.*

*Proof.* In the case $r=0$, the argument is the same as in [CGLS22, Thm. 5.1.4], replacing the appeal to [GV00, Thm. 1.3] by an appeal to our Theorem A. In the case $r=1$, we argue as in [CGLS22, Thm. 5.3.1], choosing a suitable $K$ with $L(E^K,1)\neq 0$ and applying our result in the rank 0 case to $E^K$. □

**Remark 1.2.1.** Previously, by the work of Greenberg–Vatsal [GV00] in analytic rank 0, and of the authors with Lee [CGLS22] in analytic rank 1, Theorem D was only known for roughly "half" of the $p$-Eisenstein cases, as both results required a certain parity hypothesis on $\phi$.

It is easy to produce examples of elliptic curves to which Theorem D can be applied. Let $p=5$ and $J$ be any of the three non-isomorphic elliptic curves of conductor 11; one could take for example the elliptic curve of Weierstrass equation

$$y^2+y=x^3-x^2-10x-20,$$

which is the strong Weil curve of conductor 11. It is known that $J[5]$ is reducible and its semi-simplification is isomorphic to $\mu_5\oplus\mathbb{Z}/5\mathbb{Z}$. Moreover, the rank of $J$ is equal to zero. We can then consider $\psi$ any quadratic character such that $\psi(5)=-1$ and take $E=J_\psi$ the quadratic twist of $J$ by $\psi$. Since the root number of $J$ is 1, applying [FH95, Thm. B.1], we can produce infinitely many $\psi$ such that $E=J_\psi$ has analytic (and hence algebraic) rank zero and for which the hypothesis of Theorem D are satisfied for $p=5$. Note that prior to this paper, the only elliptic curves in this family for which the theorem was known are of the form $E=J_\psi$ where $\psi$ is odd.

Similarly, take $p=5$ and consider the elliptic curve

$$J: y^2+y=x^3+x^2-10x+10.$$

The curve $J$ has conductor 123 and analytic rank 1, and satisfies $J[5]^{ss}=\mu_5\oplus\mathbb{Z}/5\mathbb{Z}$ as $G_\mathbb{Q}$-modules. Let $\psi$ any quadratic character such that $\psi(5)=-1$ and take $E=J_\psi$ the quadratic twist of $J$ by $\psi$. Since the root number of $J$ is $-1$ (being of analytic rank one), by [FH95, Thm. B.2] we can find infinitely many $\psi$ as above for which $E=J_\psi$ also has analytic rank one and hence to which Theorem D can be applied for $p=5$. Earlier result in this direction would only apply to the elliptic curve in this family of the form $E=J_\psi$ with $\psi$ even.

One can proceed similarly for $p=3,7,13,37$, taking quadratic twists of elliptic curves of rank zero or one and with a rational $p$-isogeny. If the character describing the kernel of the isogeny is not trivial (which has to be the case for $p=13$ or $p=37$), one might have to impose further conditions to the quadratic character at some bad primes in order to apply [FH95, Thm. B].

1.3. **Further applications and relation to previous works.** In addition to being a key ingredient in the proof of our main results, the Kolyvagin system argument with error terms for the $p$-adic Tate module of $E$ twisted by characters close to the trivial one contained in Sect. 6 (see Theorem 6.1.1) is used in a forthcoming work of the authors with A. Burungale [BCGS23] to establish Kolyvagin's conjecture on the nonvanishing of derived Heegner classes under mild hypotheses on $E[p]$, including the first cases for Eisenstein primes $p$ (many cases in the non-Eisenstein case were first proved by W. Zhang [Zha14]).

Finally, we note that the idea of using Beilinson–Flach classes to relate different Iwasawa main conjectures has appeared in earlier works, notably in [Wan21, CW22], but the congruence argument mechanism introduced

in this paper to deduce Theorem A from Theorem C is new, and should be useful in other settings, as we plan to exploit in forthcoming work.

1.4. **Outline of the paper.** We begin in Sect. 2 by introducing the different one- and two-variable $p$-adic $L$-functions, and the various relations between them that will be needed for our arguments. Then in Sect. 3 we introduce corresponding Selmer groups, both primitive and imprimitive, and prove some ancillary results for the latter ones. In Sect. 4 we discuss Beilinson–Flach classes and some direct applications of their relations with $p$-adic $L$-functions. As a guide to the general case, in Sect. 5 we give a simplified proof of Theorem A in the case of rank one. In Sect. 6 we prove our new Kolyvagin system bound for twists by characters arbitrarily close to 1, resulting in Theorem C. Finally, in Sect. 7 we run our congruence argument and conclude the proof of Theorem A.

1.5. **Acknowledgements.** We would like to thank Ashay Burungale, Shinichi Kobayashi, and Romyar Sharifi for useful exchanges related to this work. During the preparation of this paper, F.C. was supported by the NSF grants DMS-1946136 and DMS-2101458; G.G. was partially supported by the postdoctoral fellowship of the Fondation Sciences Mathématiques de Paris; C.S. was partially supported by the Simons Investigator Grant #376203 from the Simons Foundation and by the NSF grant DMS-1901985.

## 2. $p$-ADIC $L$-FUNCTIONS

Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N$, and let $p \nmid 2N$ be an odd prime of good ordinary reduction for $E$. Let $K$ be an imaginary quadratic field of discriminant $D_K < 0$ prime to $N$, and assume that

$$(p) = v\bar{v} \text{ splits in } K. \tag{spl}$$

We denote by $\Gamma_{\mathbb{Q}}$ (resp. $\Gamma_K$) the Galois group of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$ (resp. the $\mathbb{Z}_p^2$-extension $K_\infty/K$). Since $p > 2$ the action of complex conjugation gives an eigenspace decomposition

$$\Gamma_K = \Gamma_K^+ \times \Gamma_K^-.$$

Note that $\Gamma_K^+$ (resp. $\Gamma_K^-$) is identified with the Galois group of the cyclotomic $\mathbb{Z}_p$-extension $K_\infty^+/K$ (resp. the anticyclotomic $\mathbb{Z}_p$-extension of $K_\infty^-/K$), and hence $\Gamma_K^+$ is naturally identified with $\Gamma_{\mathbb{Q}}$. Let

$$\Lambda_{\mathbb{Q}} = \mathbb{Z}_p[\![\Gamma_{\mathbb{Q}}]\!], \quad \Lambda_K = \mathbb{Z}_p[\![\Gamma_K]\!], \quad \Lambda_K^\pm = \mathbb{Z}_p[\![\Gamma_K^\pm]\!]$$

be the corresponding Iwasawa algebras, so in particular $\Lambda_K^+$ is naturally identified with $\Lambda_{\mathbb{Q}}$.

2.1. **Cyclotomic $p$-adic $L$-function.** Given a modular parametrization $\pi_E : X_0(N) \to E$, we denote by $c_E \in \mathbb{Z}$ the corresponding Manin constant, so that

$$\pi_E^*(\omega_E) = c_E \cdot 2\pi i f(\tau) d\tau,$$

where $\omega_E$ is a minimal differential on $E$ and $f = \sum_{n=1}^\infty a_n q^n \in S_2(\Gamma_0(N))$ is the newform associated with $E$. 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 $\Omega_E^- \in i\mathbb{R}_{>0}$.

The Fourier coefficient $a_p$ is a $p$-adic unit by hypothesis, and we let $\alpha_p$ be the $p$-adic unit root of $x^2 - a_p x + p$.

**Theorem 2.1.1.** *There exists an element $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q}) \in \Lambda_{\mathbb{Q}}$ such that for any finite order character $\chi$ of $\Gamma_{\mathbb{Q}}$ of conductor $p^r$ with $r > 0$, we have*

$$\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})(\chi) = \frac{p^r}{\tau(\overline{\chi})\alpha_p^r} \cdot \frac{L(E,\overline{\chi},1)}{\Omega_E^+},$$

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

$$\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})(1) = \left(1 - \alpha_p^{-1}\right)^2 \cdot \frac{L(E,1)}{\Omega_E^+}.$$

*Proof.* The construction of $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$ as an element in $\Lambda_{\mathbb{Q}} \otimes \mathbb{Q}_p$ with the stated interpolation property is given in [MSD74, §9]. The integrality of $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$ is shown in [GV00, Prop. 3.7] in the case where $E[p]$ is irreducible as a $G_{\mathbb{Q}}$-module, and in [Wut14, Cor. 18] in the reducible case. Since the latter integrality result and some of the ingredients in the proof will be important later, we briefly outline the argument. First, Wüthrich shows the existence of an elliptic curve $E_\bullet/\mathbb{Q}$ in the isogeny class of $E$ with $\mathcal{L}_p^{\mathrm{MSD}}(E_\bullet/\mathbb{Q}) \in \Lambda_{\mathbb{Q}}$ and whose $p$-adic Tate module satisfies

$$T_p E_\bullet \simeq V_{\mathbb{Z}_p}(f)(1),$$

where $V_{\mathbb{Z}_p}(f)$ is the geometric lattice in the $p$-adic Galois representation $V_{\mathbb{Q}_p}(f)$ associated to $f$ considered in [Kat04, §8.3]. Building on the theorem of Ferrero–Washington [FW79], Kato's divisibility in the Iwasawa main conjecture for $E_\bullet$ "without zeta functions" [Kat04, Thm. 12.5(4)] is shown to be integral, from which the integrality of $\mathcal{L}_p^{\mathrm{MSD}}(E_\bullet/\mathbb{Q})$ and of $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$ itself follows by global duality and the invariance of Mazur's main conjecture under isogenies. □

2.2. **Two-variable $p$-adic $L$-function, I.** In this section we recall the $p$-adic $L$-function constructed in [PR88] following Hida's $p$-adic Rankin method [Hid85], and explain the relation with the $p$-adic $L$-function of Mazur–Swinnerton-Dyer.

Let $\Sigma$ be the set of infinity types of Hecke characters $\psi$ of $K$ for which $s = 1$ is a critical value of the Rankin $L$-function $L(f/K, \psi, s)$. Following the notations and conventions in [LLZ15, §6.1], the set $\Sigma$ decomposes as

$$\Sigma = \Sigma^{(1)} \cup \Sigma^{(2)} \cup \Sigma^{(2')},$$

where $\Sigma^{(1)} = \{(0,0)\}$ (i.e., corresponding to characters $\psi$ of finite order), $\Sigma^{(2)} = \{(a,b)\colon a \leq -1, b \geq 1\}$, and $\Sigma^{(2')} = \{(b,a)\colon a \leq -1, b \geq 1\}$. Note that the regions $\Sigma^{(2)}$ and $\Sigma^{(2')}$ are interchanged by the involution $\psi \mapsto \psi^\tau$, where $\psi^\tau$ denotes the composition of $\psi$ with the non-trivial automorphism $\tau \in \mathrm{Gal}(K/\mathbb{Q})$.

For $\psi$ a finite order Hecke character of $K$ of conductor $\mathfrak{c}$, denote by $\theta(\psi)$ the associated theta series, which is an eigenform of weight one and level $M = D_K \mathbf{N}(\mathfrak{c})$. As in [PR87b, p. 457], define the "Artin root number" of $\psi$ to be the complex number $W(\psi)$ with $|W(\psi)| = 1$ given by

$$\theta(\psi)|_1 \left(\begin{smallmatrix} & -1 \\ M & \end{smallmatrix}\right) = -iW(\psi) \cdot \theta(\psi);$$

then the completed $L$-function $\Lambda(\psi, s) = M^{s/2}(2\pi)^{-s}\Gamma(s)\sum_{\mathfrak{a}} \psi(\mathfrak{a})\mathbf{N}(\mathfrak{a})^{-s}$ satisfies the functional equation $\Lambda(\psi, s) = W(\psi)\Lambda(\overline{\psi}, 1-s)$. As before, let $f \in S_2(\Gamma_0(N))$ be the newform associated with $E$, and put

$$H_p(f) = \Big(1 - \frac{p}{\alpha_p^2}\Big)\Big(1 - \frac{1}{\alpha_p^2}\Big).$$

Denote by $c_f \in \mathbb{Z}_p$ the (cuspidal) *congruence number* of $f$, as defined in e.g. [Hid81, §7] or [Rib83].

**Theorem 2.2.1.** *There exists an element $\mathcal{L}_p(f/K, \Sigma^{(1)}) \in c_f^{-1}\Lambda_K$ such that for every finite order character $\psi$ of $\Gamma_K$ of conductor $v^m\bar{v}^n$ with $m + n > 0$, we have*

$$\mathcal{L}_p(f/K, \Sigma^{(1)})(\psi) = \frac{W(\psi)p^{(m+n)/2}}{\alpha_p^{m+n}H_p(f)} \cdot \frac{L(f/K, \overline{\psi}, 1)}{8\pi^2\langle f, f\rangle_N},$$

*where $W(\psi)$ is the Artin root number of $\psi$, and*

$$\mathcal{L}_p(f/K, \Sigma^{(1)})(1) = \frac{(1-\alpha_p^{-1})^4}{H_p(f)} \cdot \frac{L(f/K, 1)}{8\pi^2\langle f, f\rangle_N},$$

*where $\langle f, g\rangle_N = \int_{\Gamma_0(N)\backslash\mathcal{H}} \overline{f(\tau)}g(\tau)dxdy$ is the Petersson inner product on $S_2(\Gamma_1(N))$.*

*Proof.* This is a reformulation of [PR87b, Thm. 1.1]. For our later use, we note that this is the same as the two-variable $p$-adic $L$-function

$$L_p(f, \boldsymbol{g}) \in c_f^{-1}\mathbb{Z}_p\widehat{\otimes}\Lambda_{\boldsymbol{g}}[\![\Gamma_{\mathbb{Q}}]\!]$$

obtained by specializing to $f$ the three-variable $p$-adic Rankin $L$-series in [KLZ17, Thm. 7.7.2], where $\boldsymbol{g}$ is the CM Hida family introduced in the proof of Lemma 2.4.4 below. □

**Definition 2.2.2** ("Perrin-Riou's $p$-adic $L$-function")**.** Let $f \in S_2(\Gamma_0(N))$ be the newform associated to $E$, and let $\pi_E : X_0(N) \to E$ be a modular parametrization. Then we put

$$\mathcal{L}_p^{\mathrm{PR}}(E/K) := \frac{\deg(\pi_E)}{c_E^2} \cdot H_p(f) \cdot \mathcal{L}_p(f/K, \Sigma^{(1)}),$$

where $c_E$ is the Manin constant associated to $\pi_E$.

**Remark 2.2.3.** Note that the factor $H_p(f)$ can be interpreted as an Euler factor coming from the adjoint $L$-function of $f$ (see [KLZ20, Rem. 6.5.10]). Moreover, setting

$$\Omega_{E/K} := \frac{1}{\sqrt{|D_K|}} \int_{E(\mathbb{C})} \omega_E \wedge i\,\overline{\omega_E}$$

we find

$$8\pi^2 \langle f, f\rangle_N = \int_{X_0(N)} \omega_f \wedge i\,\overline{\omega_f} = \frac{\deg(\pi_E)}{c_E^2} \cdot \Omega_{E/K},$$

and so Theorem 2.2.1 says that $\mathcal{L}_p^{\mathrm{PR}}(E/K)$ interpolates the finite order twists of $L(f/K,1)$ normalized by the complex period $\Omega_{E/K}$.

Denote by $\mathcal{L}_p^{\mathrm{PR}}(E/K)^+ \in \Lambda_{\mathbb{Q}}$ the image of $\mathcal{L}_p^{\mathrm{PR}}(E/K)$ under the map induced by the projection $\Gamma_K \twoheadrightarrow \Gamma_K^+ \simeq \Gamma_{\mathbb{Q}}$.

**Proposition 2.2.4.** *Up to a unit in $\Lambda_{\mathbb{Q}}^\times$, we have*

$$\mathcal{L}_p^{\mathrm{PR}}(E/K)^+ = \mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q}) \cdot \mathcal{L}_p^{\mathrm{MSD}}(E^K/\mathbb{Q}),$$

*where $E^K$ is the twist of $E$ by the quadratic character corresponding to $K/\mathbb{Q}$.*

*Proof.* Let $\chi$ be a Dirichlet character of conductor $p^r$. Using the standard formula

$$W(\chi\circ\mathbf{N}) = \chi(|D_K|)\frac{\tau(\chi)^2}{p^r} = \chi(|D_K|)\frac{p^r}{\tau(\overline{\chi})^2}$$

(see e.g. [Miy06, Lem. 4.8.1]) and the factorization

$$L(f/K, \overline{\chi}\circ\mathbf{N}, 1) = L(E,\overline{\chi},1)\cdot L(E^K,\overline{\chi},1),$$

from Theorem 2.1.1 and Theorem 2.2.1 we find

$$\begin{aligned}
\mathcal{L}_p(f/K,\Sigma^{(1)})(\chi\circ\mathbf{N})\cdot H_p(f) &= W(\chi\circ\mathbf{N})\cdot\frac{p^r}{\alpha_p^{2r}}\cdot L(f/K,\overline{\chi}\circ\mathbf{N},1)\\
&= \chi(|D_K|)\cdot\frac{p^{2r}}{\tau(\overline{\chi})\alpha_p^{2r}}\cdot L(E,\overline{\chi},1)\cdot L(E^K,\overline{\chi},1)\\
&= \chi(|D_K|)\cdot\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})(\chi)\cdot\mathcal{L}_p^{\mathrm{MSD}}(E^K/\mathbb{Q})(\chi)\cdot\frac{\Omega_E^+\cdot\Omega_{E^K}^+}{8\pi^2\langle f,f\rangle_N}.
\end{aligned}$$

Since the complex period $\Omega_{E/K}$ in Remark 2.3.2 satisfies

$$\Omega_{E/K} = [E(\mathbb{R}) : E^0(\mathbb{R})]\cdot\Omega_E^+\cdot\Omega_{E^K}^+$$

(see [GZ86, §V.2]), the result in now clear from the definition of $\mathcal{L}_p^{\mathrm{PR}}(E/K)^+$. □

2.3. **Anticyclotomic $p$-adic $L$-function.** We next recall the "square-root" $p$-adic $L$-function of Bertolini–Darmon–Prasanna [BDP13], explicitly shown to be a $p$-adic measure in [CH18]. Assume that

(Heeg) every prime $\ell|N$ splits in $K$,

and fix an integral ideal $\mathfrak{N}\subset\mathcal{O}_K$ with $\mathcal{O}_K/\mathfrak{N} = \mathbb{Z}/N\mathbb{Z}$. For simplicity, we also assume that

(disc) the discriminant $D_K<0$ is odd and $D_K\neq -3$.

In the following we let $\Omega_p$ and $\Omega_K$ be CM periods attached to $K$ as in [CH18, §2.5] and put $\Lambda_K^{-,\mathrm{ur}} = \Lambda_K\widehat{\otimes}\mathbb{Z}_p^{\mathrm{ur}}$, where $\mathbb{Z}_p^{\mathrm{ur}}$ is the completion of the ring of integers of the maximal unramified extension of $\mathbb{Q}_p$.

**Theorem 2.3.1.** *There exists an element $\mathcal{L}_p^{\mathrm{BDP}}(f/K)\in\Lambda_K^{-,\mathrm{ur}}$ characterized by the following interpolation property: for every character $\xi$ of $\Gamma_K^-$ 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*

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

*Moreover, $\mathcal{L}_p^{\mathrm{BDP}}(f/K)$ is a nonzero element of $\Lambda_K^{-,\mathrm{ur}}$.*

*Proof.* See [CGLS22, Thm. 2.1.1] for the construction, which is deduced from [CH18, §3]. Since (Heeg) implies that $f$ does not have CM by $K$, the nonvanishing of $\mathcal{L}_p^{\mathrm{BDP}}(f/K)$ follows from [CH18, Thm. 3.9]. □

**Remark 2.3.2.** The CM period $\Omega_K \in \mathbb{C}^\times$ in Theorem 2.3.1 agrees with that in [BDP13, (5.1.16)], but is *different* from the period $\Omega_\infty$ defined in [dS87, p. 66] and [HT93, (4.4b)]. In fact, one has

$$\Omega_\infty = 2\pi i \cdot \Omega_K.$$

In terms of $\Omega_\infty$, the interpolation formula in Theorem 2.3.1 reads

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

This is the form of the interpolation that we shall use later.

2.4. **Two-variable $p$-adic $L$-function, II.** The main result of this section is Proposition 2.4.5, relating the $p$-adic $L$-function $\mathcal{L}_p^{\mathrm{BDP}}(f/K)$ of Theorem 2.3.1 to the anticyclotomic projection of the following two-variable $p$-adic Rankin $L$-series.

**Theorem 2.4.1.** *There exists an element $\mathcal{L}_p(f/K, \Sigma^{(2')}) \in \operatorname{Frac}\Lambda_K$ such that for every character $\xi$ of $\Gamma_K$ crystalline at both $v$ and $\bar{v}$, and of infinity type $(b,a)$ with $a \le -1$ and $b \ge 1$, we have*

$$\mathcal{L}_p(f/K, \Sigma^{(2')})(\psi) = \frac{2^{a-b} i^{b-a-1}\Gamma(b+1)\Gamma(b)N^{a+b+1}}{(2\pi)^{2b+1}\langle\theta_{\psi_b}, \theta_{\psi_b}\rangle_N} \cdot \frac{\mathcal{E}(\psi, f, 1)}{(1-\psi^{1-\tau}(\bar{v}))(1-p^{-1}\psi^{1-\tau}(\bar{v}))} \cdot L(f/K, \psi, 1),$$

*where $\theta_{\psi_b}$ is the theta series of weight $b-a+1 \ge 3$ associated to the Hecke character $\psi_b = \psi|\ |^{-b}$ of $\infty$-type $(0, a-b)$, and*

$$\mathcal{E}(\psi, f, 1) = (1 - p^{-1}\psi(\bar{v})\alpha_p)(1 - \psi(\bar{v})\alpha_p^{-1})(1 - \psi^{-1}(v)\alpha_p^{-1})(1 - p^{-1}\psi^{-1}(v)\alpha_p).$$

*Proof.* This is another instance of Hida's $p$-adic Rankin $L$-series, as explained in [LLZ15, Thm. 6.1.3] (note, however, that we have reversed the roles of $v$ and $\bar{v}$ with respect to *loc. cit.*). □

We also need to recall the interpolation property of the Katz $p$-adic $L$-functions [Kat78], following the formulation in [dS87]. Put $\Lambda_K^{\mathrm{ur}} = \Lambda_K \widehat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p^{\mathrm{ur}}$.

**Theorem 2.4.2.** *There exists an element $\mathcal{L}_{\bar{v}}(K) \in \Lambda_K^{\mathrm{ur}}$ such that for every character $\xi$ of $\Gamma_K$ of infinity type $(k,j)$ with $0 \le -j < k$ satisfies*

$$\mathcal{L}_{\bar{v}}(K)(\xi) = \frac{\Omega_p^{k-j}}{\Omega_\infty^{k-j}} \cdot \Gamma(k) \cdot \left(\frac{\sqrt{D_K}}{2\pi}\right)^j \cdot (1 - \xi^{-1}(\bar{v})p^{-1})(1 - \xi(v)) \cdot L(\xi, 0).$$

*Similarly, there exists an element $\mathcal{L}_v(K) \in \Lambda_K^{\mathrm{ur}}$ such that for every character $\xi$ of $\Gamma_K$ of infinity type $(j,k)$ with $0 \le -j < k$, we have*

$$\mathcal{L}_v(K)(\xi) = \frac{\Omega_p^{k-j}}{\Omega_\infty^{k-j}} \cdot \Gamma(k) \cdot \left(\frac{\sqrt{D_K}}{2\pi}\right)^j \cdot (1 - \xi^{-1}(v)p^{-1})(1 - \xi(\bar{v})) \cdot L(\xi, 0).$$

*Moreover, we have the functional equation*

$$\mathcal{L}_{\bar{v}}(\xi) = \mathcal{L}_v(\xi^{-1}\mathbf{N}^{-1}),$$

*where the equality is up to a $p$-adic unit.*

*Proof.* This is [dS87, Thm. II.4.14], with $\mathcal{L}_{\bar{v}}(K)$ (resp. $\mathcal{L}_v(K)$) corresponding to the measure $\mu(\bar{v}^\infty)$ (resp. $\mu(v^\infty)$) in *loc. cit.*. On the other hand, as explained in [BCG+20, Lem. 3.3.2(b)], the stated functional equation is a reformulation of [dS87, Thm. II.6.4]. □

**Definition 2.4.3** ("Greenberg's $p$-adic $L$-function")**.** Put

$$\mathcal{L}_p^{\mathrm{Gr}}(f/K) := h_K \cdot \mathcal{L}_v(K)^- \cdot \mathcal{L}_p(f/K, \Sigma^{(2')}),$$

where $h_K$ is the class number of $K$ and $\mathcal{L}_v(K)^-$ the image of $\mathcal{L}_v(K)$ under the map $\Lambda_K^{\mathrm{ur}} \to \Lambda_K^{\mathrm{ur}}$ given by $\gamma \mapsto \gamma^{1-\tau}$ for $\gamma \in \Gamma_K$.

Note that *a priori* we have $\mathcal{L}_p^{\mathrm{Gr}}(f/K) \in \operatorname{Frac}\Lambda_K^{\mathrm{ur}}$.

**Lemma 2.4.4.** *The $p$-adic $L$-function $\mathcal{L}_p^{\mathrm{Gr}}(f/K)$ is integral, i.e., $\mathcal{L}_p^{\mathrm{Gr}}(f/K) \in \Lambda_K^{\mathrm{ur}}$.*

*Proof.* Denote by $\eta = \eta_{K/\mathbb{Q}}$ the quadratic character corresponding to $K/\mathbb{Q}$, and let $\mathrm{Eis}_{1,\eta}(q)$ be the weight one Eisenstein series

$$\mathrm{Eis}_{1,\eta}(q) = \sum_{n\geq 1} q^n \sum_{d|n} \eta(d).$$

Since $p$ splits in $K$, $\mathrm{Eis}_{1,\eta}(q)$ is $p$-irregular. Letting $g$ denote the unique $p$-stabilization of $\mathrm{Eis}_{1,\eta}$, by [BDP22, Thm. A(i)] there is a unique cuspidal Hida family $\boldsymbol{g}$ passing through $g$. Moreover, $\boldsymbol{g}$ is of CM type, given explicitly as the $q$-series

$$\boldsymbol{g} = \sum_{(\mathfrak{a},\bar{v})=1} [\mathfrak{a}] q^{\mathbf{N}(\mathfrak{a})} \in \Lambda_{\boldsymbol{g}}[\![q]\!],$$

where $\Lambda_{\boldsymbol{g}} = \mathbb{Z}_p[\![\Gamma_v]\!]$, for $\Gamma_v$ the Galois group of the maximal $\mathbb{Z}_p$-extension inside $K_\infty/K$ unramified at $v$, and where $[\mathfrak{a}]$ denotes the natural image of the ideal $\mathfrak{a} \subset \mathcal{O}_K$ in $\Gamma_v$ under the Artin reciprocity map.

Now, the $p$-adic $L$-function $\mathcal{L}_p(f/K, \Sigma^{(2')})$ in Theorem 2.4.1 arises from Hida's $p$-adic Rankin $L$-series

$$L_p(\boldsymbol{g}, f) \in I_{\boldsymbol{g}} \widehat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p[\![\Gamma_{\mathbb{Q}}]\!],$$

where $I_{\boldsymbol{g}} \subset \mathrm{Frac}\,\Lambda_{\boldsymbol{g}}$ is the cuspidal congruence ideal of $\boldsymbol{g}$ (that is, the image of the $\Lambda_{\boldsymbol{g}}$-adic cuspforms in $\mathrm{Frac}\,\Lambda_{\boldsymbol{g}}$ under the projection corresponding to $\boldsymbol{g}$). Thus if $H(\boldsymbol{g}) \in \Lambda_{\boldsymbol{g}}$ denotes a characteristic power series for the denominator of $I_{\boldsymbol{g}}$, then the product $H(\boldsymbol{g}) \cdot \mathcal{L}_p(f/K, \Sigma^{(2)})$ is integral, so it suffices to show that $h_K \cdot \mathcal{L}_v(K)^-$ is divisible by $H(\boldsymbol{g})$.

By [HT94, Thm. 0.3] and Rubin's proof of the Iwasawa main conjecture for $K$, [Rub91], one has that such divisibility holds up to powers of the augmentation ideal $(\gamma_v - 1) \subset \mathbb{Z}_p[\![\Gamma_v]\!]$; since by [BDP22, Thm. A(i)] one knows that $H(\boldsymbol{g})$ is not divisible by $\gamma_v - 1$, the result follows. □

Denote by $\mathcal{L}_p^{\mathrm{Gr}}(f/K)^-$ the image of $\mathcal{L}_p^{\mathrm{Gr}}(f/K)$ under the natural projection $\Lambda_K^{\mathrm{ur}} \to \Lambda_K^{-,\mathrm{ur}}$.

**Proposition 2.4.5.** *We have the equality*

$$\mathcal{L}_p^{\mathrm{Gr}}(f/K)^- \cdot \Lambda_K^{-,\mathrm{ur}} = \mathcal{L}_p^{\mathrm{BDP}}(f/K) \cdot \Lambda_K^{-,\mathrm{ur}}.$$

*Proof.* This follows from a direct comparison of the interpolation formulas in Theorem 2.4.1, Theorem 2.3.1 and Theorem 2.4.2, together with an application of Dirichlet's class number formula (cf. [Cas17, Thm. 1.7]).

Indeed, let $\xi$ be a Hecke character of infinity type $(n,-n)$, $n \in \mathbb{Z}_{\geq 0}$, as in the statement of Theorem 2.3.1. Then the character $\xi^{1-\tau}\mathbf{N}^{-1}$, of infinity type $(2n+1, 1-2n)$, is in the range of interpolation of $\mathcal{L}_{\bar{v}}(K)$, and noting that $L(\xi^{1-\tau}\mathbf{N}^{-1}, 0) = L(\xi^{1-\tau}, 1)$, by Theorem 2.4.2 we have

$$\mathcal{L}_{\bar{v}}(K)(\xi^{1-\tau}\mathbf{N}^{-1}) = \frac{\Omega_p^{4n}}{\Omega_\infty^{4n}} \cdot \Gamma(2n+1) \cdot \left(\frac{2\pi}{\sqrt{D_K}}\right)^{2n-1} \cdot (1-\xi^{1-\tau}(\bar{v}))(1-\xi^{1-\tau}(v)p^{-1}) \cdot L(\xi^{1-\tau}, 1). \tag{2.1}$$

On the other hand, from Hida's formula for the adjoint $L$-value (see [HT93, Thm .7.1]) and Dirichlet's class number formula we obtain

$$\langle \theta_{\xi_n}, \theta_{\xi_n} \rangle_N \ \sim_p \ \Gamma(2n+1) \cdot \frac{1}{2^{4n-1}\pi^{2n+1}} \cdot h_K \cdot L(\xi^{1-\tau}, 1), \tag{2.2}$$

where $\sim_p$ denotes equality up to $p$-adic unit independent of $n$, and similarly as in Theorem 2.4.1, $\xi_n$ is the theta series of weight $2n+1 \geq 3$ associated to the Hecke character $\xi_n = \xi|\ |^{-n}$ of infinity type $(0,-2n)$. Combining (2.1), (2.2) and the functional equation in Theorem 2.4.2 this gives

$$h_K \cdot \mathcal{L}_v(K)(\xi^{1-\tau}) \ \sim_p \ \frac{\Omega_p^{4n}}{\Omega_\infty^{4n}} \cdot \left(\frac{2\pi}{\sqrt{D_K}}\right)^{2n-1} \cdot (1-\xi^{1-\tau}(\bar{v}))(1-\xi^{1-\tau}(v)p^{-1}) \cdot 2^{4n-1}\pi^{2n+1} \cdot \langle \theta_{\xi_n}, \theta_{\xi_n} \rangle_N.$$

Noting that the $p$-Euler factor $\mathcal{E}(\psi, f, 1)$ in Theorem 2.4.1 satisfies

$$\mathcal{E}(\xi, f, 1) = \left(1 - a_p \xi(\overline{v}) p^{-1} + \xi(\bar{v})^2 p^{-1}\right)^2,$$

from Definition 2.4.3, Theorem 2.4.1, and Theorem 2.3.1 we thus find that

$$\mathcal{L}_p^{\mathrm{Gr}}(f/K)(\xi) \ \sim_p \ \xi(\mathfrak{N}) \cdot 2^{3n-2} i^{2n-1} \cdot \mathcal{L}_p^{\mathrm{BDP}}(f/K)(\xi).$$

Since $\xi(\mathfrak{N}) \cdot 2^{3n-2} i^{2n-1}$ is interpolated by a unit in $\Lambda_K^{-,\mathrm{ur}}$, this completes the proof. □

2.5. **Twists and imprimitive $p$-adic $L$-functions.** Let $\alpha : \Gamma_K \to R^\times$ be a character with values in the ring of integers $R$ of a finite extension $\Phi/\mathbb{Q}_p$ with uniformiser $\varpi \in R$. Let $\Lambda_{K,R} = R\widehat{\otimes}_{\mathbb{Z}_p}\Lambda_K = R[\![\Gamma_K]\!]$, and define

$$\mathrm{Tw}_\alpha : \Lambda_{K,R} \to \Lambda_{K,R}$$

to be the $R$-linear isomorphism given by $\gamma \mapsto \alpha(\gamma)\gamma$ for $\gamma \in \Gamma_K$. Denote by $\mathcal{L}_p^{\mathrm{PR}}(E(\alpha)/K), \mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)$ the image of $\mathcal{L}_p^{\mathrm{PR}}(E/K), \mathcal{L}_p^{\mathrm{Gr}}(f/K)$, respectively, under $\mathrm{Tw}_\alpha$.

**Lemma 2.5.1.** *Suppose* $\alpha \equiv 1 \pmod{\varpi^m}$. *Then*

$$\mathcal{L}_p^{\mathrm{PR}}(E(\alpha)/K)^+ \equiv \mathcal{L}_p^{\mathrm{PR}}(E/K)^+ \pmod{\varpi^m}.$$

*Proof.* This is clear from the definitions. □

For $w$ a prime split in $K$ lying over the rational prime $\ell \neq p$, we let $\Gamma_w^\pm$ be the corresponding decomposition group in $\Gamma_K^\pm$, and $\gamma_w^\pm \in \Gamma_w^\pm$ be the image of an arithmetic Frobenius $\mathrm{Frob}_w$ under the projection $G_K \to \Gamma_K^\pm$.

**Definition 2.5.2.** Put

$$\mathcal{P}_w^\pm(\alpha) := P_w(\ell^{-1}\gamma_w^\pm) \in \Lambda_{K,R}^\pm,$$

where $P_w(X) = \det(1 - \mathrm{Frob}_w X \,|\, V(\alpha)_{I_w})$ is the Euler factor at $w$ of the $L$-function of $V(\alpha) = T_pE(\alpha) \otimes \mathbb{Q}_p$. For $S'$ a finite set of primes $w$ as above, define

$$\mathcal{L}_p^{\mathrm{PR}}(E(\alpha)/K)^{+,S'} := \mathcal{L}_p^{\mathrm{PR}}(E(\alpha)/K)^+ \cdot \prod_{w\in S'} \mathcal{P}_w^+(\alpha),$$
$$\mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^{\pm,S'} := \mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^\pm \cdot \prod_{w\in S'} \mathcal{P}_w^\pm(\alpha),$$

and similarly $\mathcal{L}_p^{\mathrm{BDP}}(f(\alpha)/K)^{S'} := \mathcal{L}_p^{\mathrm{BDP}}(f(\alpha)/K) \cdot \prod_{w\in S'} \mathcal{P}_w^-(\alpha)$.

Of course, the results of Proposition 2.2.4 and Proposition 2.4.5 directly extend to their analogues for these $S'$-imprimitive $p$-adic $L$-functions.

## 3. Selmer groups

In this section, we let $E/\mathbb{Q}$ be an elliptic curve of conductor $N$, $p$ an odd prime of good ordinary reduction for $E$, and $K$ an imaginary quadratic field satisfying (Heeg) and (spl).

3.1. **Selmer structures.** Let $\Sigma$ be a finite set of places of $\mathbb{Q}$ containing the prime $p$, $\infty$, and the prime factors of $N$. We assume throughout that

$$\text{all finite primes in } \Sigma \text{ split in } K.$$

With a slight abuse of notation, we also write $\Sigma$ for the set of places of $K$ lying above the places in $\Sigma$.

3.1.1. *Discrete coefficients.* For a discrete $\mathbb{Z}_p$-module $M$, we let

$$M^\vee = \mathrm{Hom}_{\mathrm{cts}}(M, \mathbb{Q}/\mathbb{Z}_p)$$

be the Pontryagin dual. The module $\Lambda_{\mathbb{Q}}^\vee$ is equipped with a $G_{\mathbb{Q}}$-action via $\Psi^{-1}$, where $\Psi : G_{\mathbb{Q}} \to \Lambda_{\mathbb{Q}}^\times$ is the character arising from the projection $G_{\mathbb{Q}} \twoheadrightarrow \Gamma_{\mathbb{Q}}$. Similarly, $\Lambda_K^\vee$ and $(\Lambda_K^\pm)^\vee$ are equipped with $G_K$-actions.

**Definition 3.1.1.** Let $F$ be $\mathbb{Q}$ or $K$ and $w$ a prime above $p$. For $\Lambda$ any of the Iwasawa algebras $\Lambda_{\mathbb{Q}}$, $\Lambda_K$, or $\Lambda_K^\pm$, we put

$$\mathrm{H}^1_{\mathrm{rel}}(F_w, T_pE \otimes \Lambda^\vee) = \mathrm{H}^1(F_w, T_pE \otimes \Lambda^\vee),$$
$$\mathrm{H}^1_{\mathrm{ord}}(F_w, T_pE \otimes \Lambda^\vee) = \mathrm{im}\big\{\mathrm{H}^1(F_w, \mathrm{Fil}_w^+(T_pE) \otimes \Lambda^\vee) \to \mathrm{H}^1(F_w, T_pE \otimes \Lambda^\vee)\big\},$$
$$\mathrm{H}^1_{\mathrm{str}}(F_w, T_pE \otimes \Lambda^\vee) = \{0\},$$

where $\mathrm{Fil}_w^+(T_pE) := \ker\big\{T_pE \to T_p\tilde{E}\big\}$ with $\tilde{E}$ the reduction of $E$ at $w$.

Let $G_{\mathbb{Q},\Sigma}$ and $G_{K,\Sigma}$ denote the Galois group of the maximal extension of $\mathbb{Q}$ and $K$ respectively unramified outside $\Sigma$. For $\bullet \in \{\mathrm{ord}, \mathrm{str}, \mathrm{rel}\}$ and $M = T_pE \otimes \Lambda_{\mathbb{Q}}^\vee$, we define the Selmer group

$$\mathrm{H}^1_{\mathcal{F}_\bullet}(\mathbb{Q}, M) = \ker\left(\mathrm{H}^1(G_{\mathbb{Q},\Sigma}, M) \to \prod_{w\in\Sigma, w\nmid p} \mathrm{H}^1(\mathbb{Q}_w, M) \times \frac{\mathrm{H}^1(\mathbb{Q}_p, M)}{\mathrm{H}^1_\bullet(\mathbb{Q}_p, M)}\right). \tag{3.1}$$

Similarly, for $\star, \bullet \in \{\mathrm{ord}, \mathrm{str}, \mathrm{rel}\}$ and $M = T_pE \otimes \Lambda^\vee$, where $\Lambda$ is any of the Iwasawa algebras $\Lambda_K$ or $\Lambda_K^\pm$, we let

$$\mathrm{H}^1_{\mathcal{F}_{\star,\bullet}}(K, M) = \ker\left(\mathrm{H}^1(G_{K,\Sigma}, M) \to \prod_{w\in\Sigma, w\nmid p} \mathrm{H}^1(K_w, M) \times \frac{\mathrm{H}^1(K_v, M)}{\mathrm{H}^1_\star(K_v, M)} \times \frac{\mathrm{H}^1(K_{\bar v}, M)}{\mathrm{H}^1_\bullet(K_{\bar v}, M)}\right). \tag{3.2}$$

To ease notation, we write $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, M) = \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord},\mathrm{ord}}}(K, M)$ and $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M) = \mathrm{H}^1_{\mathcal{F}_{\mathrm{rel},\mathrm{str}}}(K, M)$, and put

$$\begin{aligned}
\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty) &= \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(\mathbb{Q}, T_pE \otimes \Lambda_{\mathbb{Q}}^\vee)^\vee,\\
\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^\pm) &= \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_pE \otimes (\Lambda_K^\pm)^\vee)^\vee,\\
\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty^\pm) &= \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, T_pE \otimes (\Lambda_K^\pm)^\vee)^\vee.
\end{aligned}$$

It is a standard fact that these are finitely generated modules over the corresponding Iwasawa algebras. The Iwasawa main conjecture for $E$, as formulated by Mazur [Maz72], [MSD74, §9.5, Conj. 3], is the following.

**Conjecture 3.1.2** (Mazur)**.** The module $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)$ is $\Lambda_{\mathbb{Q}}$-torsion, with

$$\mathrm{ch}_{\Lambda_{\mathbb{Q}}}\big(\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)\big) = \big(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})\big).$$

More generally, a vast generalization of Mazur's main conjecture to $p$-adic deformations of motives formulated by Greenberg [Gre89, Gre94], predicts the following.

**Conjecture 3.1.3** (Greenberg)**.** The modules $\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^+)$ and $\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty^-)$ are torsion over $\Lambda_K^+$ and $\Lambda_K^-$ respectively, with

$$\begin{aligned}
\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^+)\big) &= \big(\mathcal{L}_p^{\mathrm{PR}}(E/K)^+\big),\\
\mathrm{ch}_{\Lambda_K^-}\big(\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty^-)\big)\Lambda_K^{-,\mathrm{ur}} &= \big(\mathcal{L}_p^{\mathrm{Gr}}(f/K)^-\big).
\end{aligned}$$

In this paper we shall prove Mazur's Main Conjecture 3.1.2 (in the case where $p$ is a good Eisenstein prime for $E$) by first proving Conjecture 3.1.3 for a suitable $K$.

3.1.2. *Isogeny invariance.* Conjectures 3.1.2 and 3.1.3 are known to be invariant under isogenies. This follows from a computation in global duality due to Schneider and Perrin-Riou [Sch87, PR87a].

**Proposition 3.1.4.** *Suppose $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ are isogenous elliptic curves with good ordinary reduction at $p$. Assume that $\mathfrak{X}_{\mathrm{ord}}(E_i/K_\infty^\pm)$ is $\Lambda_K^+$-torsion ($i = 1, 2$), and let $\mathcal{F}_{\mathrm{ord}}(E_i/K_\infty^+)$ and $\mathcal{F}_{\mathrm{ord}}(E_i/\mathbb{Q}_\infty)$ be characteristic power series for $\mathfrak{X}_{\mathrm{ord}}(E_i/K_\infty^+)$ and $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)$, respectively. Then we have the equalities up to a $p$-adic unit:*

$$\begin{aligned}
\Omega_{E_1}\cdot\mathcal{F}_{\mathrm{ord}}(E_1/\mathbb{Q}_\infty) &\sim_p \Omega_{E_2}\cdot\mathcal{F}_{\mathrm{ord}}(E_2/\mathbb{Q}_\infty),\\
\Omega_{E_1/K}\cdot\mathcal{F}_{\mathrm{ord}}(E_1/K_\infty^+) &\sim_p \Omega_{E_2/K}\cdot\mathcal{F}_{\mathrm{ord}}(E_2/K_\infty^+).
\end{aligned}$$

*In particular, the main conjectures for $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)$ and $\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^+)$ are both invariant under isogenies.*

*Proof.* See [PR87a, Appendice]. □

Although not directly needed for our arguments, we note that the isogeny invariance of the main conjecture for $\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty^-)$ similarly follows from the main result of [PR89] (see [KO20, Prop. 2.9]).

3.1.3. *Compact coefficients.* For $\Lambda$ any of the Iwasawa algebras $\Lambda_{\mathbb{Q}}$, $\Lambda_K$, or $\Lambda_K^\pm$, consider the compact module

$$T_pE\widehat{\otimes}_{\mathbb{Z}_p}\Lambda,$$

where $\Lambda$ is equipped with a $G_K$-action via $\Psi : G_K \to \Lambda^\times$. For $\bullet \in \{\mathrm{ord}, \mathrm{str}, \mathrm{rel}\}$ and $w$ a prime of $K$ above $p$, we define the local conditions $\mathrm{H}^1_\bullet(K_w, T_pE\widehat{\otimes}_{\mathbb{Z}_p}\Lambda) \subset \mathrm{H}^1(K_w, T_pE\widehat{\otimes}_{\mathbb{Z}_p}\Lambda)$ similarly as in Definition 3.1.1, and for $\star, \bullet \in \{\mathrm{ord}, \mathrm{str}, \mathrm{rel}\}$ we define the Selmer group $\mathrm{H}^1_{\mathcal{F}_{*,\bullet}}(K, T_pE\widehat{\otimes}_{\mathbb{Z}_p}\Lambda)$ by the same recipe as in (3.2). Put

$$\mathfrak{S}_{\mathrm{ord},\mathrm{rel}}(E/K_\infty) = \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord},\mathrm{rel}}}(K, T_pE\widehat{\otimes}_{\mathbb{Z}_p}\Lambda_K), \quad \mathfrak{S}_{\mathrm{ord}}(E/K_\infty) = \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord},\mathrm{ord}}}(K, T_pE\widehat{\otimes}_{\mathbb{Z}_p}\Lambda_K),$$

etc., and similarly for $E/K_\infty^\pm$ with $\Lambda_K$ in place of $\Lambda_K^\pm$, respectively.

3.2. **Imprimitive Selmer groups.** For any subset $S' \subset \Sigma$ consisting of primes away from $p$, we define $S'$-imprimitive versions of the above Selmer groups by relaxing the local conditions at the primes $w \in S'$, e.g. for $M = T_pE \otimes \Lambda_{\mathbb{Q}}^\vee$:

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

We denote with a superscript $S'$ the Pontryagin duals of these modules:

$$\begin{aligned}
\mathfrak{X}^{S'}_{\mathrm{ord}}(E/\mathbb{Q}_\infty) &= \mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{ord}}}(\mathbb{Q}, T_pE \otimes \Lambda_{\mathbb{Q}}^\vee)^\vee,\\
\mathfrak{X}^{S'}_{\mathrm{ord}}(E/K^\pm_\infty) &= \mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{ord}}}(K, T_pE \otimes (\Lambda^\pm_K)^\vee)^\vee,\\
\mathfrak{X}^{S'}_{\mathrm{Gr}}(E/K^\pm_\infty) &= \mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, T_pE \otimes (\Lambda^\pm_K)^\vee)^\vee.
\end{aligned}$$

The next result will be used to descend from $K$ to $\mathbb{Q}$ (*cf.* Proposition 2.2.4). As done here, in the following we shall often identify the Iwasawa algebras $\Lambda^+_K$ and $\Lambda_{\mathbb{Q}}$ (via the natural projection $\Lambda^+_K \xrightarrow{\sim} \Gamma_{\mathbb{Q}}$).

**Proposition 3.2.1.** *Let $S' \subset \Sigma$ be any subset of primes not lying above $p$. Then the restriction map from $G_{\mathbb{Q}}$ to $G_K$ induces a $\Lambda_{\mathbb{Q}}$-module isomorphism*

$$\mathfrak{X}^{S'}_{\mathrm{ord}}(E/K^+_\infty) \simeq \mathfrak{X}^{S'}_{\mathrm{ord}}(E/\mathbb{Q}_\infty) \oplus \mathfrak{X}^{S'}_{\mathrm{ord}}(E^K/\mathbb{Q}_\infty).$$

*In particular,*

$$\mathrm{ch}_{\Lambda^+_K}\big(\mathfrak{X}^{S'}_{\mathrm{ord}}(E/K^+_\infty)\big) = \mathrm{ch}_{\Lambda_{\mathbb{Q}}}\big(\mathfrak{X}^{S'}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)\big) \cdot \mathrm{ch}_{\Lambda_{\mathbb{Q}}}\big(\mathfrak{X}^{S'}_{\mathrm{ord}}(E^K/\mathbb{Q}_\infty)\big).$$

*Proof.* This follows readily from the inflation-restriction exact sequence and Shapiro's lemma (see e.g. [SU14, Lem. 3.6]). □

3.2.1. *From imprimitive to primitive.* As observed by Greenberg, imprimitive Selmer groups as above tend to have better properties with respect to congruences than their primitive counterparts. For our arguments, we shall also find it convenient to work first with imprimitive Selmer group, and so the next results will be useful.

**Proposition 3.2.2.** *Assume that $E(K)[p] = 0$ and that $\mathfrak{X}_{\mathrm{ord}}(E/K^+_\infty)$ is $\Lambda^+_K$-torsion. Then for any $S' \subset \Sigma$ consisting of primes away from $p$, the Selmer group $\mathfrak{X}^{S'}_{\mathrm{ord}}(E/K^+_\infty)$ is also $\Lambda^+_K$-torsion, with*

$$\mathrm{ch}_{\Lambda^+_K}\big(\mathfrak{X}^{S'}_{\mathrm{ord}}(E/K^+_\infty)\big) = \mathrm{ch}_{\Lambda^+_K}\big(\mathfrak{X}_{\mathrm{ord}}(E/K^+_\infty)\big) \cdot \prod_{w\in S'} \big(\mathcal{P}^+_w(1)\big),$$

*where $\mathcal{P}^+_w(1) \in \Lambda^+_K$ is as in Definition 2.5.2, with $\alpha = 1$.*

*Proof.* From the assumption that $E(K)[p] = 0$, we see that the $G_{K^+_\infty}$-invariants of $\mathrm{Hom}(T_pE, \mu_{p^\infty})$ are trivial, and so by [PW11, Prop. A.2] the global-to-local map defining $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T_pE \otimes (\Lambda^+_K)^\vee)$ as in (3.2) is surjective. We therefore find an exact sequence

$$0 \to \prod_{w\in S'} \mathrm{H}^1(K_w, T_pE \otimes (\Lambda^+_K)^\vee)^\vee \to \mathfrak{X}^{S'}_{\mathrm{ord}}(E/K^+_\infty) \to \mathfrak{X}_{\mathrm{ord}}(E/K^+_\infty) \to 0. \tag{3.3}$$

Since the primes $w \in S'$ split in $K$, by [GV00, Prop. 2.4] the module $\mathrm{H}^1(K_w, T_pE \otimes (\Lambda^+_K)^\vee)^\vee$ is $\Lambda^+_K$-torsion, with

$$\mathrm{ch}_{\Lambda^+_K}\big(\mathrm{H}^1(K_w, T_pE \otimes (\Lambda^+_K)^\vee)^\vee\big) = \big(\mathcal{P}^+_w(1)\big).$$

The result now follows by taking characteristic ideals in (3.3). □

**Corollary 3.2.3.** *Assume that $E(K)[p] = 0$ and let $S' \subset \Sigma$ be any subset consisting of primes away from $p$. Then Conjecture 3.1.3 for $\mathfrak{X}_{\mathrm{ord}}(E/K^+_\infty)$ holds if and only if $\mathfrak{X}^{S'}_{\mathrm{ord}}(E/K^+_\infty)$ is $\Lambda^+_K$-torsion, with*

$$\mathrm{ch}_{\Lambda^+_K}\big(\mathfrak{X}^{S'}_{\mathrm{ord}}(E/K^+_\infty)\big) = \big(\mathcal{L}^{\mathrm{PR}}_p(E/K)^{+,S'}\big).$$

*Proof.* Since for any prime $w \in S'$, the element $\mathcal{P}^+_w(1) \in \Lambda^+_K$ is nonzero, this is clear from Definition 2.5.2 and Proposition 3.2.2. □

3.3. **Anticyclotomic twists and congruences.** We now introduce the twisted variants of the Selmer groups from the preceding sections that we shall need. The results of Proposition 3.3.2 and Proposition 3.3.4 will play an important role later.

Let $\Phi$ be a finite extension of $\mathbb{Q}_p$, and let $R$ be the ring of integers of $\Phi$ with uniformizer $\varpi$. We consider a character $\alpha : \Gamma_K^- \to R^\times$ which satisfies

$$\alpha \equiv 1 \pmod{\varpi^m}$$

for some $m > 0$. Let $S' \subset \Sigma$ be any subset consisting of primes away from $p$. Replacing $T_pE$ by the twist

$$T_\alpha := T_pE \otimes_{\mathbb{Z}_p} R(\alpha),$$

we define (imprimitive) Selmer groups $\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{ord}}}(K, T_\alpha \otimes (\Lambda_K^\pm)^\vee)$ and $\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, T_\alpha \otimes (\Lambda_K^\pm)^\vee)$ (with Pontryagin duals $\mathfrak{X}^{S'}_{\mathrm{ord}}(E(\alpha)/K_\infty^\pm)$ and $\mathfrak{X}^{S'}_{\mathrm{Gr}}(E(\alpha)/K_\infty^\pm)$, respectively) in the same way as before, replacing $\mathrm{Fil}^+_w(T_pE)$ by $\mathrm{Fil}^+_w(T_pE) \otimes_{\mathbb{Z}_p} R(\alpha)$ in Definition 3.1.1. We also consider their counterparts with $K_\infty^\pm$ and $\Lambda_K^\pm$ replaced by $K_\infty$ and $\Lambda_K$, respectively. Each of these Selmer groups is a module for the Iwasawa algebra $\Lambda_R = R\widehat{\otimes}_{\mathbb{Z}_p}\Lambda$ with $\Lambda$ either $\Lambda_{\mathbb{Q}}$, $\Lambda_K$, or $\Lambda_K^\pm$ (per the definitions).

Put $V_\alpha = T_\alpha \otimes \mathbb{Q}_p$ and $W_\alpha = T_\alpha \otimes \mathbb{Q}_p/\mathbb{Z}_p = V_\alpha/T_\alpha$. We shall also need to consider the following variant of the above Selmer groups for the module $W_\alpha := T_\alpha \otimes \mathbb{Q}_p/\mathbb{Z}_p$:

$$\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, V_\alpha) := \ker\left(\mathrm{H}^1(G_{K,\Sigma}, V_\alpha) \to \prod_{w\in\Sigma\smallsetminus S', w\nmid p} \mathrm{H}^1(K_w, V_\alpha) \times \mathrm{H}^1(K_{\bar{v}}, V_\alpha)\right),$$

and the resulting $\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, T_\alpha)$ and $\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, W_\alpha)$ obtained by propagation via $0 \to T_\alpha \to V_\alpha \to W_\alpha \to 0$. We also consider the Bloch–Kato Selmer group $\mathrm{H}^1_{\mathcal{F}_{\mathrm{BK}}}(K, V_\alpha)$ consisting of classes that land in

$$\mathrm{H}^1_f(K_w, V_\alpha) := \ker(\mathrm{H}^1(K_w, V_\alpha) \to \mathrm{H}^1(K_w, V_\alpha \otimes \mathbf{B}_{\mathrm{cris}}))$$

at the primes $w \mid p$ and are trivial at the primes $w \nmid p$, and its counterparts $\mathrm{H}^1_{\mathcal{F}_{\mathrm{BK}}}(K, T_\alpha)$ and $\mathrm{H}^1_{\mathcal{F}_{\mathrm{BK}}}(K, W_\alpha)$ defined by propagating the local conditions.

3.3.1. *Ancillary results for $\mathfrak{X}_{\mathrm{Gr}}(E(\alpha)/K_\infty^\pm)$.* The main result of this section is a relation between the specializations of the cyclotomic Selmer group $\mathfrak{X}_{\mathrm{Gr}}(E(\alpha)/K_\infty^+)$ and the anticyclotomic Selmer group $\mathfrak{X}_{\mathrm{Gr}}(E(\alpha)/K_\infty^-)$ at the trivial character.

Define

$$M_\alpha^\pm = T_\alpha \widehat{\otimes}_{\mathbb{Z}_p} (\Lambda_K^\pm)^\vee,$$

and for any $S' \subset \Sigma$ consisting of primes not dividing $p$, put

$$\mathcal{P}_{\mathrm{Gr}}(M_\alpha; S') := \mathrm{H}^1(K_{\bar{v}}, M_\alpha) \times \prod_{w\in\Sigma\smallsetminus S', w\nmid p} \mathrm{H}^1(K_w, M_\alpha),$$

and similarly,

$$\mathcal{P}_{\mathrm{Gr}}(W_\alpha; S') := \frac{\mathrm{H}^1(K_v, W_\alpha)}{\mathrm{H}^1(K_v, W_\alpha)_{\mathrm{div}}} \times \mathrm{H}^1(K_{\bar{v}}, W_\alpha) \times \prod_{w\in\Sigma\smallsetminus S', w\nmid p} \mathrm{H}^1(K_w, W_\alpha),$$

so in particular $\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, W_\alpha)$ is the kernel of the global-to-local map $\mathrm{H}^1(G_{K,\Sigma}, W_\alpha) \to \mathcal{P}_{\mathrm{Gr}}(W_\alpha; S')$.

**Lemma 3.3.1.** *Assume $E(K)[p] = 0$ and $\alpha : \Gamma_K^- \to R^\times$ is a crystalline character such that:*

(a) $\mathrm{corank}_R \mathrm{H}^1_{\mathcal{F}_{\mathrm{BK}}}(K, W_{\alpha^{-1}}) = 1$,

(b) *The restriction map*

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{BK}}}(K, W_{\alpha^{-1}}) \xrightarrow{\mathrm{loc}_v} \mathrm{H}^1_f(K_v, W_{\alpha^{-1}})$$

*is nonzero.*

*Then the following hold:*

(i) $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, W_\alpha)$ *is finite, and* $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, T_\alpha) = 0$.

(ii) $\mathrm{H}^1(G_{K,\Sigma}, M_\alpha^\pm)_{\Gamma_K^\pm} = 0$.

(iii) *For any $S' \subset \Sigma$ consisting of primes away from $p$,* $\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, M_\alpha^\pm)_{\Gamma_K^\pm} = 0$.

*Proof.* It follows from their definition by propagation that $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K,T_\alpha)$ is the $p$-adic Tate module of $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K,W_\alpha)$, and so part (i) is shown in Proposition 3.2.1 of [JSW17]. For the proof of parts (ii) and (iii), we shall adapt the arguments in the proof of [*op. cit.*, Lem. 3.3.5]. Let $\gamma^\pm \in \Gamma_K^\pm$ be any topological generator. From the relation $W_\alpha = (M_\alpha^\pm)^{\Gamma_K^\pm} = M_\alpha^\pm[\gamma^\pm - 1]$ we get an injection

$$\mathrm{H}^1(G_{K,\Sigma}, M_\alpha^\pm)_{\Gamma_K^\pm} \hookrightarrow \mathrm{H}^2(G_{K,\Sigma}, W_\alpha).$$

Since the $p$-adic representation $V_{\alpha^{-1}}$ is pure of weight $-1$, we have $\mathrm{H}^2(K_w, W_\alpha) = \mathrm{H}^0(K_w, T_{\alpha^{-1}})^\vee = 0$ for all $w \in \Sigma$, and so $\mathrm{H}^2(G_{K,\Sigma}, W_\alpha) = Ш^2_\Sigma(K, W_\alpha)$ which by Poitou–Tate duality is dual to $Ш^1_\Sigma(K, T_{\alpha^{-1}})$. However, from $E(K)[p] = 0$ the group $Ш^1_\Sigma(K, T_{\alpha^{-1}})$ is torsion-free, and from our assumption on $\alpha$ it is also of $\mathbb{Z}_p$-corank 0. Hence $Ш^1_\Sigma(K, T_{\alpha^{-1}}) = 0$, so also $\mathrm{H}^2(G_{K,\Sigma}, W_\alpha) = 0$, and the vanishing of $\mathrm{H}^1(G_{K,\Sigma}, M_\alpha^\pm)_{\Gamma_K^\pm}$ follows.

This shows part (ii), and the vanishing of $\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, M_\alpha^\pm)_{\Gamma_K^\pm}$ for any $S' \subset \Sigma$ as in part (iii) then follows from the exact sequence

$$\mathrm{H}^1(G_{K,\Sigma}, W) = \mathrm{H}^1(G_{K,\Sigma}, M_\alpha^\pm)^{\Gamma_K^\pm} \xrightarrow{\lambda} \mathcal{P}_{\mathrm{Gr}}(M_\alpha^\pm; S')^{\Gamma_K^\pm} \to \mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, M_\alpha^\pm)_{\Gamma_K^\pm} \to \mathrm{H}^1(K^\Sigma/K, M_\alpha^\pm)_{\Gamma_K^\pm},$$

in which the map $\lambda$ is surjective, being the composition of the restriction map $\mathrm{H}^1(G_{K,\Sigma}, W_\alpha) \to \mathcal{P}_{\mathrm{Gr}}(W_\alpha; S')$ (whose cokernel naturally injects into the dual of $\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, T_\alpha) = 0$) and the natural map $\mathcal{P}_{\mathrm{Gr}}(W_\alpha; S') \to \mathcal{P}_{\mathrm{Gr}}(M_\alpha^\pm; S')^{\Gamma_K^\pm}$, whose surjectivity follows from the fact that for $w \in \Sigma$, the local Galois group $\mathrm{Gal}(K^\pm_{\infty,\eta}/K_w)$ (for any $\eta | w$ in $K^\pm_\infty$) is either trivial or isomorphic to $\mathbb{Z}_p$, and so has $p$-cohomological dimension $\leq 1$. □

Denoting by $\mathcal{L} \mapsto \mathcal{L}^\pm$ the natural projection $\Lambda_K \to \Lambda_K^\pm$, the equality

$$\mathcal{L}_p^{\mathrm{PR}}(E(\alpha)/K)^{+,S'}(0) = \mathcal{L}_p^{\mathrm{PR}}(E(\alpha)/K)^{-,S'}(0)$$

is clear, reflecting the fact that the trivial character is both cyclotomic and anticyclotomic. The next important result (which we shall only need for $S' = \emptyset$) is a parallel equality for characteristic power series.

**Proposition 3.3.2.** *Suppose $E(K)[p] = 0$ and $\alpha : \Gamma_K^- \to R^\times$ is such that the conditions in Lemma 3.3.1 hold. Then the Selmer groups $\mathfrak{X}^{S'}_{\mathrm{Gr}}(E(\alpha)/K^+_\infty)$ and $\mathfrak{X}^{S'}_{\mathrm{Gr}}(E(\alpha)/K^-_\infty)$ are torsion over $\Lambda_K^+$ and $\Lambda_K^-$, respectively, where $S' \subset \Sigma$ is any subset consisting of primes away from $p$. Furthermore, we have the equality up to a $p$-adic unit:*

$$\mathcal{F}^{S'}_{\mathrm{Gr}}(E(\alpha)/K^+_\infty)(0) \sim_p \mathcal{F}^{S'}_{\mathrm{Gr}}(E(\alpha)/K^-_\infty)(0),$$

*where $\mathcal{F}^{S'}_{\mathrm{Gr}}(E(\alpha)/K^\pm_\infty) \in \Lambda^\pm_{K,R}$ is any characteristic power series for $\mathfrak{X}^{S'}_{\mathrm{Gr}}(E(\alpha)/K^\pm_\infty)$.*

*Proof.* By Poitou–Tate duality, the cokernel of the global-to-local map in the defining exact sequence

$$0 \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, W_\alpha) \to \mathrm{H}^1(G_{K,\Sigma}, W_\alpha) \to \mathcal{P}_{\mathrm{Gr}}(W_\alpha; \emptyset)$$

injects into the Pontryagin dual of the Selmer group $\mathrm{H}^1_{\mathcal{F}^*_{\mathrm{Gr}}}(K, T_{\alpha^{-1}})$ dual to $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, W_\alpha)$, defined by the local conditions given by the orthogonal complement of those in $\mathcal{P}_{\mathrm{Gr}}(W_\alpha; \emptyset)$ under local Tate duality. Since this dual Selmer group is torsion-free by the assumption $E(K)[p] = 0$, and it follows from part (i) of Lemma 3.3.1 and the finiteness of $\mathrm{H}^1(K_w, T_{\alpha^{-1}})$ for finite primes $w \nmid p$ that it has finite order, we conclude that the above global-to-local map is surjective. It is then immediate that for any $S'$ as in the statement, we have an analogous exact sequence

$$0 \to \mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, W_\alpha) \to \mathrm{H}^1(G_{K,\Sigma}, W_\alpha) \to \mathcal{P}_{\mathrm{Gr}}(W_\alpha; S') \to 0.$$

A variant of Mazur's control theorem shows that the natural restriction map

$$\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, W_\alpha) \to \mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, M_\alpha^\pm)^{\Gamma_K^\pm}$$

has finite kernel and cokernel. By Lemma 3.3.1 and the above remarks, it follows that $\mathfrak{X}^{S'}_{\mathrm{Gr}}(E(\alpha)/K^\pm_\infty)$ is $\Lambda_K^\pm$-torsion (for both choices of sign $\pm$), and together with the general result [Gre99, Lem. 4.2] for the $\Gamma_K^\pm$-Euler characteristic of $\mathcal{F}^{S'}_{\mathrm{Gr}}(E(\alpha)/K^\pm_\infty)$ we obtain the equality up to a $p$-adic unit:

$$\mathcal{F}^{S'}_{\mathrm{Gr}}(E(\alpha)/K^\pm_\infty)(0) \sim_p \#\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, M_\alpha^\pm)^{\Gamma_K^\pm}. \tag{3.4}$$

Now, from the Snake Lemma applied to the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, W_\alpha) & \longrightarrow & \mathrm{H}^1(K^\Sigma/K, W_\alpha) & \longrightarrow & \mathcal{P}_{\mathrm{Gr}}(W_\alpha; S') & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle s^\pm} & & \downarrow{\scriptstyle h^\pm} & & \downarrow{\scriptstyle r^\pm} & & \\ 0 & \longrightarrow & \mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, M_\alpha^\pm)^{\Gamma_K^\pm} & \longrightarrow & \mathrm{H}^1(K^\Sigma/K, M_\alpha^\pm)^{\Gamma_K^\pm} & \longrightarrow & \mathcal{P}_{\mathrm{Gr}}(M_\alpha^\pm; S')^{\Gamma_K^\pm}, & & \end{array}$$

we obtain

$$\#\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, M_\alpha^\pm)^{\Gamma_K^\pm} = \#\mathrm{H}^1_{\mathcal{F}^{S'}_{\mathrm{Gr}}}(K, W_\alpha) \cdot \frac{\#\ker(r^\pm)}{\#\ker(h^\pm)}. \tag{3.5}$$

Clearly,

$$\ker(h^\pm) = \mathrm{H}^1(\Gamma_K^\pm, (M_\alpha^\pm)^{G_K}) = (M_\alpha^\pm)^{G_K}/(\gamma^\pm - 1)(M_\alpha^\pm)^{G_K} = \mathrm{H}^0(K_\infty^\pm, W_\alpha),$$

and this vanishes by our assumptions. On the other hand, since we assume that every finite prime $w \in \Sigma$ splits in $K$, the argument in the proof of [JSW17, Prop. 3.3.7] (but noting that here the roles $v$ and $\bar{v}$ are reversed) shows that for both choices of sign $\pm$, the order of $\ker(r^\pm)$ is given

$$\#\ker(r^\pm) = \#\mathrm{H}^0(K_v, W_{\alpha^{-1}})^2 \cdot \prod_{w \in \Sigma \smallsetminus S', w \nmid p} c_w^{(p)}(W_\alpha),$$

where $c_w^{(p)} = \#\mathrm{H}^1_{\mathrm{ur}}(K_w, W_\alpha)$ is the $p$-part of the local Tamagawa number of $W_\alpha$ at $w$. Thus the value in (3.5) is the same for both choices of sign $\pm$, and together with (3.4) this yields the result. □

3.3.2. *Ancillary results for $\mathfrak{X}_{\mathrm{ord}}(E(\alpha)/K_\infty^+)$.* Finally, in this section we prove a congruence relation modulo $\varpi^m$ for the (characteristic power series of the) Selmer groups $\mathfrak{X}^S_{\mathrm{ord}}(E(\alpha)/K_\infty^+)$ and $\mathfrak{X}^S_{\mathrm{ord}}(E/K_\infty^+)$, where $\alpha$ is an anticyclotomic character as above such that $\alpha \equiv 1 \mod \varpi^m$. We start with the following preliminary lemma.

**Lemma 3.3.3.** *Assume that $E(K)[p] = 0$ and that $\mathfrak{X}^{S'}_{\mathrm{ord}}(E(\alpha)/K_\infty^+)$ is $\Lambda^+_{K,R}$-torsion, where $S' \subset \Sigma$ is a subset consisting of primes away from $p$. Then $\mathfrak{X}^{S'}_{\mathrm{ord}}(E(\alpha)/K_\infty^+)$ has no nonzero finite $\Lambda^+_{K,R}$-submodules.*

*Proof.* This is shown in [Gre99, Prop. 4.14] when $\alpha = 1$ and $S' = \emptyset$, and the general case follows from a slight variation of the same arguments (see e.g. [Ski16, Prop. 2.3.3]). Alternatively, this can be seen as a special case of Greenberg's results [Gre16]. □

Put

$$S = \Sigma \smallsetminus \{p, \infty\},$$

which as above we shall view as a set of primes of $\mathbb{Q}$ or of $K$ according to context. The next important result is an algebraic counterpart of Lemma 2.5.1.

**Proposition 3.3.4.** *Assume that $E(K)[p] = 0$, that $\mathfrak{X}^S_{\mathrm{ord}}(E(\alpha)/K_\infty^+)$ is $\Lambda^+_{K,R}$-torsion, and that $\mathfrak{X}^S_{\mathrm{ord}}(E/K_\infty^+)$ is $\Lambda^+_K$-torsion. If $\alpha \equiv 1 \pmod{\varpi^m}$, then there are suitable characteristic power series $\mathcal{F}^S_{\mathrm{ord}}(E(\alpha)/K_\infty^+)$ and $\mathcal{F}^S_{\mathrm{ord}}(E/K_\infty^+)$ for the modules $\mathfrak{X}^S_{\mathrm{ord}}(E(\alpha)/K_\infty^+)$ and $\mathfrak{X}^S_{\mathrm{ord}}(E/K_\infty^+)$, respectively, such that*

$$\mathcal{F}^S_{\mathrm{ord}}(E(\alpha)/K_\infty^+) \equiv \mathcal{F}^S_{\mathrm{ord}}(E/K_\infty^+) \pmod{\varpi^m}.$$

*Proof.* Since $\mathfrak{X}^S_{\mathrm{ord}}(E(\alpha)/K_\infty^+)$ and $\mathfrak{X}^S_{\mathrm{ord}}(E/K_\infty^+)$ have no nonzero finite $\Lambda^+_K$-submodules by Lemma 3.3.3, their characteristic ideals are the same as their Fitting ideals (see [Ski16, Lem. 2.3.4(ii)]), so to prove the result it suffices to show that

$$\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{ord}}}(K, M)[\varpi^m] \simeq \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{ord}}}(K, M_\alpha)[\varpi^m], \tag{3.6}$$

where $M = T_p E \widehat{\otimes}_{\mathbb{Z}_p} (\Lambda^+_{K,R})^\vee$ and $M_\alpha = T_p E(\alpha) \widehat{\otimes}_{\mathbb{Z}_p} (\Lambda^+_K)^\vee$. By the assumption $E(K)[p] = 0$, the natural maps

$$\mathrm{H}^1(G_{K,\Sigma}, M[\varpi^m]) \to \mathrm{H}^1(G_{K,\Sigma}, M)[\varpi^m], \quad \mathrm{H}^1(G_{K,\Sigma}, M_\alpha[\varpi^m]) \to \mathrm{H}^1(G_{K,\Sigma}, M_\alpha)[\varpi^m]$$

are isomorphisms. Moreover, since $p \nmid N$, for any $w|p$ the restriction map $\mathrm{H}^1(K_w, M) \to \mathrm{H}^1(I_w, M)$ is an injection. Thus $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{ord}}}(K, M)[\varpi^m]$ is naturally identified with the kernel of the restriction map

$$\mathrm{H}^1(G_{K,\Sigma}, M[\varpi^m]) \to \prod_{w|p} \mathrm{H}^1(I_w, M^-),$$

which factors through $\mathrm{H}^1(G_{K,\Sigma}, M[\varpi^m]) \to \prod_{w|p} \mathrm{H}^1(I_w, M^-[\varpi^m])$. Here we put $M^- = (T_pE/\mathrm{Fil}_w^+ T_pE) \otimes (\Lambda_K^+)^\vee$. Since the kernel of the natural map $\mathrm{H}^1(I_w, M^-[\varpi^m]) \to \mathrm{H}^1(I_w, M^-)$ is given by $(M^-)^{I_w}/p^m(M^-)^{I_w}$, and this is zero since $(M^-)^{I_w} \simeq \mathrm{Hom}_{\mathrm{cts}}(R, \mathbb{Q}_p/\mathbb{Z}_p)$ is $p$-divisible, we conclude that

$$\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{ord}}}(K, M)[\varpi^m] = \ker\left(\mathrm{H}^1(G_{K,\Sigma}, M[\varpi^m]) \to \prod_{w|p} \mathrm{H}^1(I_w, M^-[\varpi^m])\right).$$

Letting $M_\alpha^- = (T_pE(\alpha)/\mathrm{Fil}_w^+ T_pE(\alpha)) \otimes (\Lambda_K^+)^\vee$ we similarly find $(M_\alpha^-)^{I_w} \simeq \mathrm{Hom}_{\mathrm{cts}}(R, \mathbb{Q}_p/\mathbb{Z}_p)$, noting that after restriction to $G_{K_{\infty,w}^+}$ the character $\alpha$ becomes unramified, and so $(M_\alpha^-)^{I_w}/p^m(M_\alpha^-)^{I_w} = 0$ and $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{ord}}}(K, M_\alpha)[\varpi^m]$ is identified with the kernel of the restriction map

$$\mathrm{H}^1(G_{K,\Sigma}, M_\alpha[\varpi^m]) \to \prod_{w|p} \mathrm{H}^1(I_w, M_\alpha^-[\varpi^m]).$$

Since $M_\alpha[\varpi^m] = M[\varpi^m]$, this proves (3.6) and yields the result. □

## 4. Beilinson–Flach classes

Let $f = \sum_{n=1}^\infty a_n q^n \in S_2(\Gamma_0(N))$ be a newform with Fourier coefficients in $\mathbb{Q}$, and fix a prime $p \nmid 2N$. We denote by $Y_1(N)$ the modular curve of level $\Gamma_1(N)$. The $p$-adic Galois representation $V_f$ associated to $f$ can be geometrically realized as the maximal quotient of $\mathrm{H}^1_{\text{ét}}(\overline{Y_1(N)}, \mathbb{Q}_p)(1)$ on which the Hecke operators $T_n$ acts as $a_n$. (Note that this is denoted $V_{\mathbb{Q}_p}(f)^*$ in [LLZ14, Def. 6.3], and corresponds to $V_{\mathbb{Q}_p}(f)(1)$ in the notations of [Kat04].) Let $T_f$ be the $\mathbb{Z}_p$-submodule $V_f$ generated by the image of $\mathrm{H}^1_{\text{ét}}(\overline{Y_1(N)}, \mathbb{Z}_p)(1)$, which is a $G_{\mathbb{Q}}$-stable $\mathbb{Z}_p$-lattice in $V_f$.

We assume that $f$ is ordinary at $p$, i.e., $a_p \in \mathbb{Z}_p^\times$, so there is a $G_p$-stable filtration

$$0 \to T_f^+ \to T_f \to T_f^- \to 0$$

with $T_f^\pm$ free rank one $\mathbb{Z}_p$-modules with the $G_p$-action on $T_f^-$ given by the unramified character sending an arithmetic Frobenius to the $p$-adic unit root of $x^2 - a_p x + p$. Replacing $\mathrm{Fil}_w^+(T_pE)$ with $T_f^+$ we can define the ordinary local condition for $T_f$ as in Definition 3.1.1.

Let $K$ be an imaginary quadratic field satisfying (spl). In this section we introduce the special case of the Beilinson–Flach classes of [KLZ17] that will be needed for our arguments, and deduce some applications.

4.1. **Reciprocity laws.** Let $\boldsymbol{g} \in \Lambda_{\boldsymbol{g}}[\![q]\!]$ be the CM Hida family from §2.4, and fix a character $\alpha : \Gamma_K \to R^\times$ with values in the ring of integers of a finite extension $\Phi/\mathbb{Q}_p$. With a slight abuse of notation, we continue to denote by $\Lambda_K$ the Iwasawa algebra $R[\![\Gamma_K]\!]$ and by $\Lambda_{\boldsymbol{g}}$ the extension of scalars $\Lambda_{\boldsymbol{g}} \otimes_{\mathbb{Z}_p} R$.

Let $I_f \subset \mathbb{Q}_p$ be the image of the unique Hecke-equivariant map $M_2(\Gamma_0(N), \mathbb{Z}_p) \to \mathbb{Q}_p$, with the Hecke action on $\mathbb{Q}_p$ such that $T_n$ acts as multiplication by $a_n$, that sends $f$ to 1. Then $I_f$ is a free $\mathbb{Z}_p$-module of rank one. We similarly define $I_{\boldsymbol{g}} \subset \mathrm{Frac}(\Lambda_{\boldsymbol{g}})$. Note that $I_{\boldsymbol{g}}$ is a finitely-generated $\Lambda_{\boldsymbol{g}}$-module.

**Theorem 4.1.1.** *There exists a class*

$$BF_\alpha \in \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord,rel}}}(K, T_f(\alpha)\widehat{\otimes}\Lambda_K)$$

*and injective $\Lambda_K$-linear maps with pseudo-null cokernel*

$$\widetilde{\mathrm{Col}}_f : \mathrm{H}^1(K_{\bar v}, T_f^-(\alpha)\widehat{\otimes}\Lambda_K) \to I_f\widehat{\otimes}\Lambda_K, \quad \widetilde{\mathrm{Col}}_{\boldsymbol{g}} : \mathrm{H}^1(K_v, T_f^+(\alpha)\widehat{\otimes}\Lambda_K) \to I_{\boldsymbol{g}}\widehat{\otimes}\Lambda_K,$$

*satisfying:*

(a) $\widetilde{\mathrm{Col}}_f(p^-(\mathrm{loc}_{\bar v}(BF_\alpha))) = \mathcal{L}_p(f(\alpha)/K, \Sigma^{(1)})$, *where $p^-(\mathrm{loc}_{\bar v}(BF_\alpha))$ is the natural image of $\mathrm{loc}_{\bar v}(BF_\alpha)$ in $\mathrm{H}^1(K_{\bar v}, T_f^-(\alpha)\widehat{\otimes}\Lambda_K)$;*

(b) $\mathrm{loc}_v(BF_\alpha) \in \mathrm{H}^1(K_v, T_f^+(\alpha)\widehat{\otimes}\Lambda_K) \subset \mathrm{H}^1(K_v, T_f(\alpha)\widehat{\otimes}\Lambda_K)$, *and $\widetilde{\mathrm{Col}}_{\boldsymbol{g}}(\mathrm{loc}_v(BF_\alpha)) = \mathcal{L}_p(f(\alpha)/K, \Sigma^{(2')})$.*

*Proof.* This is proved in [BST21, §5], where it is deduced from results in [KLZ17] in combination with results in [BDP22], though here we have reversed the roles of $v$ and $\bar v$. □

Let $E_1$ be the optimal curve in the isogeny class associated with $f$, in the sense of [Ste89], with optimal parametrization $\pi_1 : X_1(N) \to E_1$. The inclusion $Y_1(N) \hookrightarrow X_1(N)$ identifies the maximal quotient of $\mathrm{H}^1_{\text{ét}}(\overline{X_1(N)}, \mathbb{Q}_p(1))$ on which the Hecke operators $T_n$ acts as $a_n$ with the similar quotient of $\mathrm{H}^1_{\text{ét}}(\overline{Y_1(N)}, \mathbb{Q}_p(1))$, that is, with $V_f$. Via this identification and the parametrization $\pi_1$, the Tate module $T_pE_1$ is identified with

the image of $\mathrm{H}^1_{\text{ét}}(\overline{X_1(N)},\mathbb{Z}_p(1))$ in $V_f$; this is a sublattice of $T_f$. Let $E_\bullet/\mathbb{Q}$ be the elliptic curve in the isogeny class associated with $f$ constructed in [Wut14]. By construction, there is a cyclic isogeny $\phi : E_1 \to E_\bullet$ that is étale in characteristic $p$ and for which the resulting parameterisation $\pi_\bullet = \phi \circ \pi_1 : X_1(N) \to E_\bullet$ identifies $T_pE$ with $T_f$ in $V_f$:

$$T_pE_\bullet = T_f.$$

(cf. Proposition 8 and Theorem 4 of *op. cit.*).

**Lemma 4.1.2.** *We have* $\deg(\pi_\bullet)I_f = \mathbb{Z}_p$.

*Proof.* Let $\omega_{E_\bullet}$ (resp. $\omega_{E_1}$) be a Néron differential for $E_\bullet$ (resp. $E_1$). Then

$$\pi_{\bullet,*}\pi_\bullet^*\omega_{E_\bullet} = \deg(\pi_\bullet)\omega_{E_\bullet}.$$

As the isogeny $\phi$ is étale, $\phi^*\omega_{E_\bullet} = u_1\omega_{E_1}$ for some $u_1 \in \mathbb{Z}_p^\times$. Similarly, $\pi_1^*\omega_{E_1} = c_1\omega_f$ for some $c_1 \in \mathbb{Z}_p^\times$, as $p \nmid 2N$. Hence, $\pi_{\bullet,*}\omega_f = u_1c_1\deg(\pi_\bullet)\omega_{E_\bullet}$ and so it suffices to show that $\pi_{\bullet,*}\omega_f = a\omega_{E_\bullet}$ for some $a \in \mathbb{Z}_p$ such that $aI_f = \mathbb{Z}_p$.

As $E_\bullet$ has ordinary reduction at the prime $p$, the induced map $\mathrm{H}^1_{\text{ét}}(\overline{Y_1(N)},\mathbb{Z}_p(1)) \twoheadrightarrow T_f = T_pE_\bullet$ factors through projection to the ordinary summand $\mathcal{H}^{\mathrm{ord}} := e_{\mathrm{ord}}\mathrm{H}^1_{\text{ét}}(\overline{Y_1(N)},\mathbb{Z}_p(1))$. There is a corresponding commutative diagram

$$\begin{array}{ccccc}
\mathcal{H}^+ & \hookrightarrow & \mathcal{H}^{\mathrm{ord}} & \twoheadrightarrow & \mathcal{H}^- \\
\downarrow & & \downarrow & & \downarrow \\
T_f^+ & \hookrightarrow & T_f & \twoheadrightarrow & T_f^-
\end{array}$$

of $G_{\mathbb{Q}_p}$-modules, where $\mathcal{H}^+$ (resp. $\mathcal{H}^-$) is the maximal submodule (resp. quotient) on which the inertia group $I_p$ acts non-trivially (resp. trivially); this non-trivial action is via the cyclotomic character. The middle arrow is the defining projection, which induces the other two maps.

Since $p \nmid 2N$, the integral de Rham - étale comparison isomorphisms (we need the log version for the open curve $Y_1(N)$) induce compatible identifications

$$e_{\mathrm{ord}}\mathrm{H}^0(\Omega_{X_1(N)/\mathbb{Z}_p}(\log(\mathrm{cusps})) = e_{\mathrm{ord}}M_2(\Gamma_1(N)) \simeq \mathcal{H}^-$$

and

$$M(f) \simeq T_f^- = T_pE_\bullet^- \simeq \mathrm{H}^0(\Omega_{E_\bullet/\mathbb{Z}_p}) = \mathbb{Z}_p\omega_{E_\bullet}.$$

Via these, $\pi_{\bullet,*}\omega_f$ is identified with the image of $f$ in $M(f)$. Since $\omega_{E_\bullet}$ is identified with a $\mathbb{Z}_p$-generator of $M(f)$ and we have an isomorphism of rank one $\mathbb{Z}_p$-modules $M(f) \simeq I_f$, $f \mapsto 1$, it follows that $\pi_{\bullet,*}\omega_f = a\omega_{E_\bullet}$ for some $a \in \mathbb{Z}_p$ such that $aI_f = \mathbb{Z}_p$, as desired. □

Recall the $\alpha$-twisted versions of the two-variable $p$-adic $L$-functions $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)$ and $\mathcal{L}_p^{\mathrm{Gr}}(f/K)$ introduced in Definitions 2.2.2 and 2.4.3, respectively.

**Corollary 4.1.3.** *There are injective $\Lambda_K$-linear maps with pseudo-null cokernel*

$$\mathrm{Col}_{E_\bullet} : \mathrm{H}^1(K_{\bar v},(T_pE_\bullet)^-(\alpha)\widehat{\otimes}\Lambda_K) \to \Lambda_K, \quad \mathrm{Col}_{\boldsymbol{g}} : \mathrm{H}^1(K_v,(T_pE_\bullet)^+(\alpha)\widehat{\otimes}\Lambda_K) \to \Lambda_K^{\mathrm{ur}},$$

*such that*

$$\mathrm{Col}_{E_\bullet}(p^-(\mathrm{loc}_{\bar v}(BF_\alpha))) = \mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K), \quad \mathrm{Col}_{\boldsymbol{g}}(\mathrm{loc}_v(BF_\alpha)) = \mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K).$$

*Proof.* By [Maz78, Cor. 4.1] and [GV00, Prop. 3.3], the Manin constant associated to the modular parametrization $\pi_\bullet : X_1(N) \to E_\bullet$ is a $p$-adic unit, so setting

$$\mathrm{Col}_{E_\bullet} := \deg(\pi_\bullet)\cdot H_p(f)\cdot\widetilde{\mathrm{Col}}_f,$$

the first part of the result follows from Theorem 4.1.1 and Lemma 4.1.2. On the other hand, as explained in the proof of Lemma 2.4.4, the characteristic power series $H(\boldsymbol{g})$ of the CM family $\boldsymbol{g}$ divides $h_K\cdot\mathcal{L}_v(K)^-$. Since on the other hand by [Hid07, Cor. 5.6] $H(\boldsymbol{g})$ is divisible by $h_K\cdot\mathcal{L}_v(K)^-$, it follows that the congruence ideal of $\boldsymbol{g}$ is generated by $h_K\cdot\mathcal{L}_v(K)^-$. Thus setting

$$\mathrm{Col}_{\boldsymbol{g}} := h_K\cdot\mathcal{L}_v(K)^-\cdot\widetilde{\mathrm{Col}}_{\boldsymbol{g}}$$

the second part of the result follows from Theorem 4.1.1. □

4.2. **Iwasawa main conjectures.** One key application of Corollary 4.1.3 is in relating different instances of the main conjectures for the cyclotomic $\mathbb{Z}_p$-extension $K_\infty^+/K$. Similarly as in §3.1, for any elliptic curve $E/\mathbb{Q}$ we put

$$\mathfrak{X}_{\mathrm{Gr}}(E(\alpha)/K_\infty^+) := \mathfrak{X}_{\mathrm{rel,str}}(E(\alpha)/K_\infty^+), \quad \mathfrak{S}_{\mathrm{ord,rel}}(E(\alpha)/K_\infty^+) = \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord,rel}}}(K, T_pE(\alpha)\otimes\Lambda_K^+),$$

etc.. Write $BF_\alpha^+$ for the image of the class $BF_\alpha$ of Theorem 4.1.1 under the natural projection

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord,rel}}}(K, (T_pE_\bullet)(\alpha)\widehat{\otimes}\Lambda_K) \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{ord,rel}}}(K, (T_pE_\bullet)(\alpha)\widehat{\otimes}\Lambda_K^+),$$

so we have $BF_\alpha^+ \in \mathfrak{S}_{\mathrm{ord,rel}}(E_\bullet(\alpha)/K_\infty^+)$.

**Proposition 4.2.1.** *Suppose $E_\bullet(K)[p] = 0$ and that $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^+$ and $\mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^+$ are both nonzero. Then the following are equivalent:*

(i) *$\mathfrak{S}_{\mathrm{ord,rel}}(E_\bullet(\alpha)/K_\infty^+)$ has $\Lambda_K^+$-rank one, $\mathfrak{X}_{\mathrm{ord,str}}(E_\bullet(\alpha^{-1})/K_\infty^+)$ is $\Lambda_K^+$-torsion, and*

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord,str}}(E_\bullet(\alpha^{-1})/K_\infty^+)\big) \supset \mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{S}_{\mathrm{ord,rel}}(E_\bullet(\alpha)/K_\infty^+)/\Lambda_K^+BF_\alpha^+\big).$$

(ii) *$\mathfrak{S}_{\mathrm{str,rel}}(E_\bullet(\alpha)/K_\infty^+)$ and $\mathfrak{X}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^+)$ are both $\Lambda_K^+$-torsion, and*

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^+)\big)\Lambda_K^{+,\mathrm{ur}} \supset \big(\mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^+\big).$$

(iii) *$\mathfrak{S}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)$ and $\mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)$ are both $\Lambda_K^+$-torsion, and*

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)\big) \supset \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^+\big).$$

*The same result holds for the opposite divisibilities.*

*Proof.* This is a well-known consequence of Poitou–Tate duality and the reciprocity laws of Theorem 4.1.1, but we provide the details for the convenience of the reader. Below we set $\mathfrak{S}_{\mathrm{str,rel}} = \mathfrak{S}_{\mathrm{str,rel}}(E_\bullet(\alpha)/K_\infty^+)$, $\mathfrak{X}_{\mathrm{Gr}} = \mathfrak{X}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^+)$, etc. for the ease of notation; and similarly, $\mathfrak{X}_{\mathrm{ord}}(\alpha^{-1}) = \mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha^{-1})/K_\infty^+)$, $\mathfrak{X}_{\mathrm{Gr}}(\alpha^{-1}) = \mathfrak{X}_{\mathrm{Gr}}(E_\bullet(\alpha^{-1})/K_\infty^+)$, etc.. Note that, since $\alpha^\tau = \alpha^{-1}$ and $(T_pE_0\otimes(\Lambda_K^+)^\vee)^\tau \simeq T_pE_0\otimes(\Lambda_K^+)^\vee$, the action of complex conjugation gives rise to isomorphisms of $\Lambda_K^+$-modules:

$$\mathfrak{X}_{\mathrm{Gr}}(\alpha^{-1}) \simeq \mathfrak{X}_{\mathrm{Gr}}, \quad \mathfrak{X}_{\mathrm{ord}}(\alpha^{-1}) \simeq \mathfrak{X}_{\mathrm{ord}} \quad \mathfrak{X}_{\mathrm{ord,str}}(\alpha^{-1}) \simeq \mathfrak{X}_{\mathrm{str,ord}}. \tag{4.1}$$

For the equivalence (i) ⇔ (ii) consider the exact sequence

$$0 \to \mathfrak{S}_{\mathrm{str,rel}} \to \mathfrak{S}_{\mathrm{ord,rel}} \to \mathrm{H}^1_{\mathrm{ord}}(K_v, T_pE_\bullet(\alpha)\otimes\Lambda_K^+) \to \mathfrak{X}_{\mathrm{Gr}}(\alpha^{-1}) \to \mathfrak{X}_{\mathrm{ord,str}}(\alpha^{-1}) \to 0. \tag{4.2}$$

In both cases, we see that $\mathfrak{S}_{\mathrm{str,rel}}$ is $\Lambda_K^+$-torsion, hence trivial (by the assumption $E_\bullet(K)[p] = 0$), and (4.2) yields the exact sequence

$$0 \to \mathfrak{S}_{\mathrm{ord,rel}}/\Lambda_K^+BF_\alpha^+ \to \mathrm{H}^1_{\mathrm{ord}}(K_v, T_pE_\bullet(\alpha)\otimes\Lambda_K^+)/\Lambda_K^+\,\mathrm{loc}_v(BF_\alpha^+) \to \mathfrak{X}_{\mathrm{Gr}}(\alpha^{-1}) \to \mathfrak{X}_{\mathrm{ord,str}}(\alpha^{-1}) \to 0.$$

Since by Corollary 4.1.3 the second term in this exact sequence is pseudo-isomorphic—via the map $\mathrm{Col}_{\boldsymbol{g}}$—to $\Lambda_K^{+,\mathrm{ur}}/(\mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^+)$, the equivalence (i) ⇔ (ii) follows from this, the multiplicativity of characteristic ideals, and the isomorphisms (4.1). On the other hand, for the equivalence (i) ⇔ (iii) consider the exact sequence

$$0 \to \mathfrak{S}_{\mathrm{ord}} \to \mathfrak{S}_{\mathrm{ord,rel}} \to \mathrm{H}^1_{/\mathrm{ord}}(K_{\bar v}, T_pE_\bullet(\alpha)\otimes\Lambda_K^+) \to \mathfrak{X}_{\mathrm{ord}}(\alpha^{-1}) \to \mathfrak{X}_{\mathrm{ord,str}}(\alpha^{-1}) \to 0, \tag{4.3}$$

where

$$\mathrm{H}^1_{/\mathrm{ord}}(K_{\bar v}, T_pE_\bullet(\alpha)\otimes\Lambda_K^+) := \frac{\mathrm{H}^1(K_{\bar v}, T_pE_\bullet(\alpha)\otimes\Lambda_K^+)}{\mathrm{H}^1_{\mathrm{ord}}(K_{\bar v}, T_pE_\bullet(\alpha)\otimes\Lambda_K^+)} \simeq \mathrm{H}^1(K_{\bar v}, T_f^-(\alpha)\widehat{\otimes}\Lambda_K).$$

Similarly as before, in both cases we find $\mathfrak{S}_{\mathrm{ord}}$ is $\Lambda_K^+$-torsion, so from (4.3) we obtain the exact sequence

$$0 \to \mathfrak{S}_{\mathrm{ord,rel}}/\Lambda_K^+BF_\alpha^+ \to \mathrm{H}^1_{/\mathrm{ord}}(K_{\bar v}, T_pE_\bullet\otimes\Lambda_K^+)/\Lambda_K^+p^-(\mathrm{loc}_{\bar v}(BF_\alpha^+)) \to \mathfrak{X}_{\mathrm{ord}}(\alpha^{-1}) \to \mathfrak{X}_{\mathrm{ord,str}}(\alpha^{-1}) \to 0.$$

Since by Corollary 4.1.1 the second term in this exact sequence is pseudo-isomorphic—via the map $\mathrm{Col}_{E_\bullet}$—to $\Lambda_K^+/(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^+)$, taking characteristic ideals and applying (4.1) the result follows. □

4.3. **The Beilinson–Flach Euler system divisibility.** In the case $\alpha = 1$, the "upper bound" divisibility in Conjecture 3.1.3 for $\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)$ can be deduced from Kato's work together with Proposition 3.2.1. For our later arguments (especially for elliptic curves $E/\mathbb{Q}$ of rank $> 1$), we will need a similar divisibility for a twist by a non-trivial character $\alpha$ of $\Gamma_K^-$, a result that we shall deduce from Proposition 4.2.1 and the next result.

**Theorem 4.3.1.** *Suppose $\alpha \neq 1$ is a non-trivial character of $\Gamma_K^-$ and $BF_\alpha^+ \neq 0$. Then $\mathfrak{X}_{\mathrm{ord,str}}(E_\bullet(\alpha^{-1})/K_\infty^+)$ is $\Lambda_K^+$-torsion, $\mathfrak{S}_{\mathrm{ord,rel}}(E_\bullet(\alpha)/K_\infty^+)$ has $\Lambda_K^+$-rank one, and we have the divisibility*

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord,str}}(E_\bullet(\alpha^{-1})/K_\infty^+)\big) \supset \mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{S}_{\mathrm{ord,rel}}(E_\bullet(\alpha)/K_\infty^+)/\Lambda_K^+ BF_\alpha^+\big)$$

*in $\Lambda_K^+ \otimes \mathbb{Q}_p$.*

*Proof.* As a consequence of the cyclotomic Euler system constructed in [KLZ17, Thm. 8.1.3] attached to the pair $(f, \boldsymbol{g})$, there exists an integer $r \geq 0$ such that $\pi^r BF_\alpha^+$ extends to a system of cohomology classes

$$BF_{\alpha,m}^+ \in \mathrm{H}^1(K(\mu_m), (T_pE_\bullet)(\alpha)\widehat{\otimes}\Lambda_K^+)$$

indexed by integers $m \geq 1$ coprime to $pcND_K$ for an auxiliary integer $c > 1$ coprime to $6ND_K$ with $BF_{\alpha,1}^+ = \pi^r BF_\alpha^+$ and satisfying the Euler system norm relations. (The $\varpi^r$ appears because the specialization at the character $\alpha$ of the Galois module associated to $\boldsymbol{g}$ in [KLZ17] may not equal $\mathrm{Ind}_K^{\mathbb{Q}}(\alpha)$ but only contain this lattice with finite index.) Thus by the results of [KLZ17, §12], giving in particular a refinement of the results of [Rub00] for Euler systems with a non-trivial local condition at $p$, it suffices to verify that the $G_{\mathbb{Q}}$-module $T := (T_pE_\bullet) \otimes \mathrm{Ind}_K^{\mathbb{Q}}(\alpha)$ satisfies the following hypotheses:

(i) $V = T \otimes \mathbb{Q}_p$ is irreducible as a $\Phi[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})]$-module,
(ii) There exists an element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{p^\infty}))$ such that $\dim_\Phi(V/(\sigma - 1)V) = 1$.

(Note that [KLZ17, Thm. 12.3.4] gives a refinement of [Rub00, Thm. 2.3.3] under the big image hypothesis "Hyp($BI$)" in *op. cit.*; the same methods yield a corresponding refinement of [Rub00, Thm. 2.3.4] under the above hypotheses (i)-(ii).)

But the verification of these hypotheses is standard. Indeed, since our running assumptions imply that the newform $f$ is not of CM-type, hypothesis (i) is clear. On the other hand, hypothesis (ii) follows from [Loe17, Thm. 4.4.1], noting that by [Ser68, §IV.2.2] the quaternion algebra $B_f$ considered in *loc. cit.* can be taken to be split. □

## 5. Interlude: The rank one case and the general strategy

In this section we give a proof of Theorem A under the following two additional hypotheses:

(a) $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/K) = 1$.
(b) The restriction map

$$\mathrm{Sel}_{p^\infty}(E/K) \xrightarrow{\mathrm{loc}_v} E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

is nonzero.

The short argument that follows, albeit independent from the discussion in the later sections, will allow us to motivate the more involved arguments needed for the proof of Theorem A in general, and might provide some orientation to the the reader. Note that under the additional hypotheses (a) and (b), the results in the earlier sections of this paper and those in [CGLS22] suffice for the proof.

Recall that $E_\bullet$ denotes the elliptic curve in the isogeny of $E$ constructed in [Wut14].

*Step 1.* Under the above additional hypotheses, by [CGLS22, Thm. C] the module $\mathfrak{X}_{\mathrm{Gr}}^S(E_\bullet/K_\infty^-)$ is $\Lambda_K^-$-torsion, with

$$\mathrm{ch}_{\Lambda_K^-}\big(\mathfrak{X}_{\mathrm{Gr}}(E_\bullet/K_\infty^-)\big)\Lambda_K^{-,\mathrm{ur}} = \big(\mathcal{L}_p^{\mathrm{BDP}}(f/K)\big). \tag{5.1}$$

Conditions (a) and (b) above correspond to conditions (a) and (b) in Lemma 3.3.1 with $\alpha = 1$, and so we conclude that $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, E_\bullet[p^\infty])$ is finite, and letting $\mathcal{F}_{\mathrm{Gr}}(E_\bullet/K_\infty^-) \in \mathbb{Z}_p[\![T]\!]$ be a characteristic power series for $\mathfrak{X}_{\mathrm{Gr}}(E_\bullet/K_\infty^-)$ we have

$$\mathcal{F}_{\mathrm{Gr}}(E_\bullet/K_\infty^-)(0) \ \sim_p \ \mathcal{L}_p^{\mathrm{BDP}}(f/K)(0) \neq 0, \tag{5.2}$$

where $\sim_p$ denotes equality up to a $p$-adic unit.

*Step 2.* From Kato's result [Kat04, Thm. 17.4] (as refined in [Wut14, Thm. 16] to an integral divisibility in the $p$-Eisenstein case) applied to $E_\bullet$ and $E_\bullet^K$, together with Proposition 2.2.4 and Proposition 3.2.1, we deduce that $\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)$ is $\Lambda_K^+$-torsion, and that we have the divisibility

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)\big) \supset \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+\big) \tag{5.3}$$

in $\Lambda_K^+$. Moreover, the nonvanishing of $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+$ follows from Rohrlich's nonvanishing results [Roh84], while that of $\mathcal{L}_p^{\mathrm{Gr}}(f/K)^+$ follows from (5.2) and Proposition 2.4.5, noting that $\mathcal{L}_p^{\mathrm{Gr}}(f/K)^-(0) = \mathcal{L}_p^{\mathrm{Gr}}(f/K)^+(0)$. Therefore, by Proposition 4.2.1 with $\alpha = 1$ we obtain that $\mathfrak{X}_{\mathrm{Gr}}(E_\bullet/K_\infty^+)$ is $\Lambda_K^+$-torsion, with the divisibility

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{Gr}}(E_\bullet/K_\infty^+)\big) \supset \big(\mathcal{L}_p^{\mathrm{Gr}}(f/K)^+\big) \tag{5.4}$$

in $\Lambda_K^{+,\mathrm{ur}}$.

*Step 3.* For $\mathcal{F}_{\mathrm{Gr}}(E_\bullet/K_\infty^-) \in \mathbb{Z}_p[\![T]\!]$ a characteristic power series for $\mathfrak{X}_{\mathrm{Gr}}^S(E_\bullet/K_\infty^-)$, we have the chain of relations

$$\mathcal{F}_{\mathrm{Gr}}(E_\bullet/K_\infty^+)(0) \sim_p \mathcal{F}_{\mathrm{Gr}}(E_\bullet/K_\infty^-)(0) \sim_p \mathcal{L}_p^{\mathrm{BDP}}(f/K)(0) \sim_p \mathcal{L}_p^{\mathrm{Gr}}(f/K)^-(0) = \mathcal{L}_p^{\mathrm{Gr}}(f/K)^+(0),$$

using Proposition 3.3.2 with $\alpha = 1$ (resp. Proposition 2.2.4) for the first (resp. third) equality up to a $p$-adic unit. We thus conclude that

$$\mathcal{F}_{\mathrm{Gr}}(E_\bullet/K_\infty^+)(0) \sim_p \mathcal{L}_p^{\mathrm{Gr}}(f/K)^+(0) \neq 0,$$

which by easy commutative algebra (see [SU14, Lem. 3.2]) implies that equality holds in (5.4):

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{Gr}}(E_\bullet/K_\infty^+)\big) = \big(\mathcal{L}_p^{\mathrm{Gr}}(f/K)^+\big).$$

By Proposition 4.2.1, it follows that $\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)$ is $\Lambda_K^+$-torsion, with

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)\big) = \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+\big),$$

and by Proposition 3.1.4 the same conclusion holds with $E$ in place of $E_\bullet$. By Proposition 2.2.4 and Proposition 3.2.1, this equality of characteristic ideals together with Kato's divisibility for $E$ yields Theorem A (under the additional hypotheses (a) and (b) above).

In order to obtain Theorem A in general:

- We shall prove Theorem C from the Introduction, removing the assumption $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/K) = 1$ from [CGLS22, Thm. C]. Then, similarly as in *Step 1* above, we shall obtain
$$\mathcal{F}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^-)(0) \sim_p \mathcal{L}_p^{\mathrm{BDP}}(f(\alpha)/K)(0) \neq 0,$$
for any character $\alpha$ of $\Gamma_K^-$ away from the zeros of $\mathcal{L}_p^{\mathrm{BDP}}(f/K)$ (so necessarily $\alpha \neq 1$ if the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/K)$ is greater than 1).
- By arguments similar to those in *Steps 2* and *3* above, but complicated by the need to apply certain congruences and the use of $S$-imprimitive Selmer groups, we will show that for $\alpha$ sufficiently close to 1, the module $\mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)$ is $\Lambda_K^+$-torsion, with
$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)\big) = \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^+\big).$$

From this last equality, we deduce that the original $\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)$ and $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+$ have the same Iwasawa invariants, which together with Kato's work will yield the proof of Theorem A.

## 6. Anticyclotomic main conjecture

The key new result in this section is Theorem 6.1.1. The result is a Kolyvagin system bound complementing [CGLS22, Thm. 3.2.1] for characters $\alpha$ of $\Gamma_K^-$ that are close to 1. We then use this result to obtain a version of [CGLS22, Thm. C] and its corollaries removing the assumption that $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/K) = 1$ (i.e., assumption (Sel) in *loc. cit.*).

Throughout this section, we let $E/\mathbb{Q}$ be an elliptic curve of conductor $N$, $p \nmid 2N$ be a prime of good ordinary reduction for $E$, and $K$ be an imaginary quadratic field of discriminant $D_K$ prime to $Np$. We assume that

$$E(K)[p] = 0, \tag{h1}$$

and denote by $\mathscr{L} = \mathscr{L}_E$ the set of primes $\ell \nmid N$ that are inert in $K$ and satisfy $a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}$, where $a_\ell = \ell + 1 - |\tilde{E}(\mathbb{F}_\ell)|$, and by $\mathscr{N}$ the set of square-free products of primes $\ell \in \mathscr{L}$.

6.1. **A Kolyvagin-style bound for $\alpha \equiv 1 \pmod{\varpi^m}$.** Let $R$ be the ring of integers of some finite extension $\Phi/\mathbb{Q}_p$ and let $\varpi \in R$ be a uniformizer. Let $\mathfrak{m} = (\varpi)$ be the maximal ideal of $R$. Let $\alpha : \Gamma_K^- \to R^\times$ be an anticyclotomic character and $m$ a positive integer such that

$$\alpha \equiv 1 \pmod{\varpi^m}. \tag{6.1}$$

Denote by $\rho_E : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T_pE)$ the representation on the $p$-adic Tate module of $E$, and consider the $G_K$-modules

$$T := T_pE \otimes_{\mathbb{Z}_p} R(\alpha), \quad V := T \otimes_R \Phi, \quad A := T \otimes_R \Phi/R \simeq V/T,$$

where $R(\alpha)$ is the free $R$-module of rank one on which $G_K$ acts via the composition of the projection $G_K \twoheadrightarrow \Gamma_K^-$ with $\alpha$, and the $G_K$-action on $T$ is via $\rho = \rho_E \otimes \alpha$. Let $I_\ell$ be the smallest ideal containing $\ell + 1$ for which the Frobenius element $\mathrm{Frob}_\lambda \in G_{K_\lambda}$ acts trivially on $T/I_\ell T$, where $\lambda \mid \ell \in \mathcal{L}$. For any $k \geqslant 0$, let

$$T^{(k)} = T/\varpi^k T, \quad \mathscr{L}^{(k)} = \{\ell \in \mathscr{L} \colon I_\ell \subset p^k\mathbb{Z}_p\},$$

and let $\mathscr{N}^{(k)}$ be the set of square-free products of primes $\ell \in \mathscr{L}^{(k)}$. We refer the reader to [CGLS22, §3.1] for the definition of the module of Kolyvagin systems $\mathbf{KS}(T, \mathcal{F}_{\mathrm{ord}}, \mathscr{L})$ associated to the triple $(T, \mathcal{F}_{\mathrm{ord}}, \mathscr{L})$ (here and until §6.5, $\mathcal{F}_{\mathrm{ord}}$ denotes the ordinary Selmer structure introduced in [CGLS22, p. 548], which is compatible with the discrete coefficients analogue defined in §3.3 and Definition 3.1.1).

**Theorem 6.1.1.** *There exist non-negative integers $\mathcal{M}$ and $\mathcal{E}$ depending only on $T_pE$ and $\mathrm{rank}_{\mathbb{Z}_p}(R)$ such that if $m \geq \mathcal{M}$ and if there is a Kolyvagin system $\kappa = \{\kappa_n\}_{n \in \mathscr{N}} \in \mathbf{KS}(T, \mathcal{F}_{\mathrm{ord}}, \mathscr{L})$ with $\kappa_1 \neq 0$, then $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T)$ has $R$-rank one and there is a finite $R$-module $M$ such that*

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, A) \simeq \Phi/R \oplus M \oplus M$$

*with*

$$\mathrm{length}_R(M) \leqslant \mathrm{length}_R\big(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K, T)/R \cdot \kappa_1\big) + \mathcal{E}.$$

The 'error term' $\mathcal{E}$ in this theorem is independent of $m$, but that comes at the expense of the result applying only to characters $\alpha$ that are sufficiently close to 1 (as measured by $\mathcal{M}$). The reader may wish to compare this theorem with [CGLS22, Thm. 3.2.1] whose error term $E_\alpha$ is at least as large as $m$ but which also applies to $\alpha$ that are relatively far from 1. Both results are crucial for the proof of Theorem C.

6.2. **Structure of Selmer groups.** In the following we use $\mathcal{F}$ to denote $\mathcal{F}_{\mathrm{ord}}$ for simplicity. For any $k \geq 1$, let $R^{(k)} = R/\mathfrak{m}^k$. We recall the following structure results:

**Lemma 6.2.1.** *For every $n \in \mathscr{N}^{(k)}$ and $0 \leqslant i \leqslant k$ there are natural isomorphisms*

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

*induced by the maps $T^{(k)}/\mathfrak{m}^i T^{(k)} \xrightarrow{\pi^{k-i}} T^{(k)}[\mathfrak{m}^i] \to T^{(k)}$.*

*Proof.* See [CGLS22, Lem. 3.3.1]. □

**Proposition 6.2.2.** *There is an integer $\epsilon \in \{0, 1\}$ such that for all $k$ and every every $n \in \mathscr{N}^{(k)}$ there is an $R^{(k)}$-module $M^{(k)}(n)$ such that*

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

*Proof.* See [CGLS22, Prop. 3.3.2]. □

By Lemma 6.2.1 and (6.1), if $k \geq m$ there is an isomorphism

$$\mathrm{H}^1_{\mathcal{F}(n)}(K, T_E^{(m)}) \simeq \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)})[\mathfrak{m}^m], \tag{6.2}$$

where $T_E^{(m)} = T_p(E) \otimes_{\mathbb{Z}_p} R/\mathfrak{m}^m$. We can then exploit the action of complex conjugation on the left hand side (both $T_E^{(m)}$ and the Selmer structure $\mathcal{F}(n)$ are stable under this action). We make use of this in our subsequent analysis of the structure of the $R$-modules $M(n)$ in terms of Kolyvagin classes.

6.3. **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

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

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

$$e := r(C_1 + C_2).$$

For any finitely-generated torsion $R$-module $M$ and $x \in M$, let

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

The following result is one of the main tools for our proof of Theorem 6.1.1.

**Proposition 6.3.1.** *Let $c^\pm \in \mathrm{H}^1(K, T_E^{(m)})^\pm$. Let $k \geq m$. Then there exist infinitely many primes $\ell \in \mathscr{L}^{(k)}$ such that*

$$\mathrm{ord}(\mathrm{loc}_\ell(c^\pm)) \geqslant \mathrm{ord}(c^\pm) - e.$$

*In particular, $R \cdot \mathrm{loc}_\ell(c^+) + R \cdot \mathrm{loc}_\ell(c^-)$ has an $R$-submodule isomorphic to*

$$R/\mathfrak{m}^{\max\{0,\mathrm{ord}(c^+)-e\}} \oplus R/\mathfrak{m}^{\max\{0,\mathrm{ord}(c^-)-e\}}.$$

*Proof.* The proof of this proposition follows along the lines of that of [CGLS22, Prop. 3.3.6].

Let $u \in \mathbb{Z}_p^\times \cap \mathrm{im}(\rho_E|_{G_{K_\infty}}) = \mathbb{Z}_p^\times \cap \mathrm{im}(\rho_E) \subset \mathbb{Z}_p^\times \cap \mathrm{im}(\rho_E \otimes \alpha)$ (see [CGLS22, Lemma 3.3.3]) be such that $v_p(u-1) = C_1$. Let $L$ be the fixed field of the action of $G_K$ on $T/p^kT$, so $L$ is the composite of the fixed field of the action of $G_K$ on $T_E/p^kT_E$ and the field $K_\alpha$ trivialising $\alpha \mod p^k$. Then there is some $h$ in the center of $\mathrm{Gal}(L/K)$ such that $h$ acts on $T/p^kT$, and hence on $T^{(m)} \simeq T_E^{(m)}$, as multiplication by $u$. The kernel of the restriction map $\mathrm{H}^1(K, T^{(m)}) \to \mathrm{H}^1(L, T^{(m)})$ is $\mathrm{H}^1(L/K, T^{(m)})$ and it follows from the existence of $h$ that the latter is annihilated by $u-1$ (this is essentially Sah's Lemma: if $c : \mathrm{Gal}(L/K) \to T^{(m)}$ is a 1-cocycle, then $c(gh) = c(hg)$ and so $(h-1)c(g) = (g-1)c(h)$ and hence $p^{C_1}c$ is a coboundary). It follows that

$$p^{C_1} \cdot \ker\big(\mathrm{H}^1(K, T_E^{(m)}) \to \mathrm{H}^1(L, T_E^{(m)})\big) = 0. \tag{6.3}$$

Let $d^\pm := \mathrm{ord}(c^\pm) - r(C_1 + C_2)$. If $d^+ = d^- \leq 0$, then there is nothing to prove. So assume at least one of $d^\pm$ is positive. By (6.3), the kernel of the restriction map

$$\mathrm{H}^1(K, T_E^{(m)}) \overset{res}{\to} \mathrm{H}^1(L, T_E^{(m)}) = \mathrm{Hom}_{G_K}(G_L, T_E^{(m)})$$

is annihilated by $p^{C_1} = \varpi^{rC_1}$. Let $f^\pm \in \mathrm{Hom}_{G_K}(G_L, T_E^{(m)})$ be the image of $c^\pm$. We then have

$$\mathrm{ord}(f^\pm) \geq \mathrm{ord}(c^\pm) - rC_1.$$

As $f^\pm(G_L)$ is a $G_K$-submodule, $f^\pm(G_L) = \mathrm{Im}(\rho_E) \cdot f^\pm(G_L)$ and so, by the definition of $C_2$, the image of $f^\pm$ contains $p^{C_2}\,\mathrm{End}(T_p(E)) \cdot f^\pm(G_L)$. Since $\mathrm{ord}(f^\pm) \geq \mathrm{ord}(c^\pm) - rC_1$, it follows that the $R$-span of the image of $f^\pm$ contains $\varpi^{m-\mathrm{ord}(c^\pm)+r(C_1+C_2)}T_E^{(m)}$. Since at least one of $d^+$ and $d^-$ is positive, it follows that at least one of $f^+$ and $f^-$ is non-trivial.

Let $H \subset G_L$ be the intersection of the kernels of $f^+$ and of $f^-$, and let $Z = G_L/H$. Note that $H \neq G_L$ since some $f^\pm$ is non-trivial, so $Z$ is a non-trivial torsion $R$-module. Note also that $Z$ is stable under the action of complex conjugation since each $f^\pm$ is. In particular, $Z$ decomposes into eigenspaces under the action of complex conjugation: $Z = Z^+ \oplus Z^-$.

Let $g^\pm$ be the projection of $f^\pm$ to the summand $(T_E^{(m)})^\pm \cong R/\mathfrak{m}^m$. Then the $R$-span of the image of $g^\pm$ contains an $R$-submodule isomorphic to $R/\mathfrak{m}^{\max\{0,d^\pm\}}$. We have $g^\pm(Z^-) = 0$ since $f^\pm \in \mathrm{Hom}(G_L, E[p^m])^\pm$. So we find $g^\pm(Z) = g^\pm(Z^+)$ and that the $R$-span of $g^\pm(Z^+)$ contains a submodule isomorphic to $R/\mathfrak{m}^{\max\{0,d^\pm\}}$. It follows that $Z^+$ is non-trivial.

If $d^\pm > 0$, let $W_\pm \subset Z^+$ be the proper subgroup such that $g^\pm(W_\pm) = \varpi^{m-(d^\pm-1)}(T_E^{(m)})^\pm$. If $d^\pm \leq 0$, let $W_\pm = 0$. Then both $W_+$ and $W_-$ are proper subgroups of $Z^+$ (since there exists some $z \in Z^+$ such that $g^\pm(z) \in \varpi^{m-d^\pm}(T_E^{(m)})^\pm$). It follows that $W_+ \cup W_- \neq Z^+$. Let $z \in Z^+$, $z \notin W_+ \cup W_-$. By the definition of $W^\pm$, we have

$$\mathrm{ord}(g^\pm(z)) \geq d^\pm. \tag{6.4}$$

Let $M = \overline{\mathbb{Q}}^H$, so $\mathrm{Gal}(M/L) = Z$. Let $g = \tau z \in G_{\mathbb{Q}}$, and let $\ell \nmid Np$ be any prime such that both $c^+$ and $c^-$ are unramified at $\ell$ and $\mathrm{Frob}_\ell = g$ in $\mathrm{Gal}(M/\mathbb{Q})$. The Čebotarev density theorem implies there are infinitely many such primes. Since $Z$ fixes $L$ and since $L$ contains the fixed field of the $G_K$-action on $E[p^k]$, $\mathrm{Frob}_\ell$ acts as $\tau$ on both $E[p^k]$ and $K$. This means that $a_\ell(E) \equiv \ell + 1 \equiv 0 \mod p^k$ and $\ell$ is inert in $K$. Since $L$ also contain the fixed field of $\alpha \mod p^k$, for $\lambda \mid \ell$ a prime of $K$, it follows that $\mathrm{Frob}_\lambda$ acts trivially on $T/p^kT$ and hence that $\ell \in \mathscr{L}^{(k)}$.

Since $\ell$ is inert in $K$, the Frobenius element of $\ell$ in $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ is $\mathrm{Frob}_\ell^2$. Consider the restriction of $c^\pm$ to $K_\ell$. Since $c^\pm$ is unramified at $\ell$, $\mathrm{loc}_\ell(c^\pm)$ is completely determined by the image $c^\pm(\mathrm{Frob}_\ell^2)$ in $T_E^{(m)}/(\mathrm{Frob}_\ell^2 - 1)T_E^{(m)}$. By the choice of $\ell$, $\mathrm{Frob}_\ell^2$ acts trivially on $T_E^{(m)}$, so $T_E^{(m)}/(\mathrm{Frob}_\ell^2 - 1)T_E^{(m)} = T_E^{(m)}$. Moreover, $\mathrm{Frob}_\ell^2 = g^2 = z^2 \in \mathrm{Gal}(M/L)$, so $c^\pm(\mathrm{Frob}_\ell^2) = f^\pm(z^2) = 2g^\pm(z)$, where the second equality follows from the fact that the projection of $f^\pm$ to $(T_E^{(m)})^\mp$ maps $z \in Z^+$ to zero. Since $p$ is odd, (6.4) yields $\mathrm{ord}(\mathrm{loc}_\ell(c^\pm)) = \mathrm{ord}(c^\pm(\mathrm{Frob}_\ell^2)) = \mathrm{ord}(2g^\pm(z)) = \mathrm{ord}(g^\pm(z)) \geq d^\pm$. □

**Remark 6.3.2.** The primary difference between Proposition 6.3.1 and [CGLS22, Prop. 3.3.6] is that here we have restricted ourselves to the $\mathfrak{m}^m$-torsion of the Selmer groups of $T^{(k)}$ (see (6.2)) and so we can directly work with the eigenspaces of complex conjugation. For the proof of *loc. cit.* we worked over an extension trivialising the character $\alpha \mod \varpi^k$ and then used "some quadratic forms" to estimate the linear independence of the images of the localisations of the classes. The upshot is that our error term no longer involves the $C_\alpha$ of [CGLS22]. This is crucial for removing the corank one assumption in the proof of the anticyclotomic Iwasawa main conjecture in *op. cit.*. However it causes some complications in the proof of Theorem 6.1.1: we use the $\mathfrak{m}^m$-Selmer groups to control the image of the localisation at Kolyvagin primes of classes in the $\mathfrak{m}^k$-Selmer groups, and the resulting control is not as tight as in [CGLS22].

6.4. **Proof of Theorem 6.1.1.** The (co-)rank one claim in the theorem follows from [CGLS22, Thm. 3.3.8]:

$$\mathrm{H}^1_{\mathcal{F}}(K,T) \simeq R \quad \text{and} \quad \mathrm{H}^1_{\mathcal{F}}(K,A) \simeq \Phi/R \oplus M, \quad M \simeq M_0 \oplus M_0$$

for some finitely-generated torsion $R$-module $M_0$ such that $M_0 \simeq M^{(k)}(1)$ for all $k \gg 0$. In fact, the proof of [CGLS22, Thm. 3.3.8] shows that $M_0 \simeq M^{(k)}(1)$ if $k > \mathrm{ind}(\kappa_1) + 3r(C_1 + C_2 + m)$. In the current setting, the error term $C_\alpha$ of *op. cit.* is equal to $m$; it is essentially this fact that prevents the arguments in *op. cit.* from applying to prove the theorem in the current setting and is the reason we take a different approach below to establishing the bound

$$s_1 + \mathcal{E} \geq \mathrm{length}_R(M^{(k)}(1)), \tag{B}$$

where $s_1 = \mathrm{ind}(\kappa_1, \mathrm{H}^1_{\mathcal{F}}(K,T))$ and $\mathcal{E}$ does not depend on $m$, provided $m$ is sufficiently large. As $\mathrm{length}_R(M) = \mathrm{length}_R(M^{(k)}(1))$ for $k \gg 0$, the bound (B) implies the bound in Theorem 6.1.1.

We now focus on the proof of (B). A finite torsion $R$-module $X$ is isomorphic to a sum of cyclic $R$-modules: $X \simeq \oplus_{i=1}^{s(X)} R/\mathfrak{m}^{d_i}$ for some uniquely-determined integers $d_i \geq 0$. For an integer $t \geq 0$ we let $\rho_t(X) = \#\{i : d_i > t\}$. In particular, for $n \in \mathscr{N}^{(m)}$ we let

$$\rho_t(n) := \rho_t(\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(m)})^+) + \rho_t(\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(m)})^-).$$

Note that it $t < m$ then $\rho_t(n) \geq 1$ since the $\epsilon$ of Proposition 6.2.2 is 1 (the latter fact is implicit in the above rank one result). We also let

$$\rho := 2(\rho_e(1) - 1).$$

Note that $\rho < 2\dim_{\mathbb{F}}(\mathrm{H}^1_{\mathcal{F}}(K, T^{(1)}) = 2\dim_{\mathbb{F}_p}(\mathrm{H}^1_{\mathcal{F}}(K, E[p])$, where $\mathbb{F} = R/\mathfrak{m}$ is the residue field of $R$, and hence $\rho$ is bounded by a constant independent of $k$, $m$, and $\alpha$.

*Proof of* (B). Let $s(n) = \dim_{\mathbb{F}} \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(1)}) - 1 = \dim_{\mathbb{F}} M(n)[\mathfrak{m}]$, and let

$$\mathcal{E} = (\rho + (s(1) + 1 + 2\rho)(5\rho + 1))e \quad \text{and} \quad \mathcal{M} = (1 + 5\rho)e.$$

Note that $\mathcal{E}$ and $\mathcal{M}$ are bounded by constants that are independent of $m$ (and depend on $\alpha$ only through the $\mathbb{Z}_p$-rank $r$ of $R$). Let $k$ be a fixed integer such that

$$k > \mathrm{length}_R(M(1)) + \mathrm{ind}(\kappa_1) + m + (6s(1) + 2)e. \tag{6.5}$$

We will show that (B) holds provided

$$m > \mathcal{M}.$$

If $\rho = 0$, then the exponent of $M(1)$ is at most $e$ and therefore

$$\tfrac{1}{2}\mathrm{length}_R(M(1)) \leq \tfrac{1}{2}(s(1)+1)e \leq \mathrm{ind}(\kappa_1) + \mathcal{E}.$$

So we may assume $\rho > 0$.

We will find sequences of integers $1 = n_0, n_1, ..., n_\rho \in \mathscr{N}^{(k)}$ and $1 = x_0, x_1, ..., x_\rho$ along with integers $b(n_i) \geq 0$ that satisfy

(a) $s(n_{i+1}) - 2 \leq s(n_i) \leq s(n_{i+1}) + 2$;
(b) $\frac{1}{2}\mathrm{length}_R(M(n_i)) \geq \frac{1}{2}\mathrm{length}_R(M(n_{i-1})) - b(n_i)$ ;
(c) $\frac{1}{2}\mathrm{length}_R(M(n_i)) \leq \frac{1}{2}\mathrm{length}_R(M(n_{i-1})) + e$;
(d) $\mathrm{ord}(\kappa_{n_i}) \geq \mathrm{ord}(\kappa_{n_{i-1}}) - e$;
(e) $\mathrm{ind}(\kappa_{n_{i-1}}) + e \geq \mathrm{ind}(\kappa_{n_i}) + b(n_i)$;
(f) $x_{i-1} + 2 \leq x_i \leq x_{i-1} + 5$, $\rho_{x_i e}(n_i) \leq \rho_{x_{i-1}e}(n_{i-1})$, and $\rho_{x_i e}(n_i) = \rho_{x_{i-1}e}(n_{i-1}) > 1$ only if $\rho_{(x_i+1)e}(\mathrm{H}^1_{\mathcal{F}(n_i)}(K, T^{(m)})^{\pm}) \geq 1$;
(g) if $\rho_{x_{i-2}e}(n_{i-2}) > 1$ then $\rho_{x_i e}(n_i) < \rho_{x_{i-2}e}(n_{i-2})$.

Before explaining the existence of such sequences, we demonstrate that (B) follows from (a)–(f).

From repeated appeals to (a) we obtain

$$s(n_\rho) \leq s(1) + 2\rho.$$

From repeated appeals to (g) we see that either $\rho_{x_i e}(n_i) = 1$ for some $1 \leq i < \rho$, in which case $1 \leq \rho_{x_\rho e}(n_\rho) \leq \rho_{x_i e}(n_i) = 1$, or $1 \leq \rho_{x_\rho e}(n_\rho) \leq \rho_{x_{\rho-2}e}(n_{\rho-2}) - 1 \leq \cdots \leq \rho_{x_0 e}(n_0) - \frac{1}{2}\rho = \rho_e(1) - \frac{1}{2}\rho = 1$. In either case, we see

$$\rho_{x_\rho e}(n_\rho) = 1.$$

As $x_\rho \leq x_0 + 5\rho = 1 + 5\rho$, it then follows that

$$\mathrm{length}_R(M(n_\rho)) \leq s(n_\rho) x_\rho e \leq s(n_\rho)(5\rho+1)e \leq (s(1)+2\rho)(5\rho+1)e. \tag{6.6}$$

By repeatedly applying (b) and (e) we obtain

$$\begin{aligned}\mathrm{ind}(\kappa_1) + \rho e &\geq \mathrm{ind}(\kappa_{n_\rho}) + b(n_1) + b(n_2) + \cdots + b(n_\rho) \\ &\geq \mathrm{ind}(\kappa_{n_\rho}) + \tfrac{1}{2}\mathrm{length}_R(M(1)) - \tfrac{1}{2}\mathrm{length}_R(M(n_\rho)).\end{aligned}$$

Combined with (6.6) this gives

$$\begin{aligned}\mathrm{ind}(\kappa_1) + \mathcal{E} &\geq \mathrm{ind}(\kappa_{n_\rho}) + \tfrac{1}{2}\mathrm{length}_R(M(1)) - \tfrac{1}{2}\mathrm{length}_R(M(n_\rho)) + (s(1)+2\rho)(5\rho+1)e \\ &\geq \mathrm{ind}(\kappa_{n_\rho}) + \tfrac{1}{2}\mathrm{length}_R(M(1)) + \tfrac{1}{2}\mathrm{length}_R(M(n_\rho)) \\ &\geq \tfrac{1}{2}\mathrm{length}_R(M(1)),\end{aligned}$$

which is the bound (B).

We will now define the sequence $n_0 = 1, n_1, \ldots, n_T \in \mathscr{N}^{(k)}$ (and subsequently the $b(n_i)$ and $x_i$) by making repeated use of Proposition 6.3.1 to choose suitable primes in $\mathscr{L}^{(k)}$.

Suppose $1 = n_0, n_1, \ldots, n_j \in \mathscr{N}^{(k)}$, $1 = x_0, x_1, \ldots, x_j$, and $0 = b(n_0), b(n_1), \ldots, b(n_j)$, $j < \rho$, are such that (a)–(f) hold for all $1 \leq i \leq j$ (note that if $j = 0$ then (a)–(f) are vacuously true). We will explain how to choose a prime $\ell \in \mathscr{L}^{(k)}$ such that $n_0, \ldots, n_i, n_{j+1} = n_j\ell$ satisfy (a)–(f) for all $1 \leq i \leq j+1$. Repeating this process yields the desired sequence $n_0, \ldots, n_\rho$.

Let $c_0 \in \mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(k)})$ generate an $R/\mathfrak{m}^k$-summand complementary to $M(n_j)$, so $\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(k)}) = Rc_0 \oplus M(n_j) \simeq R/\mathfrak{m}^k \oplus M(n_j)$. Let $\nu \in \{\pm\}$ such that $\mathrm{ord}((1+\nu\tau)\varpi^{k-m}c_0) = m$, that is, the order of $c^\nu = (1+\nu\tau)(\varpi^{k-m}c_0) \in \mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^\nu$ is $m$. Note that the order of $\varpi^{k-m}c_0$ is $m$, so there exists at least one $\nu \in \{\pm\}$ satisfying the desired condition. Let $N := \exp(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{-\nu})$ and let $c^{-\nu} \in \mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{-\nu}$ have order $N$. We apply Proposition 6.3.1 to the classes $c^\nu$ and $c^{-\nu}$ and obtain a prime $\ell \in \mathscr{L}^{(k)}$ such that

$$\mathrm{ord}(\mathrm{loc}_\ell(\varpi^{k-m}c_0)) \geq \mathrm{ord}(\mathrm{loc}_\ell(c^\nu)) \geq m - e \quad \text{and} \quad \mathrm{ord}(\mathrm{loc}_\ell(c^{-\nu})) \geq N - e,$$

and $\mathrm{loc}_\ell(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)}))$ has an $R$-submodule isomorphic to $R/\mathfrak{m}^{m-e} \oplus R/\mathfrak{m}^{N-e}$. As $m > e$, it follows that $\mathrm{ord}(\mathrm{loc}_\ell(c_0)) \geq k - e$, and hence $\mathrm{loc}_\ell(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(k)})) \simeq R/\mathfrak{m}^{k-a} \oplus R/\mathfrak{m}^b$ for some $a \leq e$ and $b \geq N - e$. In particular, there is a short exact sequence

$$0 \to H \to \mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(k)}) \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{k-a} \oplus R/\mathfrak{m}^b \to 0, \quad a \leq e,\ b \geq N - e, \tag{6.7}$$

where $H := \mathrm{H}^1_{\mathcal{F}(n_j)_\ell}(K, T^{(k)}))$ is the kernel of the localisation at $\ell$. Global duality then implies that there is an exact sequence

$$0 \to H \to \mathrm{H}^1_{\mathcal{F}(n_j\ell)}(K, T^{(k)}) \simeq R/\mathfrak{m}^k \oplus M(n_j\ell) \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{k-b'} \oplus R/\mathfrak{m}^{a'} \to 0, \quad a \geq a', b' \geq b. \tag{6.8}$$

Here we have used that the arithmetic dual of $T^{(k)} = T^{(k)}_\alpha$ is $T^{(k)}_{\alpha^{-1}}$ and that the complex conjugation $\tau$ induces an isomorphism $\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)}_{\alpha^{-1}}) \simeq \mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)}_\alpha)$.

We now show (a)-(e) hold for $i = j+1$ with $n_{j+1} = n_j\ell$ and $b(n_{j+1}) = b'$.

Let $h := \dim_{\mathbb{F}} H[\mathfrak{m}]$. From (6.7) it follows that $h \leq 1 + s(n_j) \leq h+2$, and from (6.8) it follows that $h \leq 1 + s(n_{j+1}) \leq h+2$. Hence $s(n_j) - 2 \leq h-1 \leq s(n_{j+1}) \leq h+1 \leq s(n_j)+2$, which shows that (a) holds.

From(6.8) and (6.7) we find

$$\mathrm{length}_R(M(n_{j+1})) = \mathrm{length}_R(H) - b' + a' = \mathrm{length}_R(M(n_j)) - (b+b') + (a+a').$$

As $(b+b') \leq 2b' = 2b(n_{j+1})$, it follows that (b) holds. And as $(a+a') \leq 2e$, it follows that (c) holds.

To verify that (d) holds for $i = j+1$, we first observe that

$$\mathrm{ord}(\kappa_{n_{i+1}}) = \mathrm{ord}(\kappa_{n_i\ell}) \geqslant \mathrm{ord}(\mathrm{loc}_\ell(\kappa_{n_i\ell})) = \mathrm{ord}(\mathrm{loc}_\ell(\kappa_{n_i})),$$

the last equality following from the finite-singular relations of the Kolyvagin system. So (d) holds if $\mathrm{ord}(\mathrm{loc}_\ell(\kappa_{n_j})) \geqslant \mathrm{ord}(\kappa_{n_j}) - e$. To see that this last inequality holds, we note that $\mathrm{ord}(\kappa_{n_j}) \geq \mathrm{ord}(\kappa_{n_0}) - je$ by (d) for $1 \leqslant i \leqslant j$. But $\mathrm{ord}(\kappa_{n_0}) = \mathrm{ord}(\kappa_1) = k - \mathrm{ind}(\kappa_1)$ by the choice of $k$ (and the fact that $\mathrm{H}^1_{\mathcal{F}}(K,T)$ is torsion-free by (h1)), and so by (6.5) and repeated application of (c) for $1 \leq i \leq j$ we have

$$\begin{aligned} \mathrm{ord}(\kappa_{n_j}) \geq k - \mathrm{ind}(\kappa_1) - je &> \mathrm{length}_R(M(1)) + m + (6s(1) + 2 - j)e \\ &\geq \mathrm{length}_R(M(n_j)) + m + (6s(1) + 2 - 3j)e \\ &\geq \mathrm{length}_R(M(n_j)) + m + 2e \\ &\geq \mathrm{length}_R(M(n_j)) + 2e. \end{aligned} \tag{6.9}$$

Write $\kappa_{n_j} = xc_0 + y$ with $x \in R$ and $y \in M(n_j)$. Since $\mathrm{ord}(\kappa_{n_j}) > \exp(M(n_j))$ by (6.9), it follows that $x = \varpi^t u$ for $t = k - \mathrm{ord}(\kappa_{n_j})$ and some $u \in R^\times$. It follows that

$$\pi^{\exp(M(n_j))}\,\mathrm{loc}_\ell(\kappa_{n_i}) = \pi^{\exp(M(n_j))+t} u\,\mathrm{loc}_\ell(c_0).$$

By the choice of $\ell$, $\mathrm{ord}(\mathrm{loc}_\ell(c_0)) \geqslant k - e = t + \mathrm{ord}(\kappa_{n_j}) - e > t + \exp(M(n_j)) + e$, where the last inequality follows by (6.9). We then deduce that

$$\mathrm{ord}(\mathrm{loc}_\ell(\kappa_{n_j})) = \mathrm{ord}(\mathrm{loc}_\ell(c_0)) - t \geq k - e - t = \mathrm{ord}(\kappa_{n_i}) - e,$$

which – as noted at the start of this paragraph – implies that (d) holds.

Next we verify (e) for $i = j+1$. Let $c_1 \in \mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(k)})$ be a generator of an $R/\mathfrak{m}^k$-summand complementary to $M(n_{i+1})$, so $\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(k)}) = Rc_1 \oplus M(n_{j+1}) \simeq R/\mathfrak{m}^k \oplus M(n_{j+1})$. Write $\kappa_{n_j} = u\pi^g c_1 + y$ and $\kappa_{n_{i+1}} = v\pi^h c + y'$, where $u, v \in R^\times$, $y \in M(n_j)$ and $y' \in M(n_{j+1})$. Arguing as in the preceding proof that (d) holds for $i = j+1$ shows that $\mathrm{ord}(\kappa_{n_i}) > \exp(M(n_i)) + 2e$ for $1 \leqslant i \leqslant j+1$ and in particular for $i = j$ and $i = j+1$. Hence $g = k - \mathrm{ord}(\kappa_{n_j})$ and $h = k - \mathrm{ord}(\kappa_{n_{j+1}})$. Arguing further as in the proof that (d) holds also yields

$$\mathrm{ord}(\mathrm{loc}_\ell(\kappa_{n_j})) = \mathrm{ord}(\mathrm{loc}_\ell(c_0)) - g \quad \text{and} \quad \mathrm{ord}(\mathrm{loc}_\ell(\kappa_{n_{j+1}})) = \mathrm{ord}(\mathrm{loc}_\ell(c_1)) - h.$$

From the finite-singular relations for the Kolyvagin system the left-hand sides of both equalities are equal and therefore

$$h - g = \mathrm{ord}(\mathrm{loc}_\ell(c_1)) - \mathrm{ord}(\mathrm{loc}_\ell(c_0)).$$

We refer again to the short exact sequences (6.7) and (6.8). By the choice of $\ell$, $\mathrm{ord}(\mathrm{loc}_\ell(c_0)) \geq k - e > \exp(M(n_j)) \geq b$, the last inequality by [CGLS22, Lem. 3.3.10(ii)]. Hence we must have $\mathrm{ord}(\mathrm{loc}_\ell(c_0)) = k - a$. Similarly, we also must have $\mathrm{ord}(\mathrm{loc}_\ell(c_1)) = k - b'$. Thus we find

$$h - g = (k - b') - (k - a) = a - b' \leq e - b'.$$

Since $h - g = \mathrm{ord}(\kappa_{n_j}) - \mathrm{ord}(\kappa_{n_{j+1}})$, this proves $\mathrm{ord}(\kappa_{n_j}) + b' \leq \mathrm{ord}(\kappa_{n_{j+1}}) + e$ and hence, since we have shown $\mathrm{ord}(\kappa_{n_j}) = k - \mathrm{ind}(\kappa_{n_j})$ and $\mathrm{ord}(\kappa_{n_{i+1}}) = k - \mathrm{ind}(\kappa_{n_{j+1}})$, (e) holds.

So far, our arguments have not wandered far from the lanes of [CGLS22, §3.3.3]. However, at this point we cannot continue along the same path and deduce – in the notation of *op. cit.* (see also below) – that

$d_t(M(n_{i+1})) \geqslant d_{t+2}(M(n_i))$, $t = 1, \dots, \dim_{\mathbb{F}}(M(n_i)[\mathfrak{m}]) - 2$. This is because knowing the localisation of $\mathrm{H}^1_{\mathcal{F}(n_i)}(K, T^{(k)})[\mathfrak{m}^m]^{-\nu}$ is not sufficient to determine which class(es) in $\mathrm{H}^1_{\mathcal{F}(n_i)}(K, T^{(k)})$ have localistion generating the summand $R/\mathfrak{m}^b$ in (6.7). Instead, to conclude the proof of (B), we establish (f). This roughly tells us that – even without being able to control the individual $d_t(M(n_i))$s – the number of large exponents decreases. Actually, in general we can only show that this number does not increase, but if we are in the unfortunate situation where it is stable (which happens essentially if all the "big summands" are in the same eigenspace), then at the step $n_{i+1}$ this number decreases.

It remains to define $x_{j+1}$ and verify (f) and (g). To this end we introduce some more notation. A finitely-generated torsion $R$-module $X$ can be written as sum of cyclic $R$-modules $X \simeq \oplus_{i=1}^{s(X)} R/\mathfrak{m}^{d_i(X)}$, with the exponents $d_i(X)$ uniquely determined. We shall always suppose that the $d_i(X)$ have been labeled so that $d_1(X) \geq d_(X) \geq \cdots \geq d_{s(X)}(X)$. Note that $s(X) = \dim_{\mathbb{F}} X[\mathfrak{m}]$. We will adopt the convention that $d_i(X) = 0$ if $i > s(X)$, extending the $d_i(X)$ to all positive $i$.

Taking the $\mathfrak{m}^m$-torsion of the exact sequence (6.7) we obtain two short exact sequences:

$$0 \to H[\mathfrak{m}^m]^{\nu} \to \mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{\nu} \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{m-a_\nu} \to 0, \quad 0 \leq a_\nu \leq e, \tag{6.10}$$

and

$$0 \to H[\mathfrak{m}^m]^{-\nu} \to \mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{-\nu} \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{b_\nu} \to 0, \quad N - e \leq b_\nu \leq N, \tag{6.11}$$

The bounds on the exponents for the modules on the right come from the choice of $\ell$ with respect to the classes $c^{\nu} = (1 + \nu\tau)\varpi^{k-m}c_0$ and $c^{-\nu}$. Global duality then yields two additional short exact sequences

$$0 \to H[\mathfrak{m}^m]^{\nu} \to \mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(m)})^{\nu} \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{a'_\nu} \to 0, \quad 0 \leq a'_\nu \leq e, \tag{6.12}$$

and

$$0 \to H[\mathfrak{m}^m]^{-\nu} \to \mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(m)})^{-\nu} \xrightarrow{\mathrm{loc}_\ell} R/\mathfrak{m}^{m-b'_\nu} \to 0, \quad b'_\nu \leq b_\nu. \tag{6.13}$$

As $\mathrm{ord}(c^{\nu}) = m$ and $\mathrm{ord}(\mathrm{loc}_\ell(c^{\nu})) = m - a$ with $a \leq e$, it follows from (6.10) that $d_i(H[\mathfrak{m}^m]^{\nu}) \leq d_{i+1}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{\nu}) + e$. From (6.12) we deduce that $d_i(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(m)})^{\nu}) \leq d_i(H[\mathfrak{m}^m]^{\nu}) + e$, and so

$$d_i(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(m)})^{\nu}) \leq d_{i+1}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{\nu}) + 2e.$$

Let $i_0 = \rho_{x_i e}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{\nu})$. It follows that $d_{i_0}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(m)})^{\nu}) \leq d_{i_0+1}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{\nu}) + 2e \leq x_j e + 2e$, so

$$\rho_{(x_j+2)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(m)})^{\nu}) \leq i_0 - 1 = \rho_{x_i e}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{\nu}) - 1. \tag{6.14}$$

Next we consider the exact sequence (6.13). One of the cyclic summands of $\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(m)})^{-\nu}$, say one isomorphic to $R/\mathfrak{m}^{d_t}$ for $d_t = d_t(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}, T^{(m)})^{-\nu})$, surjects under $\mathrm{loc}_\ell$ onto $R/\mathfrak{m}^{m-b'_\nu}$. There is therefore an $R$-module surjection $H[\mathfrak{m}^m]^{-\nu} \twoheadrightarrow \mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(m)})^{-\nu}/(R/\mathfrak{m}^{d_t})$, and so – upon taking Pontryagin duals – an $R$-module injection $\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(m)})^{-\nu}/(R/\mathfrak{m}^{d_t}) \hookrightarrow H[\mathfrak{m}^m]^{-\nu}$. From this together with the injection in (6.11) we conclude that

$$d_i(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, , T^{(m)})^{-\nu}) \leq \begin{cases} d_i(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{-\nu}) & i < t \\ d_{i-1}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{-\nu}) & i > t. \end{cases} \tag{6.15}$$

It then follows that

$$\rho_{x_j e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K, T^{(m)})^{-\nu}) \leq \rho_{x_j e}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{-\nu}) + 1$$

Together with (6.14) this implies

$$\rho_{(x_j+2)e}(n_{j+1}) \leq \rho_{x_j e}(n_j), \tag{6.16}$$

which proves the first inequality in (f) for any choice of $x_{j+1} \geq x_j + 2$.

Suppose

$$x_j e + e < N = \exp(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{-\nu}). \tag{♠}$$

Considering the exact sequence (6.11), we see that one of the cyclic summands of $\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{-\nu}$, say one isomorphic to $R/\mathfrak{m}^{d_h}$ for $d_h = d_h(\mathrm{H}^1_{\mathcal{F}(n_j)}(K, T^{(m)})^{-\nu})$, surjects onto $R/\mathfrak{m}^{b_\nu}$. As $b_\nu \geq N - e > x_j e$, it follows

that $d_h > x_j e$, and so $\rho_{x_j e}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K,T^{(m)})^{-\nu}/(R/\mathfrak{m}^{d_h})) = \rho_{x_j e}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K,T^{(m)})^{-\nu}) - 1$. On the other hand, since $d_h \leq N$, the $R$-module surjection $H[\mathfrak{m}^m]^{-\nu} \twoheadrightarrow \mathrm{H}^1_{\mathcal{F}(n_j)}(K,T^{(m)})^{-\nu}/(R/\mathfrak{m}^{d_h})$ has kernel annihilated by $\varpi^e$ and so $\rho_{x_j e+e}(H[\mathfrak{m}^m]^{-\nu}) \leq \rho_{x_j e}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K,T^{(m)})^{-\nu}/(R/\mathfrak{m}^{d_h}))$. Combining these inequalities yields

$$\rho_{x_j e+2e}(H[\mathfrak{m}^m]^{-\nu}) \leq \rho_{x_j e+e}(H[\mathfrak{m}^m]^{-\nu}) \leq \rho_{x_j e}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K,T^{(m)})^{-\nu}) - 1.$$

From the previously noted injection $\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}/(R/\mathfrak{m}^{d_t}) \hookrightarrow H[\mathfrak{m}^m]^{-\nu}$ we deduce that

$$\rho_{x_j e+2e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) - 1 \leq \rho_{x_j e+2e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}/(R/\mathfrak{m}^{d_t})) \leq \rho_{x_j e+2e}(H[\mathfrak{m}^m]^{-\nu}).$$

Together the two displayed equations yield

$$\rho_{x_j e+2e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) \leq \rho_{x_j e}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K,T^{(m)})^{-\nu}).$$

Combining this with (6.14) we find

$$(\spadesuit) \implies \rho_{(x_j+2)e}(n_{j+1}) < \rho_{x_j e}(n_j). \tag{6.17}$$

If ($\spadesuit$) does not hold, then $N = \exp(\mathrm{H}^1_{\mathcal{F}(n_j)}(K,T^{(m)})^{-\nu}) \leq (x_j+1)e$. From (6.15) we see that each $d_i(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) \leq (x_j+1)e$ except possibly for $i = t$. So either $\rho_{(x_j+1)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) = 0$ or $t = 1$ and $\rho_{(x_j+1)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) = 1$. If $\rho_{(x_j+1)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) = 0$, then it follows from (6.14) that $\rho_{(x_j+2)e}(n_{j+1}) < \rho_{x_j e}(n_j)$. If $d_t \leq (x_j+3)e$, then we also have $\rho_{(x_j+3)e}(n_{j+1}) < \rho_{x_j e}(n_j)$ by similar reasoning.

Suppose $\rho_{(x_j+3)e}(n_j) = 1$. The proof of (6.16) also holds for $x_j$ replaced with $x_j+3$, which shows $\rho_{(x_j+5)e}(n_{j+1}) \leq \rho_{(x_j+3)e}(n_j) = 1$.

To summarize, we have shown that

$$\rho_{(x_j+5)e}(n_{j+1}) = \rho_{x_j e}(n_j) > 1 \implies \begin{cases} (\spadesuit) \text{ does not hold,} \\ \rho_{(x_j+1)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) = 1, \\ d_t > (x_j+3)e, \\ \rho_{(x_j+3)e}(n_j) > 1. \end{cases} \tag{6.18}$$

Suppose $\rho_{(x_j+5)e}(n_{j+1}) = \rho_{x_j e}(n_j) > 1$. Since $\rho_{(x_j+5)e}(n_{j+1}) \leq \rho_{(x_j+3)e}(n_{j+1}) \leq \rho_{(x_j+2)e}(n_{j+1}) \leq \rho_{x_j e}(n_j)$, it follows that we also have $\rho_{(x_j+3)e}(n_{j+1}) = \rho_{(x_j+2)e}(n_{j+1}) = \rho_{x_j e}(n_j)$. Furthermore, all the conditions on the right-hand side of (6.18) hold. As $d_t > (x_j+3)e$, $\exp(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) > (x_j+3)e$, so $\rho_{(x_j+3)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) \geq 1$. As $\rho_{(x_j+3)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) \leq \rho_{(x_j+1)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) = 1$, it follows that $\rho_{(x_j+3)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) = 1$. Since $\rho_{x_j e}(n_j) \geq 2$, $\rho_{(x_j+3)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{\nu}) = \rho_{(x_j+3)e}(n_{j+1}) - \rho_{(x_j+3)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{-\nu}) = \rho_{x_j e}(n_j) - 1 \geq 1$. This shows

$$\rho_{(x_j+5)e}(n_{j+1}) = \rho_{x_j e}(n_j) > 1 \implies \begin{cases} \rho_{(x_j+2)e}(n_{j+1}) = \rho_{x_j e}(n_j), \\ \rho_{(x_j+3)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{\pm}) \geq 1. \end{cases} \tag{6.19}$$

We can now complete our definition of $x_{j+1}$ and the verification of (f):

(i) If $\rho_{(x_j+5)e}(n_{j+1}) = 1$ or $\rho_{(x_j+5)e}(n_{j+1}) < \rho_{x_j e}(n_j)$, then $x_{j+1} := x_j + 5$.
(ii) If $\rho_{(x_j+5)e}(n_{j+1}) = \rho_{x_j e}(n_j) > 1$, then $x_{j+1} := x_j + 2$ and (6.19) shows that

$$\rho_{(x_{j+1}+1)e}(\mathrm{H}^1_{\mathcal{F}(n_{j+1})}(K,T^{(m)})^{\pm}) \geq 1.$$

Hence (f) holds for $i = j+1$.

Finally, we verify (g) for $i = j+1$. Suppose $\rho_{x_{j-1}e}(n_{j-1}) > 1$. If $\rho_{x_j e}(n_j) < \rho_{x_{j-1}e}(n_{j-1})$, then $\rho_{x_{j+1}e}(n_{j+1}) \leq \rho_{x_j e}(n_j) < \rho_{x_{j-1}e}(n_{j-1})$. Suppose then that $\rho_{x_j e}(n_j) = \rho_{x_{j-1}e}(n_{j-1})$. It follows from (f) in the case $i = j$ (which holds by induction) that $\rho_{(x_j+1)e}(\mathrm{H}^1_{\mathcal{F}(n_j)}(K,T^{(m)})^{\pm}) \geq 1$. This implies that ($\spadesuit$) holds, and so, by (6.18) above, $\rho_{(x_j+5)e}(n_{j+1}) < \rho_{x_j e}(n_j) = \rho_{x_{j-1}e}(n_{j-1})$. As $x_{j+1} = x_j + 5$ in this case (see (i) above), this shows that (g) holds. □

This completes the proof of Theorem 6.1.1.

**Remark 6.4.1.** The strategy to produce the $n_i \in \mathscr{N}^{(k)}$ as in the preceding proof is similar to the one employed in [CGLS22, §3.3.3] but technically more delicate. In particular, comparing the condition (b) here and the condition (b) in *op. cit.*, one will notice that the one stated herein is weaker (and would follow from condition (b) in *op. cit.*). The issue is exactly the one hinted at previously: we have removed the dependence of the error term on $\alpha$, but at the cost of having to work with the $\mathfrak{m}^m$-torsion. This prevents us from proving that we can take $b_{M(n_{t-1})}(n_t) = d_1(M(n_{t-1})) - e$ (notation as in [CGLS22]) – and so being able to work with the stronger condition (b). This results in the need for the additional conditions (f) and (g), which can be thought as an induction step on "the number of summands of the $\mathfrak{m}^m$-torsion of the Selmer groups that are not bounded by (controlled) multiples of $e$". Philosophically, this is what is done in the proof of [How04, Lemma 1.6.4], where however, as $e = 0$, one can work with the $\mathfrak{m}$-torsion and have an equality for the order in Proposition 6.3.1.

6.5. **The anticyclotomic Iwasawa main conjectures.** With Theorem 6.1.1 in hand, we can state and prove a strengthening of [CGLS22, Thm. 3.4,1] and consequent strengthenings of [CGLS22, Thm. 4.1.2, Thm. 4.2.2] as well as [CGLS22, Cor. 4.2.3]. Let $\Lambda = \Lambda_K^-$, and note that the modules

$$\mathcal{X} = \mathrm{H}^1_{\mathcal{F}_\Lambda}(K, M_E)^\vee, \quad \mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$$

in [CGLS22, §3.4] are the same as the modules $\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^-)$ and $\mathfrak{S}_{\mathrm{ord}}(E/K_\infty^-)$ in §3.1, respectively.

**Theorem 6.5.1.** *Assume $E(K)[p] = 0$ and suppose there is a Kolyvagin system $\kappa \in \mathbf{KS}(\mathbf{T}, \mathcal{F}_\Lambda, \mathscr{L}_E)$ with $\kappa_1 \neq 0$. Then $\mathfrak{S}_{\mathrm{ord}}(E/K_\infty^-)$ has $\Lambda$-rank one, and there is a finitely generated torsion $\Lambda$-module $M$ such that*

(i) $\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^-) \sim \Lambda \oplus M \oplus M$,
(ii) $\mathrm{char}_\Lambda(M)$ *divides* $\mathrm{char}_\Lambda\big(\mathfrak{S}_{\mathrm{ord}}(E/K_\infty^-)/\Lambda\kappa_1\big)$ *in* $\Lambda[1/p]$.

*Proof.* The proof is the same as that of [CGLS22, Theorem 3.4.1]. However, the height one prime $(\gamma^- - 1) \subset \Lambda$ was excluded from the analysis in *loc. cit.* because the error term in [CGLS22, Thm. 3.2.1] increases as the characters $\alpha$ get $p$-adically closer to 1. Replacing the appeal to *op. cit.* with one to Theorem 6.1.1 for the case of the prime $(\gamma^- - 1)$, yields the theorem. □

Applying Theorem 6.5.1 to the Kolyvagin system $\kappa^{\mathrm{Hg}} = \{\kappa_n^{\mathrm{Hg}}\}_{n \in \mathscr{N}}$ of [CGLS22, Thm. 4.1.1], we thus obtain the following.

**Theorem 6.5.2.** *Assume $E(K)[p] = 0$. Then $\mathfrak{S}_{\mathrm{ord}}(E/K_\infty^-)$ has $\Lambda$-rank one, and there is a finitely generated torsion $\Lambda$-module $M$ such that*

(i) $\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^-) \sim \Lambda \oplus M \oplus M$,
(ii) $\mathrm{char}_\Lambda(M)$ *divides* $\mathrm{char}_\Lambda\big(\mathfrak{S}_{\mathrm{ord}}(E/K_\infty^-)/\Lambda\kappa_1^{\mathrm{Hg}}\big)$ *in* $\Lambda[1/p]$.

Using this, we conclude just as for [CGLS22, Thm. 4.2.2]:

**Theorem 6.5.3.** *Suppose $K$ satisfies hypotheses (Heeg), (spl), and (disc), and that $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ as $G_{\mathbb{Q}}$-modules, with $\phi|_{G_p} \neq \mathbb{1}, \omega$. Then $\mathfrak{X}_{\mathrm{Gr}}(E/K_\infty^-)$ is $\Lambda$-torsion, and*

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

*as ideals in $\Lambda^{\mathrm{ur}}$. Hence the anticyclotomic Iwasawa–Greenberg main conjecture in Conjecture 3.1.2 holds.*

And just as for [CGLS22, Cor. 4.2.3] (noting that the ambiguity by powers of $p$ in *loc. cit.* can be removed), we then have Theorem C in the Introduction:

**Corollary 6.5.4.** *Suppose $K$ satisfies hypotheses (Heeg), (spl), (disc), and that $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ as $G_{\mathbb{Q}}$-modules, with $\phi|_{G_p} \neq \mathbb{1}, \omega$. Then both $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ and $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K, M_E)^\vee$ have $\Lambda$-rank one, and*

$$\mathrm{char}_\Lambda\big(\mathrm{H}^1_{\mathcal{F}_\Lambda}(K, M_E)^\vee_{\mathrm{tors}}\big) = \mathrm{char}_\Lambda\big(\mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})/\Lambda\kappa_\infty\big)^2.$$

## 7. Mazur's main conjecture

In this section we put everything together to deduce the proof of Theorem A in the Introduction:

**Theorem 7.0.1.** *Let $E/\mathbb{Q}$ be an elliptic curve, and $p > 2$ a prime of good reduction for $E$ such that $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ with $\phi|_{G_{\mathbb{Q}_p}} \neq 1, \omega$. Then the module $\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)$ is $\Lambda_{\mathbb{Q}}$-torsion, with*

$$\mathrm{ch}_{\Lambda_{\mathbb{Q}}}\big(\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)\big) = \big(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})\big).$$

*In other words, Mazur's main conjecture for $E$ holds.*

7.1. **Proof of Mazur's main conjecture.** We divide it into three steps, similarly as we did in §5. Choose an imaginary quadratic field $K$ satisfying hypotheses (Heeg), (spl), and (disc). As usual, we let $E_\bullet$ denote the elliptic curve in the isogeny class of $E$ constructed in [Wut14], and put $S = \Sigma \smallsetminus \{p, \infty\}$.

*Step 1.* The $p$-adic $L$-functions $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+ \in \Lambda_K^+$ and $\mathcal{L}_p^{\mathrm{BDP}}(f/K) \in \Lambda_K^{-,\mathrm{ur}}$ are nonzero: For $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+$ this follows Proposition 2.2.4, Theorem 2.1.1, and Rohrlich's nonvanishing result [Roh84]; and for $\mathcal{L}_p^{\mathrm{BDP}}(f/K)$ this is part of Theorem 2.3.1. Fix an integer $m > 0$ such that

$$\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+ \neq 0 \in \Lambda_K^+/p^m\Lambda_K^+, \tag{7.1}$$

and take a crystalline character $\alpha : \Gamma_K^- \to R^\times$ with $\alpha \equiv 1 \pmod{\varpi^m}$ such that $\mathcal{L}_p^{\mathrm{BDP}}(f(\alpha)/K)(0) \neq 0$.

By Theorem 6.5.3 we then have that $\mathfrak{X}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^-)$ is $\Lambda_K^-$-torsion, with

$$\mathcal{F}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^-)(0) \ \sim_p \ \mathcal{L}_p^{\mathrm{BDP}}(f(\alpha)/K)(0) \neq 0, \tag{7.2}$$

where $\mathcal{F}_{\mathrm{Gr}}^S(E_\bullet/K_\infty^-) \in R[\![T]\!]$ is any characteristic power series for $\mathfrak{X}_{\mathrm{Gr}}^S(E_\bullet(\alpha)/K_\infty^-)$.

*Step 2.* Since $\alpha$ is anticyclotomic, for $\alpha \neq 1$ the nonvanishing of $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^+$ and $\mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^+$ is not automatic, but for our choice of $\alpha$ we can show this easily.

**Lemma 7.1.1.** *With $\alpha$ chosen as above, the $p$-adic $L$-functions $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^+$ and $\mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^+$ are both nonzero.*

*Proof.* For $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^+$, this is clear from (7.1) and the congruence of Lemma 2.5.1; and for $\mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^+$ it follows from the relations

$$\mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^+(0) = \mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^-(0) \ \sim_p \ \mathcal{L}_p^{\mathrm{BDP}}(f(\alpha)/K)(0), \tag{7.3}$$

using Proposition 2.4.5 for the last equality up to a $p$-adic unit. □

In light of this nonvanishing, by Corollary 4.1.3 the class $BF_\alpha^+ \in \mathfrak{S}_{\mathrm{ord,rel}}(E_\bullet(\alpha)/K_\infty^+)$ is nonzero, and so by Theorem 4.3.1 the Selmer group $\mathfrak{X}_{\mathrm{ord,str}}(E_\bullet(\alpha^{-1})/K_\infty^+)$ is $\Lambda_K^+$-torsion, with

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord,str}}(E_\bullet(\alpha^{-1})/K_\infty^+)\big) \supset \mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{S}_{\mathrm{ord,rel}}(E_\bullet(\alpha)/K_\infty^+)/\Lambda_K^+ BF_\alpha^+\big) \tag{7.4}$$

in $\Lambda_K^+ \otimes \mathbb{Q}_p$. Note the need to invert $p$ in this divisibility, an ambiguity that we shall remove in the next result.

**Lemma 7.1.2.** *The module $\mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)$ is $\Lambda_K^+$-torsion, with*

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)\big) \supset \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^+\big) \tag{7.5}$$

*in $\Lambda_K^+$.*

*Proof.* Directly from the combination of Proposition 4.2.1, Lemma 7.1.1, and (7.4) we get that $\mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)$ is $\Lambda_K^+$-torsion, with the claimed divisibility holding in $\Lambda_K^+ \otimes \mathbb{Q}_p$. Let $S = \Sigma \smallsetminus \{p, \infty\}$. By Corollary 3.2.3, it follows that $\mathfrak{X}_{\mathrm{ord}}^S(E_\bullet(\alpha)/K_\infty^+)$ is also $\Lambda_K^+$-torsion, with

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}^S(E_\bullet(\alpha)/K_\infty^+)\big) \supset \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^{+,S}\big) \tag{7.6}$$

in $\Lambda_K^+ \otimes \mathbb{Q}_p$. Denote by $\mathcal{F}_{\mathrm{ord}}^S(E_\bullet(\alpha)/K_\infty^+) \in \Lambda_K^+$ a characteristic power series for $\mathfrak{X}_{\mathrm{ord}}^S(E_\bullet(\alpha)/K_\infty^+)$, so from the above we have

$$\mathcal{F}_{\mathrm{ord}}^S(E_\bullet(\alpha)/K_\infty^+) \cdot h = \varpi^k \cdot \mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^{+,S} \tag{7.7}$$

for some $h \in \Lambda_K^+$ and $k \in \mathbb{Z}$. If $k < 0$ there is nothing to show, so assume $k \geq 0$. From Kato's divisibility [Kat04, Thm. 17.4] (refined to an integral statement as in [Wut14, Thm. 16]), Proposition 2.2.4, and Proposition 3.2.1 we have that the untwisted Selmer group $\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)$ is $\Lambda_K^+$-torsion, with the integral divisibility

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)\big) \supset \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^+\big) \tag{7.8}$$

in $\Lambda_K^+$, and so from Proposition 3.2.2 we get that $\mathfrak{X}_{\mathrm{ord}}^S(E_\bullet/K_\infty^+)$ is also $\Lambda_K^+$-torsion, and we have the integral divisibility

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}^S(E_\bullet/K_\infty^+)\big) \supset \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^{+,S}\big) \tag{7.9}$$

in $\Lambda_K^+$. By the congruences of Proposition 3.3.4 and Lemma 2.5.1, it follows from (7.12) that for $\alpha$ sufficiently close to 1 (i.e. taking $m \gg 0$ above) the $\mu$-invariant of $\mathcal{F}_{\mathrm{ord}}^S(E_\bullet(\alpha)/K_\infty^+)$ is at most that of $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^{+,S}$.

Thus from (7.7) we see that $h$ is divisible by $\varpi^k$, and therefore the divisibility (7.6) holds in $\Lambda_K^+$. Together with Corollary 3.2.3, this yields the result. □

From the preceding two lemmas and Proposition 4.2.1, we deduce that $\mathfrak{X}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^+)$ is $\Lambda_K^+$-torsion, with

$$\big(\mathcal{F}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^+)\big) \supset \big(\mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^+\big) \tag{7.10}$$

in $\Lambda_K^{+,\mathrm{ur}}$, where $\mathcal{F}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^+) \in \Lambda_K^+$ is any characteristic power series for $\mathfrak{X}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^+)$. Together with the relations

$$\mathcal{F}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^+)(0) \sim_p \mathcal{F}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^-)(0) \sim_p \mathcal{L}_p^{\mathrm{BDP}}(f(\alpha)/K)(0) \sim_p \mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^-(0) \neq 0$$

following from Proposition 3.3.2, relation (7.2), and Proposition 2.4.5, and noting that

$$\mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^-(0) = \mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^+(0),$$

by easy commutative algebra (see [SU14, Lem. 3.2]) it follows that equality holds in (7.10), so we have

$$\big(\mathcal{F}_{\mathrm{Gr}}(E_\bullet(\alpha)/K_\infty^+)\big) = \big(\mathcal{L}_p^{\mathrm{Gr}}(f(\alpha)/K)^+\big).$$

(Note that conditions (a) and (b) in Lemma 3.3.1 needed for the above application of Proposition 3.3.2 follow from our choice of $\alpha$ with $\mathcal{L}_p^{\mathrm{BDP}}(f(\alpha)/K)(0) \neq 0$ together with the reciprocity law of [CH18, Thm. 5.7] and the result of [CGLS22, Thm. 3.2.1] applied to the Heegner point Kolyvagin system in [CGLS22, §4.1].)

In particular, for $\alpha$ as above sufficiently close to 1, we conclude by Proposition 4.2.1 that $\mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)$ is $\Lambda_K^+$-torsion, with

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}(E_\bullet(\alpha)/K_\infty^+)\big) = \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^+\big). \tag{7.11}$$

*Step 3.* We are now in a position to prove Conjecture 3.1.3 for $\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^+)$.

**Theorem 7.1.3.** *Let $E/\mathbb{Q}$ be an elliptic curve, and $p > 2$ a prime of good reduction for $E$ such that $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ with $\phi|_{G_{\mathbb{Q}_p}} \neq 1, \omega$. Then module $\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^+)$ is $\Lambda_K^+$-torsion, with*

$$\mathrm{ch}_{\Lambda_K^+}(\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^+)) = (\mathcal{L}_p^{\mathrm{PR}}(E/K)^+).$$

*Proof.* By Proposition 3.1.4, it suffices to prove the result of $E_\bullet$. Let $S = \Sigma \smallsetminus \{p, \infty\}$. As shown above, from Kato's work we can deduce that $\mathfrak{X}_{\mathrm{ord}}^S(E_\bullet/K_\infty^+)$ is $\Lambda_K^+$-torsion, and we have the integral divisibility

$$\mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}^S(E_\bullet/K_\infty^+)\big) \supset \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^{+,S}\big) \tag{7.12}$$

in $\Lambda_K^+$. Take a character $\alpha : \Gamma_K^- \to R^\times$ with

$$\alpha \equiv 1 \pmod{\varpi^m}$$

for some $m \gg 0$ so that the equality (7.11) holds. (Note that the argument in *Step 1* and *Step 2* leading to that equality only excludes finitely many $\alpha$.) By Corollary 3.2.3 it follows that $\mathfrak{X}_{\mathrm{ord}}^S(E_\bullet/K_\infty^+)$ is also $\Lambda_K^+$-torsion, and denoting by $\mathcal{F}_{\mathrm{ord}}^S(E_\bullet/K_\infty^+)$ and $\mathcal{F}_{\mathrm{ord}}^S(E_\bullet(\alpha)/K_\infty^+) \in \Lambda_K^+$ characteristic power series for $\mathfrak{X}_{\mathrm{ord}}(E_\bullet/K_\infty^+)$ and $\mathfrak{X}_{\mathrm{ord}}^S(E_\bullet(\alpha)/K_\infty^+)$, respectively, we have

$$\mathcal{F}_{\mathrm{ord}}^S(E_\bullet/K_\infty^+) \equiv \mathcal{F}_{\mathrm{ord}}^S(E_\bullet(\alpha)/K_\infty^+) \equiv \mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^{+,S} \equiv \mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^{+,S} \pmod{\varpi^m}, \tag{7.13}$$

as a consequence of Proposition 3.3.4, the combination of (7.11) and Corollary 3.2.3, and Lemma 2.5.1, respectively. Taking $m \gg 0$, it follows from the congruence (7.13) that $\mathcal{F}_{\mathrm{ord}}^S(E_\bullet/K_\infty^+)$ and $\mathcal{L}_p^{\mathrm{PR}}(E_\bullet/K)^{+,S}$ have *the same* Iwasawa invariants $\lambda$ and $\mu$, and so equality holds in (7.12). By Corollary 3.2.3, this yields the proof of the theorem. □

The proof of Mazur's main conjecture for $E$ now follows easily.

*Proof of Theorem 7.0.1.* Choose an imaginary quadratic field $K$ satisfying hypotheses (disc), (Heeg), and (spl). As before, from [Kat04] and [Wut14] we have the divisibilities

$$\mathrm{ch}_{\Lambda_{\mathbb{Q}}}\big(\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)\big) \supset \big(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})\big), \quad \mathrm{ch}_{\Lambda_{\mathbb{Q}}}\big(\mathfrak{X}_{\mathrm{ord}}(E^K/\mathbb{Q}_\infty)\big) \supset \big(\mathcal{L}_p^{\mathrm{MSD}}(E^K/\mathbb{Q})\big)$$

in $\Lambda_{\mathbb{Q}}$. If $\mathrm{ch}_{\Lambda_{\mathbb{Q}}}(\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)) \neq (\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q}))$ then from Propositions 2.2.4 and Proposition 3.2.1 we conclude that

$$\big(\mathcal{L}_p^{\mathrm{PR}}(E/K)^+\big) \subsetneq \mathrm{ch}_{\Lambda_K^+}\big(\mathfrak{X}_{\mathrm{ord}}(E/K_\infty^+)\big),$$

but this contradicts Theorem 7.1.3. Thus $\mathrm{ch}_{\Lambda_{\mathbb{Q}}}(\mathfrak{X}_{\mathrm{ord}}(E/\mathbb{Q}_\infty)) = (\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q}))$, concluding the proof. □

## References


[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[BCG+20] F. M. Bleher, T. Chinburg, R. Greenberg, M. Kakde, G. Pappas, R. Sharifi, and M. J. Taylor. Higher Chern classes in Iwasawa theory. *Amer. J. Math.*, 142(2):627–682, 2020.

[BCGS23] Ashay Burunagle, Francesc Castella, Giada Grossi, and Christopher Skinner. Nonvanishing of Kolyvagin systems and Iwasawa theory. *preprint*, 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.

[BDP22] Adel Betina, Mladen Dimitrov, and Alice Pozzi. On the failure of Gorensteinness at weight 1 Eisenstein points of the eigencurve. *Amer. J. Math.*, 144(1):227–265, 2022.

[BST21] Ashay Burungale, Christopher Skinner, and Ye Tian. Elliptic curves and Beilinson-Kato elements: rank one aspects. *preprint*, 2021.

[Cas17] Francesc Castella. $p$-adic heights of Heegner points and Beilinson-Flach classes. *J. Lond. Math. Soc. (2)*, 96(1):156–180, 2017.

[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.

[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.

[CW22] Francesc Castella and Xin Wan. The Iwasawa main conjectures for $\mathrm{GL}_2$ and derivatives of $p$-adic $L$-functions. *Adv. Math.*, 400:Paper No. 108266, 45, 2022.

[dS87] Ehud de Shalit. *Iwasawa theory of elliptic curves with complex multiplication*, volume 3 of *Perspectives in Mathematics*. Academic Press, Inc., Boston, MA, 1987. $p$-adic $L$ functions.

[FH95] Solomon Friedberg and Jeffrey Hoffstein. Nonvanishing theorems for automorphic $L$-functions on GL(2). *Ann. of Math. (2)*, 142(2):385–423, 1995.

[FW79] Bruce Ferrero and Lawrence C. Washington. The Iwasawa invariant $\mu_p$ vanishes for abelian number fields. *Ann. of Math. (2)*, 109(2):377–395, 1979.

[Gre89] Ralph Greenberg. Iwasawa theory for $p$-adic representations. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 97–137. Academic Press, Boston, MA, 1989.

[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.

[Gre16] Ralph Greenberg. On the structure of Selmer groups. In *Elliptic curves, modular forms and Iwasawa theory*, volume 188 of *Springer Proc. Math. Stat.*, pages 225–252. Springer, Cham, 2016.

[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.

[Hid81] Haruzo Hida. Congruence of cusp forms and special values of their zeta functions. *Invent. Math.*, 63(2):225–261, 1981.

[Hid85] Haruzo Hida. A $p$-adic measure attached to the zeta functions associated with two elliptic modular forms. I. *Invent. Math.*, 79(1):159–195, 1985.

[Hid07] Haruzo Hida. Non-vanishing modulo $p$ of Hecke $L$-values and application. In *L-functions and Galois representations*, volume 320 of *London Math. Soc. Lecture Note Ser.*, pages 207–269. Cambridge Univ. Press, Cambridge, 2007.

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

[HT93] Haruzo Hida and Jacques Tilouine. Anti-cyclotomic Katz $p$-adic $L$-functions and congruence modules. *Ann. Sci. École Norm. Sup. (4)*, 26(2):189–259, 1993.

[HT94] Haruzo Hida and Jacques Tilouine. On the anticyclotomic main conjecture for CM fields. *Invent. Math.*, 117(1):89–147, 1994.

[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.

[Kat78] Nicholas M. Katz. $p$-adic $L$-functions for CM fields. *Invent. Math.*, 49(3):199–297, 1978.

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

[KLZ17] Guido Kings, David Loeffler, and Sarah Livia Zerbes. Rankin-Eisenstein classes and explicit reciprocity laws. *Camb. J. Math.*, 5(1):1–122, 2017.

[KLZ20] Guido Kings, David Loeffler, and Sarah Livia Zerbes. Rankin-Eisenstein classes for modular forms. *Amer. J. Math.*, 142(1):79–138, 2020.

[KO20] Shinichi Kobayashi and Kazuto Ota. Anticyclotomic main conjecture for modular forms and integral Perrin-Riou twists. In *Development of Iwasawa theory—the centennial of K. Iwasawa's birth*, volume 86 of *Adv. Stud. Pure Math.*, pages 537–594. Math. Soc. Japan, Tokyo, [2020] ©2020.

[LLZ14] Antonio Lei, David Loeffler, and Sarah Livia Zerbes. Euler systems for Rankin-Selberg convolutions of modular forms. *Ann. of Math. (2)*, 180(2):653–771, 2014.

[LLZ15] Antonio Lei, David Loeffler, and Sarah Livia Zerbes. Euler systems for modular forms over imaginary quadratic fields. *Compos. Math.*, 151(9):1585–1625, 2015.

[Loe17] David Loeffler. Images of adelic Galois representations for modular forms. *Glasg. Math. J.*, 59(1):11–25, 2017.

[Maz72] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.
[Maz78] Barry Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.
[Maz84] B. Mazur. Modular curves and arithmetic. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)*, pages 185–211. PWN, Warsaw, 1984.
[Miy06] Toshitsune Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.
[MSD74] Barry Mazur and Peter Swinnerton-Dyer. Arithmetic of Weil curves. *Invent. Math.*, 25:1–61, 1974.
[MW84] Berry Mazur and Andrew Wiles. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.*, 76(2):179–330, 1984.
[PR87a] Bernadette Perrin-Riou. Fonctions $L$ $p$-adiques, théorie d'Iwasawa et points de Heegner. *Bull. Soc. Math. France*, 115(4):399–456, 1987.
[PR87b] Bernadette Perrin-Riou. Points de Heegner et dérivées de fonctions $L$ $p$-adiques. *Invent. Math.*, 89(3):455–510, 1987.
[PR88] Bernadette Perrin-Riou. Fonctions $L$ $p$-adiques associées à une forme modulaire et à un corps quadratique imaginaire. *J. London Math. Soc. (2)*, 38(1):1–32, 1988.
[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.
[PW11] Robert Pollack and Tom Weston. On anticyclotomic $\mu$-invariants of modular forms. *Compos. Math.*, 147(5):1353–1381, 2011.
[Rib83] Kenneth A. Ribet. Mod $p$ Hecke operators and congruences between modular forms. *Invent. Math.*, 71(1):193–205, 1983.
[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.
[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.
[Sch87] Peter Schneider. The $\mu$-invariant of isogenies. *J. Indian Math. Soc. (N.S.)*, 52:159–170 (1988), 1987.
[Ser68] Jean-Pierre Serre. *Abelian $l$-adic representations and elliptic curves*. W. A. Benjamin, Inc., New York-Amsterdam, 1968. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute.
[Ski16] Christopher Skinner. Multiplicative reduction and the cyclotomic main conjecture for $\mathrm{GL}_2$. *Pacific J. Math.*, 283(1):171–200, 2016.
[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 $\mathrm{GL}_2$. *Invent. Math.*, 195(1):1–277, 2014.
[TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.
[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. Iwasawa Main Conjecture for supersingular elliptic curves and BSD conjecture. *preprint*, 2021.
[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.
[Wut14] Christian Wuthrich. On the integrality of modular symbols and Kato's Euler system for elliptic curves. *Doc. Math.*, 19:381–402, 2014.
[Zha14] 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

(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