ON THE ANTICYCLOTOMIC IWASAWA THEORY OF RATIONAL ELLIPTIC CURVES AT EISENSTEIN PRIMES

FRANCESC CASTELLA, GIADA GROSSI, JAEHOON LEE, AND CHRISTOPHER SKINNER

Abstract. Let $E/\mathbb{Q}$ be an elliptic curve and p an odd prime where E has good reduction, and assume that E admits a rational p-isogeny. In this paper we study the anticyclotomic Iwasawa theory of E over an imaginary quadratic field in which p splits, which we relate to the anticyclotomic Iwasawa theory of characters by a variation of the method of Greenberg–Vatsal. As a result of our study we obtain proofs (under relatively mild hypotheses) of Perrin-Riou's Heegner point main conjecture, a p-converse to the theorem of Gross–Zagier and Kolyvagin, and the p-part of the Birch–Swinnerton-Dyer formula in analytic rank 1, for Eisenstein primes p.

Contents

Introduction

0.1. **Statement of the main results.** Let $E/\mathbb{Q}$ be an elliptic curve, and let p be an odd prime of good reduction for E. We say that p is an *Eisenstein prime* (for E) if $E[p]$ is reducible as a $G_{\mathbb{Q}}$-module, where $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is the absolute Galois group of $\mathbb{Q}$ and $E[p]$ denotes the p-torsion of E. Equivalently, p is an Eisenstein prime if E admits a rational p-isogeny. By a result of Fontaine (see [Edi92] for an account), Eisenstein primes are primes of *ordinary* reduction for E, and by Mazur's results [Maz78] in fact $p \in \{3, 5, 7, 13, 37\}$.

Date: August 7, 2021.

Let $p > 2$ be an Eisenstein prime for E, and let K be an imaginary quadratic field such that

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

where v denotes the prime of K above p induced by a fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Denoting by N the conductor of E, assume also that K satisfies the following *Heegner hypothesis*:

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

Under these hypotheses, the anticyclotomic Iwasawa main conjecture for E considered in this paper can be formulated in two different guises. We begin by recalling these, since both formulations will play an important role in the proof of our main results. (Note that for the formulation p can be any odd prime of good ordinary reduction for E.) Let $\Gamma = \mathrm{Gal}(K_\infty/K)$ 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_∞ with $[K_n : K] = p^n$. Set

$$\Lambda := \mathbb{Z}_p[\![\Gamma]\!], \quad \Lambda_{\mathrm{ac}} := \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \quad \Lambda^{\mathrm{ur}} := \Lambda \hat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p^{\mathrm{ur}},$$

where $\mathbb{Z}_p^{\mathrm{ur}}$ is the completion of the ring of integers of the maximal unramified extension of $\mathbb{Q}_p$. Following the work of Bertolini–Darmon–Prasanna [BDP13], there is a p-adic L-function $\mathcal{L}_E \in \Lambda^{\mathrm{ur}}$ interpolating the central critical values of the L-function of f/K, where $f \in S_2(\Gamma_0(N))$ is the newform associated with E, twisted by certain characters of Γ of infinite order. For any subfield $L \subset \overline{\mathbb{Q}}$, let $\mathrm{Sel}_{p^m}(E/L)$ be the Selmer group fitting into the descent exact sequence

$$0 \to E(L) \otimes_{\mathbb{Z}} \mathbb{Z}/p^m\mathbb{Z} \to \mathrm{Sel}_{p^m}(E/L) \to Ш(E/L)[p^m] \to 0.$$

We put $\mathrm{Sel}_{p^\infty}(E/K_\infty) = \varinjlim_m \mathrm{Sel}_{p^m}(E/K_\infty)$, and let

$$\mathfrak{X}_E = \mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{S}_E, \mathbb{Q}_p/\mathbb{Z}_p)$$

be the Pontryagin dual of modified Selmer group $\mathfrak{S}_E$ obtained from $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ by relaxing (resp. imposing triviality) at the places above v (resp. $\bar{v}$).

The following formulation of the anticyclotomic Iwasawa main conjectures for E can be seen as a special case of Greenberg's main conjectures [Gre94].

Conjecture A. *Let $E/\mathbb{Q}$ be an elliptic curve and $p > 2$ a prime of good ordinary reduction for E, and let K be an imaginary quadratic field satisfying* (Heeg) *and* (spl)*. Then $\mathfrak{X}_E$ is Λ-torsion, and*

$$\mathrm{char}_\Lambda(\mathfrak{X}_E)\Lambda^{\mathrm{ur}} = (\mathcal{L}_E)$$

as ideals in Λ^{ur}.

A second formulation, originally due to Perrin-Riou [PR87], is in terms of Heegner points. Although a more general formulation is possible (*cf.* [BT20, §2.3]), here as in [PR87] we assume that

$$\text{the discriminant } D_K \text{ of } K \text{ is odd and } D_K \neq -3, \tag{disc}$$

and do not require hypothesis (spl). Fix a modular parametrization

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

and for any subfield $L \subset \overline{\mathbb{Q}}$ let $\mathrm{Sel}_{p^m}(E/L)$ be the Selmer group fitting into the descent exact sequence

$$0 \to E(L) \otimes_{\mathbb{Z}} \mathbb{Z}/p^m\mathbb{Z} \to \mathrm{Sel}_{p^m}(E/L) \to Ш(E/L)[p^m] \to 0.$$

Via π, the Kummer images of Heegner points on $X_0(N)$ over ring class fields of K of p-power conductor give rise to a class $\kappa_1^{\mathrm{Hg}} \in \mathcal{S}$, where

$$\mathcal{S} = \Bigl(\varprojlim_n \varprojlim_m \mathrm{Sel}_{p^m}(E/K_n)\Bigr) \otimes \mathbb{Q}_p.$$

The group $\mathcal{S}$ is naturally a Λ_{ac}-module, and the class κ_1^{Hg} is known to be non-Λ_{ac}-torsion by results of Cornut and Vatsal [Cor02], [Vat03]. Denote by $\mathcal{H} \subset \mathcal{S}$ the Λ_{ac}-submodule generated by κ_1^{Hg}, and put

$$\mathcal{X} = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p.$$

Conjecture B. *Let $E/\mathbb{Q}$ be an elliptic curve and $p > 2$ a prime of good ordinary reduction for E, and let K be an imaginary quadratic field satisfying* (Heeg) *and* (disc)*. Then $\mathcal{S}$ and $\mathcal{X}$ both have Λ_{ac}-rank one, and*

$$\mathrm{char}_{\Lambda_{\mathrm{ac}}}(\mathcal{X}_{\mathrm{tors}}) = \mathrm{char}_{\Lambda_{\mathrm{ac}}}(\mathcal{S}/\mathcal{H})^2,$$

where $\mathcal{X}_{\mathrm{tors}}$ denotes the Λ_{ac}-torsion submodule of X.

Remark. One can naturally formulate an integral version of Conjecture B, but the results of [PR87] and [How05] show that the terms appearing in the corresponding equality of Λ-module characteristic ideals are in general *not* invariant under isogenies. (With p inverted, i.e., as ideals in $\Lambda_{\rm ac}$, the terms are invariant under isogenies.) On the other hand, it is clear that the principal ideals in $\Lambda^{\rm ur}$ appearing in the equality of Conjecture A depend only on the isogeny class of E.

When p is non-Eisenstein for E, Conjectures A and B have been studied by several authors [Ber95, How04a, How04b, Wan21, Cas17, BCK21], but the residually reducible case remained largely unexplored; in particular, unless E has CM by K (a case that is excluded by our hypothesis (Heeg), but see [BT20] for this case), there seems to be no previous results towards these conjectures when p is an Eisenstein prime for E.

To state our main results on the anticyclotomic Iwasawa theory of E at Eisenstein primes p, write

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

where $\phi, \psi : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ are characters. Note that it follows from the Weil pairing that $\psi = \omega\phi^{-1}$, where ω is the Teichmüller character. Let $G_p \subset G_{\mathbb{Q}}$ be a decomposition group at p.

Our most complete results towards Conjectures A and B are proved under the additional hypothesis that

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

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

As we explain in more detail in the next section, a key step towards Theorem C is the proof of a divisibility in Conjecture B that we establish without the need to assume (spl) (see Theorem 4.1.2). On the other hand, as first observed in [Cas13] and [Wan21], when p splits in K, Conjectures A and B are essentially equivalent (see Proposition 4.2.1). Thus from Theorem 4.1.2 we deduce one of the divisibilities in Conjecture A, which by the analysis of Iwasawa invariants carried out in §§1-2 then yields the equality of ideals in $\Lambda^{\rm ur}$ predicted by Conjecture A. As a result, our analysis together with the aforementioned equivalence also yields the following.

Corollary D. *Let $E/\mathbb{Q}$ be an elliptic curve, $p > 2$ an Eisenstein prime for E, and K an imaginary quadratic field satisfying* (Heeg), (disc), *and* (Sel). *If $E(K)[p] = 0$, then $\mathcal{S}$ and $\mathcal{X}$ both have $\Lambda_{\rm ac}$-rank one, and*

$$\mathrm{char}_{\Lambda_{\rm ac}}(\mathcal{X}_{\rm tors}) \supset \mathrm{char}_{\Lambda_{\rm ac}}(\mathcal{S}/\mathcal{H})^2.$$

Moreover, if in addition K satisfies (spl) *and $\phi|_{G_p} \neq \mathbb{1}, \omega$, then*

$$\mathrm{char}_{\Lambda_{\rm ac}}(\mathcal{X}_{\rm tors}) = \mathrm{char}_{\Lambda_{\rm ac}}(\mathcal{S}/\mathcal{H})^2,$$

and hence Conjecture B holds.

Note that in both Theorem C and Corollary D, the elliptic curve E is allowed to have complex multiplication (necessarily by an imaginary quadratic field different from K).

With a judicious choice of K, Theorem C also has applications to the arithmetic over $\mathbb{Q}$ of rational elliptic curves. Specifically, for Eisenstein prime p, we obtain a p-converse to the celebrated theorem

$$\text{(0.1)} \qquad \mathrm{ord}_{s=1}\, L(E,s) = r \in \{0,1\} \implies \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r \text{ and } \#\text{Ш}(E/\mathbb{Q}) < \infty,$$

of Gross–Zagier and Kolyvagin. (The case of Eisenstein primes eluded the methods of [Ski20] and [Zha14], which require $E[p]$ to be absolutely irreducible as a $G_{\mathbb{Q}}$-module.)

Theorem E. *Let $E/\mathbb{Q}$ be an elliptic curve and $p > 2$ an Eisenstein prime for E, so that $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ as $G_{\mathbb{Q}}$-modules, and assume that $\phi|_{G_p} \neq \mathbb{1}, \omega$. Let $r \in \{0,1\}$. Then the following implication holds:*

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

and so $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r$ and $\#\text{Ш}(E/\mathbb{Q}) < \infty$.

Note that if $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r$ and $\#\text{Ш}(E/\mathbb{Q})[p^\infty] < \infty$ then $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = r$, whence the p-converse to (0.1). We also note that for $p = 3$, Theorem E together with the recent work of Bhargava–Klagsbrun–Lemke Oliver–Shnidman [BKLOS19] on the average 3-Selmer rank for abelian varieties in quadratic twist families, provides additional evidence towards Goldfeld's conjecture [Gol79] for elliptic curves $E/\mathbb{Q}$ admitting a rational 3-isogeny (see Corollary 5.2.3 and Remark 5.2.4, and see also [KL19] for earlier results along these lines).

Another application of Theorem C is the following.

Theorem F. *Under the hypotheses of Theorem E, assume in addition that ϕ is either ramified at p and odd, or unramified at p and even. If* $\mathrm{ord}_{s=1}L(E,s)=1$, *then*

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

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* ω_E, *and*
- $c_\ell(E/\mathbb{Q})$ *is the Tamagawa number of E at the prime ℓ.*

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

0.2. **Method of proof and outline of the paper.** Let us explain some of the ideas that go into the proof of our main results, beginning with the proof of Theorem C. As in [GV00], our starting point is Greenberg's old observation [Gre77] that a "main conjecture" should be equivalent to an imprimitive one. More precisely, in the context of Theorem C, for Σ any finite set of non-archimedean primes of K not containing any of the primes above p, this translates into the expectation that the Σ-imprimitive Selmer group $\mathfrak{X}_E^\Sigma$, obtained by relaxing the local condition defining (the Pontryagin dual of) $\mathfrak{X}_E$ at the primes $w\in\Sigma$, is Λ-torsion with

$$\mathrm{char}_\Lambda(\mathfrak{X}_E^\Sigma)\Lambda^{\mathrm{ur}}\overset{?}{=}(\mathcal{L}_E^\Sigma)\tag{0.2}$$

as ideals in Λ^{ur}, where $\mathcal{L}_E^\Sigma:=\mathcal{L}_E\cdot\prod_{w\in\Sigma}\mathcal{P}_w(E)$ for certain elements in $\mathcal{P}_w(E)\in\Lambda$ interpolating, for varying characters χ of Γ, the w-local Euler factor of $L(E/K,\chi,s)$ evaluated $s=1$.

A key advantage of the imprimitive main conjecture (0.2) is that (unlike the original conjecture), for suitable choices of Σ, its associated Iwasawa invariants are well-behaved with respect to congruences mod p. Identifying Λ with the power series ring $\mathbb{Z}_p[\![T]\!]$ by setting $T=\gamma-1$ for a fixed topological generator $\gamma\in\Gamma$, recall that by the Weierstrass preparation theorem, every nonzero $g\in\Lambda$ can be uniquely written in the form

$$g=u\cdot p^\mu\cdot Q(T),$$

with $u\in\Lambda^\times$, $\mu=\mu(g)\in\mathbb{Z}_{\geqslant0}$, and $Q(T)\in\mathbb{Z}_p[T]$ a distinguished polynomial of degree $\lambda(g)$. The constants λ and μ are the so-called *Iwasawa invariants* of g. For a torsion Λ-module $\mathfrak{X}$ we let $\lambda(\mathfrak{X})$ and $\mu(\mathfrak{X})$ be the Iwasawa invariants of a characteristic power series for $\mathfrak{X}$, and for a nonzero $\mathcal{L}\in\Lambda^{\mathrm{ur}}$ we let $\lambda(\mathcal{L})$ and $\mu(\mathcal{L})$ be the Iwasawa invariants of any element of Λ generating the same Λ^{ur}-ideal as $\mathcal{L}$.

As a first step towards Theorem C, we deduce from the $G_{\mathbb{Q}}$-module isomorphism $E[p]^{ss}=\mathbb{F}_p(\phi)\oplus\mathbb{F}_p(\psi)$ that, taking Σ to consist of primes that are split in K and containing all the primes of bad reduction for E, the module $\mathfrak{X}_E^\Sigma$ is Λ-torsion with

$$\mu(\mathfrak{X}_E^\Sigma)=0\quad\text{and}\quad\lambda(\mathfrak{X}_E^\Sigma)=\lambda(\mathfrak{X}_\phi^\Sigma)+\lambda(\mathfrak{X}_\psi^\Sigma),\tag{0.3}$$

where $\mathfrak{X}_\phi^\Sigma$ and $\mathfrak{X}_\psi^\Sigma$ are anticyclotomic Selmer groups (closely related to the Pontryagin dual of certain class groups) for the Teichmüller lifts of ϕ and ψ, respectively. The proof of (0.3), which is taken up in §1, uses Rubin's work [Rub91] on the Iwasawa main conjecture for imaginary quadratic fields and Hida's work [Hid10] on the vanishing of the μ-invariant of p-adic Hecke L-functions.

On the other hand, in §2 we deduce from the main result of [Kri16] that for such Σ one also has

$$\mu(\mathcal{L}_E^\Sigma)=0\quad\text{and}\quad\lambda(\mathcal{L}_E^\Sigma)=\lambda(\mathcal{L}_\phi^\Sigma)+\lambda(\mathcal{L}_\psi^\Sigma),\tag{0.4}$$

where $\mathcal{L}_\phi^\Sigma$ and $\mathcal{L}_\psi^\Sigma$ are Σ-imprimitive anticyclotomic Katz p-adic L-functions attached to ϕ and ψ, respectively.

With equalities (0.3) and (0.4) in hand, it follows easily that to prove the equality of characteristic ideals in Conjecture A it suffices to prove one of the predicted divisibilities in $\Lambda^{\mathrm{ur}}[\frac{1}{p}]$. In §3, by combining Howard's approach to proving Iwasawa-theoretic divisibilities [How04a] with a Kolyvagin system argument along the lines of Nekovář's [Nek07] (but adapted for twists by infinite order characters and for obtaining a bound on the length of Tate–Shafarevich group and not just an annihilator), we prove the main result towards one of the divisibilities in Conjecture B: $\mathrm{char}_{\Lambda_{\mathrm{ac}}}(\mathcal{X}_{\mathrm{tors}})$ divides $\mathrm{char}_{\Lambda_{\mathrm{ac}}}(\mathcal{S}/\mathcal{H})^2$ in $\Lambda_{\mathrm{ac}}[\frac{1}{T}]$, and even in Λ_{ac} assuming (Sel). As already noted, hypotheses (spl) and $\phi|_{G_p}\neq\mathbb{1},\omega$ are not needed at this point. This yields a corresponding divisibility in (0.2), from which the proof of Theorem C follows easily. The details of the final argument, and the deduction of Corollary D, are given in §4. The additional hypothesis (Sel) is required to circumvent the growth of the 'error term' in our Kolyvagin system arguments in the cases of twists by anticyclotomic characters

p-adically close to the trivial character. The arguments in §3 apply equally well to both the residually reducible and residually irreducible cases.

Finally, the proofs of Theorems E and F are given in §5, and they are both obtained as an application of Theorem C for a suitably chosen K. In particular, the proof of Theorem F requires knowing the p-part of the Birch–Swinnerton-Dyler formula in analytic rank 0 for the quadratic twist E^K; this is deduced in Theorem 5.1.4 from the results of Greenberg–Vatsal [GV00], and this is responsible for the additional hypotheses on ϕ placed in Theorem F.

0.3. Examples.

To illustrate Theorem F, 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 $J[5]^{ss} = \mathbb{Z}/5\mathbb{Z} \oplus \mu_p$ as $G_{\mathbb{Q}}$-modules (J has a rational 5-torsion point). If ψ is an even quadratic character such that $\psi(5) = -1$, corresponding to a real quadratic field $\mathbb{Q}(\sqrt{c})$ in which 5 is inert, then the twist $E = J_c$ of J by ψ satisfies the hypotheses of Theorem E with $p = 5$. Since the root number of J is -1 (being of analytic rank one), by [FH95, Thm. B.2] we can find infinitely many ψ as above for which the associated twist $E = J_c$ also has analytic rank one, and therefore for which Theorem F applies.

One can proceed similarly for $p = 3$ (resp. $p = 7$), taking real quadratic twists of, for example, the elliptic curve $y^2 + y = x^3 + x^2 - 7x + 5$ of conductor 91 (resp. $y^2 + xy + y = x^3 - x^2 - 19353x + 958713$ of conductor 574). For $p = 13$ (resp. $p = 37$), one can do the same, possibly choosing the quadratic character to be odd and/or imposing conditions at some bad primes depending on the character describing the kernel of the isogeny (which is not trivial in these cases) in order to apply [FH95, Thm. B.2]. One could consider, for example, twists of the elliptic curve $y^2 + y = x^3 - 21x + 40$ of conductor 441 (resp. $y^2 + xy + y = x^3 + x^2 - 8x + 6$ of conductor 1225).

We also note that, for each of the four primes primes above, $p = 3, 5, 7, 13$, there are infinitely many distinct j-invariants to which Theorem F applies, as $X_0(p)$ has genus 0 in these cases.

0.4. Relation to previous works.

Results in the same vein as (0.3) and (0.4) were first obtained by Greenberg–Vatsal [GV00] in the cyclotomic setting; combined with Kato's Euler system divisibility [Kat04], these results led to their proof of the cyclotomic Iwasawa main conjecture for rational elliptic curves at Eisenstein primes p (under some hypotheses on the kernel of the associated rational p-isogeny). This paper might be seen as an extension of the Greenberg–Vatsal method for Eisenstein primes to the anticyclotomic setting. However, for the anticyclotomic Selmer groups and L-functions considered in this paper we are able to avoid the possible variation within an isogeny class of elliptic curves of the μ-invariants and periods, which must be dealt with in [GV00]. In large part this is because the periods in the corresponding p-adic families are the CM periods of Hecke characters and not the periods of the elliptic curve. Consequently, the methods are slightly more robust and the resulting applications somewhat more general. The μ-invariants of anticyclotomic Selmer groups and p-adic L-functions were also studied in [PW11], but for different Selmer conditions and hypotheses on K (in fact, under the hypothesis (Heeg) the p-adic L-function in [PW11] vanishes identically and the Selmer group is not Λ-cotorsion).

The ensuing applications of Theorems C and Corollary D to the p-converse of the Gross–Zagier–Kolyvagin theorem (Theorem E) and the p-part of the Birch–Swinnerton-Dyer formula in analytic rank 1 (Theorem F) covers primes p that were either left untouched by the recent works in these directions [Ski20, Ven16, BBV16, Zha14, SZ14, JSW17, Cas18, BPS18] (where p is assumed to be non-Eisenstein), or extending previous works [Tia14, CLTZ15, CCL18] ($p = 2$), [KL19] ($p = 3$), [BT20] (CM cases). Many of these results (especially [Ski20] and [JSW17]) also rely on progress toward Conjecture A in the residually irreducible case. Such progress has generally come via Eisenstein congruences on higher rank unitary groups and has explicitly excluded the Eisenstein cases considered in this paper.

0.5. Weight two newforms.

The methods and results of this paper should easily extend to cuspidal newforms of weight two and trivial character that are congruent to Eisenstein series at a prime above p. We have focused on the case of elliptic curves in the interest of not obscuring the main features of our argument with cumbersome notation. The general case will be addressed in later work that will also consider higher weight forms as well as Hilbert modular forms.

0.6. **Acknowledgements.** This paper has its origins in one of the projects proposed by F.C. and C.S. at the 2018 Arizona Winter School on Iwasawa theory, and we would like to thank the organizers for making possible a uniquely stimulating week during which G.G. and J.L. made very substantial progress on this project. We also thank Ashay Burungale and the anonymous referees for many helpful comments and suggestions on an earlier draft of this paper. G.G. is grateful to Princeton University for the hospitality during a visit to F.C. and C.S. in February-March 2019. During the preparation of this paper, F.C. was partially supported by the NSF grant DMS-1946136 and DMS-2101458; G.G. was supported by the Engineering and Physical Sciences Research Council [EP/L015234/1], the EPSRC Centre for Doctoral Training in Geometry and Number Theory (The London School of Geometry and Number Theory), University College London; C.S. was partially supported by the Simons Investigator Grant #376203 from the Simons Foundation and by the NSF grant DMS-1901985.

1. Algebraic side

In this section we prove Theorem 1.5.1 below, relating the anticyclotomic Iwasawa invariants of an elliptic curve $E/\mathbb{Q}$ at a prime p with $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}(\psi)$ to the anticyclotomic Iwasawa invariants of the characters ϕ and ψ.

Throughout, we fix a prime $p > 2$ and an embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, and let $K \subset \overline{\mathbb{Q}}$ be an imaginary quadratic field in which $p = v\bar{v}$ splits, with v the prime of K above p induced by ι_p. We also fix an embedding $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

Let $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K) \subset G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and for each place w of K let $I_w \subset G_w \subset G_K$ be corresponding inertia and decomposition groups. Let $\mathrm{Frob}_w \in G_w/I_w$ be the arithmetic Frobenius. For the prime $v \mid p$ we assume G_v is chosen so that it is identified with $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ via ι_p.

Let $\Gamma = \mathrm{Gal}(K_\infty/K)$ be the Galois group of the anticyclotomic $\mathbb{Z}_p$-extension K_∞ of K, and let $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$ be the anticyclotomic Iwasawa algebra. We shall often identify Λ with the power series ring $\mathbb{Z}_p[\![T]\!]$ by setting $T = \gamma - 1$ for a fixed topological generator $\gamma \in \Gamma$.

1.1. Local cohomology groups of characters.

Let $\theta : G_K \to \mathbb{F}_p^\times$ be a character with conductor divisible only by primes that are split in K. Via the Teichmüller lift $\mathbb{F}_p^\times \hookrightarrow \mathbb{Z}_p^\times$, we shall also view θ as taking values in $\mathbb{Z}_p^\times$. Set

$$M_\theta = \mathbb{Z}_p(\theta) \otimes_{\mathbb{Z}_p} \Lambda^\vee,$$

where $(-)^\vee = \mathrm{Hom}_{\mathrm{cts}}(-, \mathbb{Q}_p/\mathbb{Z}_p)$ for topological $\mathbb{Z}_p$-modules. The module M_θ is equipped with a G_K-action via $\theta \otimes \Psi^{-1}$, where $\Psi : G_K \to \Lambda^\times$ is the character arising from the projection $G_K \twoheadrightarrow \Gamma$.

In this section, we study the local cohomology of M_θ at various primes w of K.

1.1.1. *$w \nmid p$ split in K.* Let w be a prime of K lying over a prime $\ell \neq p$ split in K, and let $\Gamma_w \subset \Gamma$ be the corresponding decomposition group. Let $\gamma_w \in \Gamma_w$ be the image of Frob_w, and set

$$\mathcal{P}_w(\theta) = P_w(\ell^{-1}\gamma_w) \in \Lambda, \tag{1.1}$$

where $P_w = \det(1 - \mathrm{Frob}_w X | \mathbb{Q}_p(\theta)_{I_w})$ is the Euler factor at w of the L-function of θ.

Lemma 1.1.1. *The module $\mathrm{H}^1(K_w, M_\theta)^\vee$ is Λ-torsion with*

$$\mathrm{char}_\Lambda(\mathrm{H}^1(K_w, M_\theta)^\vee) = (\mathcal{P}_w(\theta)).$$

In particular, $\mathrm{H}^1(K_w, M_\theta)^\vee$ has μ-invariant zero.

Proof. Since ℓ splits in K, it follows from class field theory that the index $[\Gamma : \Gamma_w]$ is finite (i.e., w is finitely decomposed in K_∞/K). Thus the argument proving [GV00, Prop. 2.4] can be immediately adapted to yield this result. □

1.1.2. *$w \mid p$.* Recall that we assume that $p = v\bar{v}$ splits in K. We begin by recording the following commutative algebra lemma, which shall also be used later in the paper.

Lemma 1.1.2. *Let X be a finitely generated Λ-module satisfying the following two properties:*

- *$X[T] = 0$,*
- *X/TX is a free $\mathbb{Z}_p$-module of rank r.*

Then X is a free Λ-module of rank r.

Proof. From Nakayama's lemma we obtain a surjection $\pi : \Lambda^r \twoheadrightarrow X$ which becomes an isomorphism $\bar{\pi}$ after reduction modulo T. Letting $K = \ker(\pi)$, from the snake lemma we deduce the exact sequence

$$0 \to K/TK \to (\Lambda/T\Lambda)^r \xrightarrow{\bar{\pi}} X/TX \to 0.$$

Thus $K/TK = 0$, and so $K = 0$ by another application of Nakayama's lemma. □

Let $\omega : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ be the mod p cyclotomic character. Let w be a prime of K above p.

Proposition 1.1.3. *Assume that $\theta|_{G_w} \neq \mathbb{1}, \omega$. Then:*

(i) *The restriction map*

$$r_w : \mathrm{H}^1(K_w, M_\theta) \to \mathrm{H}^1(I_w, M_\theta)^{G_w/I_w}$$

is an isomorphism.

(ii) $\mathrm{H}^1(K_w, M_\theta)$ *is Λ-cofree of rank 1.*

Proof. The map r_w is clearly surjective, so it suffices to show injectivity. Since G_w/I_w is pro-cyclic,

$$\ker(r_w) \simeq M_\theta^{I_w}/(\mathrm{Frob}_w - 1)M_\theta^{I_w},$$

where Frob_w is a Frobenius element at w. Taking Pontryagin duals to the exact sequence

$$0 \to M_\theta^{G_w} \to M_\theta^{I_w} \xrightarrow{\mathrm{Frob}_w - 1} M_\theta^{I_w} \to M_\theta^{I_w}/(\mathrm{Frob}_w - 1)M_\theta^{I_w} \to 0$$

and using the vanishing of $M_\theta^{G_w}$ (which follows from $\theta|_{G_w} \neq \mathbb{1}$) we deduce a Λ-module surjection

$$(M_\theta^\vee)_{I_w} \twoheadrightarrow (M_\theta^\vee)_{I_w}, \tag{1.2}$$

hence an isomorphism (by the Noetherian property of Λ). Since the kernel of (1.2) is isomorphic to $\ker(r_w)^\vee$, (i) follows. For (ii), in light of Lemma 1.1.2, letting

$$X := \mathrm{H}^1(K_w, M_\theta)^\vee,$$

it suffices to show that $X[T] = 0$ and the quotient X/TX is $\mathbb{Z}_p$-free of rank 1. Taking cohomology for the exact sequence $0 \to \mathbb{Q}_p/\mathbb{Z}_p(\theta) \to M_\theta \xrightarrow{\times T} M_\theta \to 0$ we obtain

$$\frac{\mathrm{H}^1(K_w, M_\theta)}{T\mathrm{H}^1(K_w, M_\theta)} = 0, \qquad \mathrm{H}^1(K_w, \mathbb{Q}_p/\mathbb{Z}_p(\theta)) \simeq \mathrm{H}^1(K_w, M_\theta)[T], \tag{1.3}$$

using that $\mathrm{H}^2(K_w, M_\theta) = 0$ (which follows from $\theta|_{G_w} \neq \omega$) for the first isomorphism and $\mathrm{H}^0(K_w, M_\theta) = 0$ for the second. The first isomorphism shows that $X[T] = 0$. On the other hand, taking cohomology for the exact sequence $0 \to \mathbb{F}_p(\theta) \to \mathbb{Q}_p/\mathbb{Z}_p(\theta) \xrightarrow{p} \mathbb{Q}_p/\mathbb{Z}_p(\theta) \to 0$ and using that $\theta|_{G_w} \neq \omega$ we obtain

$$\frac{\mathrm{H}^1(K_w, \mathbb{Q}_p/\mathbb{Z}_p(\theta))}{p\mathrm{H}^1(K_w, \mathbb{Q}_p/\mathbb{Z}_p(\theta))} \simeq \mathrm{H}^2(K_w, \mathbb{F}_p(\theta)) = 0,$$

which together with the second isomorphism in (1.3) shows that $X/TX \simeq \mathrm{H}^1(K_w, \mathbb{Q}_p/\mathbb{Z}_p(\theta))^\vee$ is $\mathbb{Z}_p$-free of rank 1 (the value of the rank following from the local Euler characteristic formula), concluding the proof. □

1.2. **Selmer groups of characters.** As in the preceding section, let $\theta : G_K \to \mathbb{F}_p^\times$ be a character whose conductor is divisible only by primes split in K (that is, which are unramified over $\mathbb{Q}$ and have degree one).

Let Σ be a finite set of places of K containing ∞ and the primes dividing p or the conductor of θ and such that every finite place in Σ is split in K, and denote by K^Σ the maximal extension of K unramified outside Σ.

Definition 1.2.1. The *Selmer group* of θ is

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_\theta) := \ker\biggl\{\mathrm{H}^1(K^\Sigma/K, M_\theta) \to \prod_{w \in \Sigma, w \nmid p} \mathrm{H}^1(K_w, M_\theta) \times \mathrm{H}^1(K_{\bar{v}}, M_\theta)\biggr\},$$

and letting $S = \Sigma \setminus \{v, \bar{v}, \infty\}$, we define the *$S$-imprimitive Selmer group* of θ by

$$\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta) := \ker\biggl\{\mathrm{H}^1(K^\Sigma/K, M_\theta) \to \mathrm{H}^1(K_{\bar{v}}, M_\theta)\biggr\}.$$

Replacing M_θ by $M_\theta[p]$ in the above definitions, we obtain the *residual Selmer group* $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_\theta[p])$ and its S-imprimitive variant $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta[p])$.

It is well-known that the above groups are cofinitely generated over the corresponding Iwasawa algebra (Λ and Λ/p), and that the Selmer group and residual Selmer groups are independent of the choice of the set Σ as above.

The following result, combining work of Rubin and Hida, will play a key role in our proofs.

Theorem 1.2.2 (Rubin, Hida). *Assume that $\theta|_{G_{\bar{v}}} \neq \mathbb{1}, \omega$. Then $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_\theta)^\vee$ is a torsion Λ-module with μ-invariant zero.*

Proof. Let $K_\theta \subset \overline{\mathbb{Q}}$ be the fixed field of $\ker(\theta)$, and set $\Delta_\theta = \mathrm{Gal}(K_\theta/K)$. The restriction map

$$\mathrm{H}^1(K^\Sigma/K, M_\theta) \to \mathrm{H}^1(K^\Sigma/K_\theta, M_\theta)^{\Delta_\theta}$$

is an isomorphism (since $p \nmid |\Delta_\theta|$), which combined with Shapiro's lemma gives rise to an identification

$$\mathrm{H}^1(K^\Sigma/K_\theta, M_\theta) \simeq \mathrm{Hom}_{\mathrm{cts}}((\mathcal{X}_\infty^\Sigma)^\theta, \mathbb{Q}_p/\mathbb{Z}_p), \tag{1.4}$$

where $\mathcal{X}_\infty^\Sigma = \mathrm{Gal}(\mathcal{M}_\infty^\Sigma/K_\infty K_\theta)$ is the Galois group of the maximal abelian pro-p extension of $K_\infty K_\theta$ unramified outside Σ, and $(\mathcal{X}_\infty^\Sigma)^\theta$ is the θ-isotypic component of $\mathcal{X}_\infty^\Sigma$ for the action of Δ_θ, identified as a subgroup of $\mathrm{Gal}(K_\infty K_\theta/K)$ via the decomposition $\mathrm{Gal}(K_\infty K_\theta/K) \simeq \Gamma \times \Delta_\theta$.

Now, by [PW11, Rem. 3.2] (since the primes $w \nmid p$ in Σ are finitely decomposed in K_∞/K) and Proposition 1.1.3(i), the Selmer group $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_\theta)$ is the same as the one defined by the unramified local conditions, i.e., as

$$\ker\biggl\{\mathrm{H}^1(K^\Sigma/K, M_\theta) \to \prod_{w \in \Sigma, w \nmid p} \mathrm{H}^1(I_w, M_\theta)^{G_v/I_v} \times \mathrm{H}^1(I_{\bar{v}}, M_\theta)^{G_{\bar{v}}/I_{\bar{v}}}\biggr\},$$

and so under the identification (1.4) we obtain

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_\theta) \simeq \mathrm{Hom}_{\mathrm{cts}}(\mathcal{X}_\infty^\theta, \mathbb{Q}_p/\mathbb{Z}_p)$$

where $\mathcal{X}_\infty = \mathrm{Gal}(\mathcal{M}_\infty/K_\infty K_\theta)$ is the Galois group of the maximal abelian pro-p extension of $K_\infty K_\theta$ unramified outside v. Thus from the works of Rubin [Rub91], which identifies $\mathrm{char}_\Lambda(\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_\theta)^\vee)$ with the ideal generated by an anticyclotomic projection of a Katz p-adic L-function, and Hida [Hid10], proving the vanishing of the μ-invariant of such anticyclotomic p-adic L-functions, we obtain the theorem. □

Remark 1.2.3. Following the notations introduced in the proof of Theorem 1.2.2, and letting $\mathcal{X}_\infty^{sp} = \mathrm{Gal}(\mathcal{M}_\infty^{sp}/K_\infty K_\theta)$ be the Galois group of the maximal abelian pro-p extension of $K_\infty K_\theta$ unramified outside v and in which the primes above $\bar{v}$ split completely, Proposition 1.1.3(i) shows $(\mathcal{X}_\infty^\Sigma)^\theta = (\mathcal{X}_\infty^{sp})^\theta$.

The next two results will allow us to determine $\lambda(\mathfrak{X}_\theta^S)$ in terms of the residual Selmer group $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta[p])$. In brief, the fact that $\mathfrak{X}_\theta^S$ has no nonzero pseudo-null Λ-submodules (shown in Proposition 1.2.5 below) yields the equality $\lambda(\mathfrak{X}_\theta^S) = \dim_{\mathbb{F}_p}\bigl(\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta)[p]\bigr)$, which combined with the next lemma yields the desired result.

Lemma 1.2.4. *Assume that $\theta|_{G_{\bar{v}}} \neq \mathbb{1}$. Then*

$$\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta[p]) \simeq \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta)[p].$$

Proof. The hypothesis on θ implies in particular that $\mathrm{H}^0(K, \mathbb{F}_p(\theta)) = 0$, and so $\mathrm{H}^0(K, M_\theta) = 0$. Thus the natural map

$$\mathrm{H}^1(K^\Sigma/K, M_\theta[p]) \to \mathrm{H}^1(K^\Sigma/K, M_\theta)[p]$$

induced by multiplication by p on M_θ is an isomorphism. To conclude it suffices to check that the natural map $r_{\bar{v}} : \mathrm{H}^1(K_{\bar{v}}, M_\theta[p]) \to \mathrm{H}^1(K_{\bar{v}}, M_\theta)[p]$ is an injection, but since $\mathrm{H}^0(K_{\bar{v}}, \mathbb{F}_p(\theta)) = 0$ by the hypothesis, the same argument as above shows that $r_{\bar{v}}$ is an isomorphism. □

Let

$$\mathfrak{X}_\theta^S := \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta)^\vee \quad \text{and} \quad \mathfrak{X}_\theta := \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_\theta)^\vee,$$

and recall the element $\mathcal{P}_w(\theta) \in \Lambda$ introduced in (1.1).

Proposition 1.2.5. *Assume that $\theta|_{G_{\bar{v}}} \neq \mathbb{1}, \omega$. Then $\mathfrak{X}_\theta^S$ is a torsion Λ-module with μ-invariant zero and its λ-invariant satisfies*

$$\lambda(\mathfrak{X}_\theta^S) = \lambda(\mathfrak{X}_\theta) + \sum_{w \in \Sigma, w \nmid p} \lambda(\mathcal{P}_w(\theta)).$$

Moreover, $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta[p])$ *is finite and*

$$\dim_{\mathbb{F}_p}\big(\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta[p])\big) = \lambda(\mathfrak{X}^S_\theta).$$

Proof. Since $\mathfrak{X}_\theta$ is Λ-torsion by Theorem 1.2.2 and the Cartier dual $\mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p(\theta), \mu_{p^\infty})$ has no non-trivial G_{K_∞}-invariants, from [PW11, Prop. A.2] we obtain that the restriction map in the definition of $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_\theta)$ is surjective, and so the sequence

$$0 \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_\theta) \to \mathrm{H}^1(K^\Sigma/K, M_\theta) \to \prod_{w\in\Sigma, w\nmid p} \mathrm{H}^1(K_w, M_\theta) \times \mathrm{H}^1(K_{\bar{v}}, M_\theta) \to 0 \tag{1.5}$$

is exact. From the definitions, this readily yields the exact sequence

$$0 \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_\theta) \to \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta) \to \prod_{w\in S} \mathrm{H}^1(K_w, M_\theta) \to 0, \tag{1.6}$$

which combined with Theorem 1.2.2 and Lemma 1.1.1 gives the first part of the proposition.

For the second part, note that $\mathrm{H}^2(K^\Sigma/K, M_\theta) = 0$. (Indeed, by the Euler characteristic formula, the Λ-cotorsionness of $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_\theta)$ implies that $\mathrm{H}^2(K^\Sigma/K, M_\theta)$ is Λ-cotorsion; being Λ-cofree, as follows immediately from the fact that $\mathrm{Gal}(K^\Sigma/K)$ has cohomological dimension 2, it must vanish.) Thus from the long exact sequence in cohomology induced by $0 \to \mathbb{Q}_p/\mathbb{Z}_p(\theta) \to M_\theta \xrightarrow{\times T} M_\theta \to 0$ we obtain the isomorphism

$$\frac{\mathrm{H}^1(K^\Sigma/K, M_\theta)}{T\mathrm{H}^1(K^\Sigma/K, M_\theta)} \simeq \mathrm{H}^2(K^\Sigma/K, \mathbb{Q}_p/\mathbb{Z}_p(\theta)).$$

Since $\mathrm{H}^2(K^\Sigma/K, \mathbb{Q}_p/\mathbb{Z}_p(\theta))$ is $\mathbb{Z}_p$-cofree (because $\mathrm{Gal}(K^\Sigma/K)$ has cohomological dimension 2), it follows that $\mathrm{H}^1(K^\Sigma/K, M_\theta)^\vee$ has no nonzero pseudo-null Λ-submodules (*cf.* [Gre89, Prop. 5]), and since (1.5) and (1.6) readily imply that

$$\mathfrak{X}^S_\theta \simeq \frac{\mathrm{H}^1(K^\Sigma/K, M_\theta)^\vee}{\mathrm{H}^1(K_{\bar{v}}, M_\theta)^\vee}$$

as Λ-modules, by Proposition 1.1.3(iii) and [GV00, Lem. 2.6] we conclude that also $\mathfrak{X}^S_\theta$ has no nonzero pseudo-null Λ-submodules. Finally, since $\mathfrak{X}^S_\theta$ is Λ-torsion with μ-invariant zero by Theorem 1.2.2, the finiteness of $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta)[p]$ (and therefore of $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta[p])$ by Lemma 1.2.4) follows from the structure theorem. It also follows that $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta)$ is divisible. In particular,

$$\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda,$$

where $\lambda = \lambda(\mathfrak{X}^S_\theta)$, which together with Lemma 1.2.4 gives the final formula for the λ-invariant. □

The following corollary will be used crucially in the next section.

Corollary 1.2.6. *Assume that* $\theta|_{G_{\bar{v}}} \neq \mathbb{1}, \omega$. *Then* $\mathrm{H}^2(K^\Sigma/K, M_\theta[p]) = 0$ *and the sequence*

$$0 \to \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta[p]) \to \mathrm{H}^1(K^\Sigma/K, M_\theta[p]) \to \mathrm{H}^1(K_{\bar{v}}, M_\theta[p]) \to 0$$

is exact.

Proof. In the course of the proof of Proposition 1.2.5 we showed that $\mathrm{H}^2(K^\Sigma/K, M_\theta) = 0$, and so the cohomology long exact sequence induced by multiplication by p on M_θ yields an isomorphism

$$\frac{\mathrm{H}^1(K^\Sigma/K, M_\theta)}{p\mathrm{H}^1(K^\Sigma/K, M_\theta)} \simeq \mathrm{H}^2(K^\Sigma/K, M_\theta[p]). \tag{1.7}$$

On the other hand, from the exactness of (1.5) we deduce the exact sequence

$$0 \to \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta) \to \mathrm{H}^1(K^\Sigma/K, M_\theta) \to \mathrm{H}^1(K_{\bar{v}}, M_\theta) \to 0. \tag{1.8}$$

Since we also showed in that proof that $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta)$ is divisible, and $\mathrm{H}^1(K_{\bar{v}}, M_\theta)$ is Λ-cofree by Proposition 1.1.3(ii), it follows from (1.8) that $\mathrm{H}^1(K^\Sigma/K, M_\theta)^\vee$ has no p-torsion, and so

$$\mathrm{H}^2(K^\Sigma/K, M_\theta[p]) = 0$$

by (1.7), giving the first claim in the statement.

For the second claim, consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta) \arrow[r] \arrow[d, "p"] & \mathrm{H}^1(K^\Sigma/K, M_\theta) \arrow[r] \arrow[d, "p"] & \mathrm{H}^1(K_{\bar{v}}, M_\theta) \arrow[r] \arrow[d, "p"] & 0 \\
0 \arrow[r] & \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta) \arrow[r] & \mathrm{H}^1(K^\Sigma/K, M_\theta) \arrow[r] & \mathrm{H}^1(K_{\bar{v}}, M_\theta) \arrow[r] & 0,
\end{tikzcd}$$

where the vertical maps are the natural ones induced by multiplication by p on M_θ. Since $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta)$ is divisible, the snake lemma applied to this diagram yields the exact sequence

$$0 \to \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\theta)[p] \to \mathrm{H}^1(K^\Sigma/K, M_\theta)[p] \to \mathrm{H}^1(K_{\bar{v}}, M_\theta)[p] \to 0,$$

which by Lemma 1.2.4 (and the natural isomorphisms shown in its proof) is identified with the exact sequence in the statement. □

1.3. **Local cohomology groups of E.** Now we let $E/\mathbb{Q}$ be an elliptic curve of conductor N with good reduction at p and admitting a rational p-isogeny. The $G_\mathbb{Q}$-module $E[p]$ is therefore reducible, fitting into an exact sequence

$$0 \to \mathbb{F}_p(\phi) \to E[p] \to \mathbb{F}_p(\psi) \to 0, \tag{1.9}$$

where $\phi, \psi : G_\mathbb{Q} \to \mathbb{F}_p^\times$ are characters such that $\phi\psi = \omega$ by the Weil pairing. We assume that every prime $\ell | N$ splits in K and continue to assume that $p = v\bar{v}$ splits in K, so the results of the preceding sections can be applied to the restrictions of ϕ and ψ to G_K.

Let $T = T_pE$ be the p-adic Tate module of E, and denote by M_E the G_K-module

$$M_E := T \otimes_{\mathbb{Z}_p} \Lambda^\vee,$$

where the tensor product is endowed with the diagonal G_K-action (and the action on $\Lambda^\vee$ is via Ψ^{-1}, as before).

Lemma 1.3.1. *Let w be a prime of K above p, and assume that $E(K_w)[p] = 0$. Then $\mathrm{H}^1(K_w, M_E)$ is Λ-cofree of rank 2.*

Proof. The proof is virtually the same as the proof of Proposition 1.1.3(ii). Letting $X := \mathrm{H}^1(K_w, M_E)^\vee$, by Lemma 1.1.2 it suffices to show that $X[T] = 0$ and X/TX is $\mathbb{Z}_p$-free of rank 2. The hypotheses imply that $E(K_w)[p^\infty] = 0$, and so $\mathrm{H}^2(K_w, E[p^\infty]) = 0$ by local duality. Taking cohomology for the exact sequence

$$0 \to E[p^\infty] \to M_E \xrightarrow{\times T} M_E \to 0$$

it follows that

$$\frac{\mathrm{H}^1(K_w, M_E)}{T\mathrm{H}^1(K_w, M_E)} \simeq \mathrm{H}^2(K_w, E[p^\infty]) = 0, \qquad \mathrm{H}^1(K_w, E[p^\infty]) \simeq \mathrm{H}^1(K_w, M_E)[T]. \tag{1.10}$$

The first isomorphism shows that $X[T] = 0$. On the other hand, taking cohomology for the exact sequence $0 \to E[p] \to E[p^\infty] \xrightarrow{p} E[p^\infty] \to 0$ we obtain

$$\frac{\mathrm{H}^1(K_w, E[p^\infty])}{p\mathrm{H}^1(K_w, E[p^\infty])} \simeq \mathrm{H}^2(K_w, E[p]) = 0,$$

which together with the second isomorphism in (1.10) shows that $X/TX \simeq \mathrm{H}^1(K_w, E[p^\infty])^\vee$ is $\mathbb{Z}_p$-free. That its rank is 2 follows from the local Euler characteristic formula. □

1.4. **Selmer groups of E.** Fix a finite set Σ of places of K containing ∞ and the primes above Np, and such that the finite places in Σ are all split in K.

Similarly as in §1.2, we define a Selmer group for E by

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_E) := \ker\Biggl\{\mathrm{H}^1(K^\Sigma/K, M_E) \to \prod_{w \in \Sigma, w \nmid p} \mathrm{H}^1(K_w, M_E) \times \mathrm{H}^1(K_{\bar{v}}, M_E)\Biggr\},$$

and an S-imprimitive Selmer group, where $S = \Sigma \setminus \{v, \bar{v}, \infty\}$, by

$$\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E) := \ker\Biggl\{\mathrm{H}^1(K^\Sigma/K, M_E) \to \mathrm{H}^1(K_{\bar{v}}, M_E)\Biggr\}.$$

The residual Selmer groups $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_E[p])$ and $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E[p])$ are defined in the same manner.

Viewing the characters ϕ and ψ appearing in the exact sequence (1.9) as taking values in $\mathbb{Z}_p^\times$ via the Teichmüller lift, we obtain an exact sequence

$$0 \to M_\phi[p] \to M_E[p] \to M_\psi[p] \to 0 \tag{1.11}$$

of $\mathrm{Gal}(K^\Sigma/K)$-modules. Let $G_p \subset G_{\mathbb{Q}}$ be a decomposition group at p.

Proposition 1.4.1. *Assume that $\phi|_{G_p} \neq \mathbb{1}, \omega$. Then (1.11) induces a natural exact sequence*

$$0 \to \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\phi[p]) \to \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E[p]) \to \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_\psi[p]) \to 0.$$

In particular, $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E[p])$ is finite, and

$$\dim_{\mathbb{F}_p}\big(\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E[p])\big) = \lambda(\mathfrak{X}^S_\phi) + \lambda(\mathfrak{X}^S_\psi).$$

Proof. Taking cohomology for the exact sequence (1.11) we obtain the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(K^\Sigma/K, M_\phi[p]) \arrow[r] \arrow[d] & \mathrm{H}^1(K^\Sigma/K, M_E[p]) \arrow[r] \arrow[d] & \mathrm{H}^1(K^\Sigma/K, M_\psi[p]) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{H}^1(K_{\bar v}, M_\phi[p]) \arrow[r] & \mathrm{H}^1(K_{\bar v}, M_E[p]) \arrow[r] & \mathrm{H}^1(K_{\bar v}, M_\psi[p]) \arrow[r] & 0,
\end{tikzcd}$$

where the exactness of the rows follows immediately from Corollary 1.2.6 and the hypothesis on ϕ (which implies that $\psi|_{G_p} \neq \mathbb{1}, \omega$ as well), and the vertical maps are given by restriction. Since the left vertical arrow is surjective by Corollary 1.2.6, the snake lemma applied to this diagram yields the exact sequence in the statement. The last claim now follows from the last claim of Proposition 1.2.5. □

Now we can relate the imprimitive residual and p^∞-Selmer groups. Set

$$\mathfrak{X}^S_E := \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E)^\vee, \quad \mathfrak{X}_E := \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_E)^\vee.$$

Proposition 1.4.2. *Assume that $\phi|_{G_p} \neq \mathbb{1}, \omega$. Then*

$$\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E[p]) \simeq \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E)[p].$$

Moreover, the modules $\mathfrak{X}^S_E$ and $\mathfrak{X}_E$ are both Λ-torsion with $\mu = 0$.

Proof. Since $\psi = \omega\phi^{-1}$, our assumption on ϕ implies that $E(K_{\bar v})[p] = 0$, and therefore $\mathrm{H}^0(K_{\bar v}, M_E) = 0$. Thus the same argument as in the proof of Lemma 1.2.4 yields the isomorphism in the statement. It follows from Proposition 1.4.1 that $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E)[p]$ is finite, and so $\mathfrak{X}^S_E$ is Λ-cotorsion with $\mu = 0$. Since $\mathfrak{X}_E$ is a quotient of $\mathfrak{X}^S_E$, this completes the proof. □

Now we can deduce the following analogue of Proposition 1.2.5 for M_E.

Corollary 1.4.3. *Assume that $\phi|_{G_p} \neq \mathbb{1}, \omega$. Then $\mathfrak{X}^S_E$ has no non-trivial finite Λ-submodules, and*

$$\lambda(\mathfrak{X}^S_E) = \dim_{\mathbb{F}_p}\big(\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E[p])\big).$$

Proof. Since $M_E^* = \mathrm{Hom}(M_E, \mu_{p^\infty})$ has no non-trivial G_K-invariants and $\mathfrak{X}^S_E$ is Λ-torsion by Proposition 1.4.2, from [PW11, Prop. A.2] we deduce that the sequence

$$0 \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_E) \to \mathrm{H}^1(K^\Sigma/K, M_E) \to \prod_{w\in\Sigma, w\nmid p} \mathrm{H}^1(K_w, M_E) \times \mathrm{H}^1(K_{\bar v}, M_E) \to 0 \tag{1.12}$$

is exact. Proceeding as in the proof of Proposition 1.2.5, we see that the Λ-torsionness of $\mathfrak{X}_E$ implies that $\mathrm{H}^2(K^\Sigma/K, M_E) = 0$ and that $\mathrm{H}^1(K^\Sigma/K, M_E)^\vee$ has no nonzero pseudo-null Λ-submodules. The exactness of (1.12) readily implies a Λ-module isomorphism

$$\mathfrak{X}^S_E \simeq \frac{\mathrm{H}^1(K^\Sigma/K, M_E)^\vee}{\mathrm{H}^1(K_{\bar v}, M_E)^\vee}.$$

Since $\mathrm{H}^1(K_{\bar v}, M_E)$ is Λ-cofree by Lemma 1.3.1, we thus conclude from [GV00, Lem. 2.6] that $\mathfrak{X}^S_E$ has no nonzero finite Λ-submodules. Together with the isomorphism $\mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E[p]) \simeq \mathrm{H}^1_{\mathcal{F}^S_{\mathrm{Gr}}}(K, M_E)[p]$ of Proposition 1.4.2, the last claim in the statement of the corollary follows from this. □

Finally, we note that as in Lemma 1.1.1, one can show that for primes $w \nmid p$ split in K, the module $\mathrm{H}^1(K_w, M_E)^\vee$ is Λ-torsion with characteristic ideal generated by the element

$$\mathcal{P}_w(E) = P_w(\ell^{-1}\gamma_w) \in \Lambda,$$

where $P_w = \det(1 - \mathrm{Frob}_w X | V_{I_w})$, for $V = T \otimes \mathbb{Q}_p$, is the Euler factor at w of the L-function of E.

1.5. **Comparison I: Algebraic Iwasawa invariants.** We now arrive at the main result of this section. Recall that every prime $w \in \Sigma \setminus \{\infty\}$ is split in K, and we set $S = \Sigma \setminus \{v, \bar{v}, \infty\}$.

Theorem 1.5.1. *Assume that $\phi|_{G_p} \neq \mathbb{1}, \omega$. Then the module $\mathfrak{X}_E$ is Λ-torsion with $\mu(\mathfrak{X}_E) = 0$ and*

$$\lambda(\mathfrak{X}_E) = \lambda(\mathfrak{X}_\phi) + \lambda(\mathfrak{X}_\psi) + \sum_{w \in S} \{\lambda(\mathcal{P}_w(\phi)) + \lambda(\mathcal{P}_w(\psi)) - \lambda(\mathcal{P}_w(E))\}.$$

Proof. That $\mathfrak{X}_E$ is Λ-torsion with μ-invariant zero is part of Proposition 1.4.2. For the λ-invariant, combining Corollary 1.4.3 and the last claim of Proposition 1.4.1 we obtain

$$\lambda(\mathfrak{X}_E^S) = \lambda(\mathfrak{X}_\phi^S) + \lambda(\mathfrak{X}_\psi^S). \tag{1.13}$$

On the other hand, from (1.12) we deduce the exact sequence

$$0 \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K, M_E) \to \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}^S}(K, M_E) \to \prod_{w \in S} \mathrm{H}^1(K_w, M_E) \to 0,$$

and therefore the relation $\lambda(\mathfrak{X}_E^S) = \lambda(\mathfrak{X}_E) + \sum_{w \in S} \lambda(\mathcal{P}_w(E))$. This, combined with the second part of Proposition 1.2.5 shows that (1.13) reduces to the equality of λ-invariants in the statement of the theorem. □

2. Analytic side

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, $p \nmid 2N$ a prime of good reduction for E, and K an imaginary quadratic field satisfying hypotheses (Heeg), (spl), and (disc) from the introduction; in particular, $p = v\bar{v}$ splits in K.

In this section, assuming $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ as $G_{\mathbb{Q}}$-modules, we prove an analogue of Theorem 1.5.1 on the analytic side, relating the Iwasawa invariants of an anticyclotomic p-adic L-function of E to the Iwasawa invariants of anticyclotomic Katz p-adic L-functions attached to ϕ and ψ.

2.1. ***p*-adic *L*-functions.** Recall that $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$ denotes the anticyclotomic Iwasawa algebra, and set $\Lambda^{\mathrm{ur}} = \Lambda \hat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p^{\mathrm{ur}}$, for $\mathbb{Z}_p^{\mathrm{ur}}$ the completion of the ring of integers of the maximal unramified extension of $\mathbb{Q}_p$.

We shall say that an algebraic Hecke character $\psi : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{C}^\times$ has infinity type (m, n) if the component ψ_∞ of ψ at ∞ satisfies $\psi_\infty(z) = z^m \bar{z}^n$ for all $z \in (K \otimes \mathbb{R})^\times \simeq \mathbb{C}^\times$, where the last identification is made via $\imath_\infty$.

2.1.1. *The Bertolini–Darmon–Prasanna p-adic L-functions.* Fix an integral ideal $\mathfrak{N} \subset \mathcal{O}_K$ with

$$\mathcal{O}_K/\mathfrak{N} \simeq \mathbb{Z}/N\mathbb{Z}. \tag{2.1}$$

Let $f \in S_2(\Gamma_0(N))$ be the newform associated with E. Following [BDP13], one has the following result.

Theorem 2.1.1. *There exists an element $\mathcal{L}_E \in \Lambda^{\mathrm{ur}}$ characterized by the following interpolation property: For every character ξ of Γ crystalline at both v and $\bar{v}$ and corresponding to a Hecke character of K of infinity type $(n, -n)$ with $n \in \mathbb{Z}_{>0}$ and $n \equiv 0 \pmod{p-1}$, we have*

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

where Ω_p and Ω_∞ are CM periods attached to K as in [CH18, §2.5].

Proof. This was originally constructed in [BDP13] as a continuous function of ξ, and later explicitly constructed as a measure in [CH18] (following the approach in [Bra11]). Since this refined construction will be important for our purposes in this section, we recall some of the details.

Let $\mathrm{Ig}(N)$ be the Igusa scheme over $\mathbb{Z}_{(p)}$ parametrizing elliptic curves with $\Gamma_1(Np^\infty)$-level structure as in [CH18, §2.1]; its complex points admit a uniformization

$$[\ ,\ ] : \mathfrak{H} \times \mathrm{GL}_2(\hat{\mathbb{Q}}) \to \mathrm{Ig}(N)(\mathbb{C}). \tag{2.2}$$

Let c be a positive integer prime to Np. Then $\vartheta := (D_K + \sqrt{-D_K})/2$ and the element $\xi_c := \varsigma^{(\infty)}\gamma_c \in \mathrm{GL}_2(\hat{\mathbb{Q}})$ constructed in [CH18, p. 577] define a point

$$x_c := [(\vartheta, \xi_c)] \in \mathrm{Ig}(N)(\mathbb{C})$$

rational over $K[c](v^\infty)$, the compositum of the ring class field K of conductor c and the ray class field of K of conductor v^∞. For every $\mathcal{O}_c$-ideal $\mathfrak{a}$ prime to $\mathfrak{N}v$, let $a \in \hat{K}^{(cp),\times}$ be such that $\mathfrak{a} = a\hat{\mathcal{O}}_c \cap K$ and set

$$\sigma_{\mathfrak{a}} := \mathrm{rec}_K(a^{-1})|_{K[c](v^\infty)} \in \mathrm{Gal}(K[c](v^\infty)/K),$$

where $\mathrm{rec}_K : K^\times \backslash \hat{K}^\times \to G_K^{\mathrm{ab}}$ is the reciprocity map (geometrically normalized). Then by Shimura's reciprocity law, the point $x_{\mathfrak{a}} := x_c^{\sigma_{\mathfrak{a}}}$ is defined by the pair $(\vartheta, \overline{a}^{-1}\xi_c)$ under (2.2).

Let $V_p(N;R)$ be the space of p-adic modular forms of tame level N defined over a p-adic ring R (as recalled in [CH18, §2.2]), and let $S_{\mathfrak{a}} \hookrightarrow \mathrm{Ig}(N)_{/\mathbb{Z}_p^{\mathrm{ur}}}$ be the local deformation space of $x_{\mathfrak{a}} \otimes \overline{\mathbb{F}}_p \in \mathrm{Ig}(N)(\overline{\mathbb{F}}_p)$, so we have $\mathcal{O}_{S_{\mathfrak{a}}} \simeq \mathbb{Z}_p^{\mathrm{ur}}[\![t_{\mathfrak{a}} - 1]\!]$ by Serre–Tate theory. Viewing f as a p-adic modular form, the Serre–Tate expansion

$$f(t_{\mathfrak{a}}) := f|_{S_{\mathfrak{a}}} \in \mathbb{Z}_p^{\mathrm{ur}}[\![t_{\mathfrak{a}} - 1]\!]$$

defines a $\mathbb{Z}_p^{\mathrm{ur}}$-valued measure $\mathrm{d}\mu_{f,\mathfrak{a}}$ on $\mathbb{Z}_p$ characterized (by Mahler's theorem, see e.g. [Hid93, §3.3, Thm. 1]) by

$$\int_{\mathbb{Z}_p} \binom{x}{m} \mathrm{d}\mu_{f,\mathfrak{a}} = \binom{\theta}{m} f(x_{\mathfrak{a}}) \tag{2.3}$$

for all $m \geqslant 0$, where $\theta : V_p(N;\mathbb{Z}_p) \to V_p(N;\mathbb{Z}_p)$ is the Atkin–Serre operator, acting as qd/dq on q-expansions. Similarly, the p-depletion

$$f^\flat = \sum_{p\nmid n} a_n q^n$$

defines a $\mathbb{Z}_p^{\mathrm{ur}}$-valued measure $\mathrm{d}\mu_{f^\flat,\mathfrak{a}}$ on $\mathbb{Z}_p$ (supported on $\mathbb{Z}_p^\times$) with p-adic Mellin transform $f^\flat(t_{\mathfrak{a}})$, and we let $\mathrm{d}\mu_{f^\flat_{\mathfrak{a}}}$ be the measure on $\mathbb{Z}_p^\times$ corresponding to $f(t_{\mathfrak{a}}^{\mathrm{N}(\mathfrak{a})^{-1}\sqrt{-D_K}^{-1}})$ (see [CH18, Prop. 3.3]).

Letting η be an auxiliary anticyclotomic Hecke character of K of infinity type $(1,-1)$ and conductor c, define $\mathscr{L}_{v,\eta} \in \Lambda^{\mathrm{ur}}$ by

$$\mathscr{L}_{v,\eta}(\phi) = \sum_{[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_c)} \eta(\mathfrak{a})\mathbf{N}(\mathfrak{a})^{-1} \int_{\mathbb{Z}_p^\times} \eta_v(\phi|[\mathfrak{a}])\, \mathrm{d}\mu_{f^\flat_{\mathfrak{a}}} \tag{2.4}$$

where η_v denotes the v-component of η, and $\phi|[\mathfrak{a}] : \mathbb{Z}_p^\times \to \mathcal{O}_{\mathbb{C}_p}^\times$ is defined by $(\phi|[\mathfrak{a}])(x) = \phi(\mathrm{rec}_v(x)\sigma_{\mathfrak{a}}^{-1})$ for the local reciprocity map $\mathrm{rec}_v : K_v^\times \to G_K^{\mathrm{ab}} \twoheadrightarrow \Gamma$. Then by [CH18, Prop. 3.8] the element $\mathcal{L}_E \in \Lambda^{\mathrm{ur}}$ defined by

$$\mathcal{L}_E(\xi) := \mathscr{L}_{v,\eta}(\eta^{-1}\xi)^2$$

has the stated interpolation property. □

2.1.2. *Katz p-adic L-functions.* Let $\theta : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ be a Dirichlet character of conductor C. As it will suffice for our purposes, we assume that $C|N$ (so $p \nmid C$), and let $\mathfrak{C}|\mathfrak{N}$ be such that $\mathcal{O}_K/\mathfrak{C} = \mathbb{Z}/C\mathbb{Z}$.

The next result follows from the work of Katz [Kat78], as extended by Hida–Tilouine [HT93].

Theorem 2.1.2. *There exists an element $\mathcal{L}_\theta \in \Lambda^{\mathrm{ur}}$ characterized by the following interpolation property: For every character ξ of Γ crystalline at both v and $\bar{v}$ and corresponding to a Hecke character of K of infinity type $(n,-n)$ with $n \in \mathbb{Z}_{>0}$ and $n \equiv 0 \pmod{p-1}$, we have*

$$\begin{aligned}\mathcal{L}_\theta(\xi) = \frac{\Omega_p^{2n}}{\Omega_\infty^{2n}} \cdot 4\Gamma(n+1) \cdot \frac{(2\pi i)^{n-1}}{\sqrt{D_K}^{n-1}} \cdot \bigl(1 - \theta^{-1}(p)\xi^{-1}(v)\bigr) \cdot \bigl(1 - \theta(p)\xi(\bar{v})p^{-1}\bigr)\bigr) \\ \times \prod_{\ell|C}(1 - \theta(\ell)\xi(w)\ell^{-1}) \cdot L(\theta_K\xi\mathbf{N}_K, 0),\end{aligned}$$

where Ω_p and Ω_∞ are as in Theorem 2.1.1, and for each $\ell|C$ we take the prime $w|\ell$ with $w|\mathfrak{C}$.

Proof. The character θ (viewed as a character of K) defines a projection

$$\pi_\theta : \mathbb{Z}_p^{\mathrm{ur}}[\![\mathrm{Gal}(K(\mathfrak{C}p^\infty)/K)]\!] \to \Lambda^{\mathrm{ur}},$$

where $K(\mathfrak{C}p^\infty)$ is the ray class field of K of conductor $\mathfrak{C}p^\infty$ (this projection is just $g \mapsto \theta(g)[g]$ for $g \in \mathrm{Gal}(K(\mathfrak{C}p^\infty)/K$ and $[g]$ the image of g in Γ). The element $\mathcal{L}_\theta$ is then obtained by applying π_θ to the Katz p-adic L-function described in [Kri16, Thm. 27], setting $\chi^{-1} = \theta_K \xi \mathbf{N}_K$. □

2.2. **Comparison II: Analytic Iwasawa invariants.** The following theorem follows from the main result of [Kri16]. Following the notations in *op. cit*, we let N_0 be the square-full part of N (so the quotient N/N_0 is square-free), and fix an integral ideal $\mathfrak{N} \subset \mathcal{O}_K$ as in (2.1).

Let also $f = \sum_{n=1}^\infty a_n q^n \in S_2(\Gamma_0(N))$ be the newform associated with E, and denote by λ^ι the image of $\lambda \in \Lambda$ under the involution of Λ given by $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \Gamma$.

Theorem 2.2.1. *Assume that $E[p]^{ss} \simeq \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ as $G_\mathbb{Q}$-modules, with the characters ϕ, ψ labeled so that $p \nmid \mathrm{cond}(\phi)$, and suppose $\phi \neq \mathbb{1}$. Then there is a factorization $N/N_0 = N_+N_-$ with*

$$\begin{cases} a_\ell \equiv \phi(\ell) \pmod p & \text{if } \ell | N_+, \\ a_\ell \equiv \psi(\ell) \pmod p & \text{if } \ell | N_-, \\ a_\ell \equiv 0 \pmod p & \text{if } \ell | N_0, \end{cases}$$

such that the following congruence holds

$$\mathcal{L}_E \equiv (\mathcal{E}^\iota_{\phi,\psi})^2 \cdot (\mathcal{L}_\phi)^2 \pmod{p\Lambda^{\mathrm{ur}}},$$

where

$$\mathcal{E}_{\phi,\psi} = \prod_{\ell | N_0 N_-} \mathcal{P}_w(\phi) \cdot \prod_{\ell | N_0 N_+} \mathcal{P}_w(\psi),$$

and for each $\ell | N$ we take the prime $w | \ell$ with $w | \mathfrak{N}$.

Proof. By Theorem 34 and Remark 32 in [Kri16], our hypothesis on $E[p]$ implies that there is a congruence

$$f \equiv G \pmod p, \tag{2.5}$$

where G is a certain weight two Eisenstein series (denoted $E_2^{\phi,\phi^{-1},(N)}$ in *loc. cit.*). Viewed as a p-adic modular form, G defines $\mathbb{Z}_p^{\mathrm{ur}}$-valued measures $\mu_{G,\mathfrak{a}}$ on $\mathbb{Z}_p$ by the rule (2.3). With the notations introduced in the proof of Theorem 2.1.1, set

$$\mathscr{L}_{v,\eta}(G,\phi) = \sum_{[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_c)} \eta(\mathfrak{a}) \mathbf{N}(\mathfrak{a})^{-1} \int_{\mathbb{Z}_p^\times} \eta_v(\phi | [\mathfrak{a}]) \, \mathrm{d}\mu_{G^\flat,\mathfrak{a}} \tag{2.6}$$

where the cusp form f in (2.3) has been replaced by G, and let $\mathcal{L}_G \in \Lambda^{\mathrm{ur}}$ be the element defined by

$$\mathcal{L}_G(\xi) := \mathscr{L}_{v,\eta}(\eta^{-1}\xi).$$

Then for ξ an arbitrary character of Γ crystalline at both v and $\bar{v}$ and corresponding to a Hecke character of K of infinity type $(n, -n)$ for some $n \in \mathbb{Z}_{>0}$ with $n \equiv 0 \pmod{p-1}$, the calculation in [Kri16, Prop. 37] (taking $\chi^{-1} = \xi \mathbf{N}_K$, $\psi_1 = \phi$, and $\psi_2 = \phi^{-1} = \psi\omega^{-1}$ in the notations of *loc.cit.*, so in particular $j = n - 1$) shows that

$$\mathcal{L}_G(\xi) = \frac{\Omega_p^{2n}}{\Omega_\infty^{2n}} \cdot \frac{\Gamma(n+1)\phi^{-1}(-\sqrt{D_K})\xi(\mathfrak{t})t}{\mathfrak{g}(\phi)} \cdot \frac{(2\pi i)^{n-1}}{\sqrt{D_K}^{n-1}} \cdot \Xi_{\xi^{-1}\mathbf{N}_K^{-1}}(\phi, \psi\omega^{-1}, N_+, N_-, N_0) \cdot L(\phi_K \xi \mathbf{N}_K, 0), \tag{2.7}$$

where ϕ_K denotes the base change of ϕ to K, and

$$\begin{aligned} \Xi_{\xi^{-1}\mathbf{N}_K^{-1}}(\phi, \psi\omega^{-1}, N_+, N_-, N_0) = \prod_{\ell | N_+} (1 - \phi^{-1}\xi(\bar{w})) \cdot \prod_{\ell | N_-} (1 - \phi\xi(\bar{w})\ell^{-1}) \\ \times \prod_{\ell | N_0} (1 - \phi^{-1}\xi(\bar{w}))(1 - \phi\xi(\bar{w})\ell^{-1}). \end{aligned}$$

Comparing with the interpolation property of $\mathcal{L}_\phi$ in Theorem 2.2.1, and noting that

$$\mathcal{E}_{\phi,\psi}(\xi^{-1}) = \Xi_{\xi^{-1}\mathbf{N}_K^{-1}}(\phi, \psi\omega^{-1}, N_+, N_-, N_0)$$

for all ξ as above, the equality (2.7) implies that

$$\mathcal{L}_G = \mathcal{E}^\iota_{\phi,\psi} \cdot \mathcal{L}_\phi. \tag{2.8}$$

On the other hand, the congruence (2.5) implies the congruences

$$\binom{\theta}{m} f(x_{\mathfrak{a}}) \equiv \binom{\theta}{m} G(x_{\mathfrak{a}}) \pmod{p\mathbb{Z}_p^{\mathrm{ur}}}$$

for all $m \geqslant 0$, which in turn yield the congruence

$$\mathcal{L}_E \equiv (\mathcal{L}_G)^2 \pmod{p\Lambda^{\mathrm{ur}}}. \tag{2.9}$$

The combination of (2.8) and (2.9) now yields the theorem. □

Theorem 2.2.2. *Assume that $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ as $G_{\mathbb{Q}}$-modules, with the characters ϕ, ψ labeled so that $p \nmid \mathrm{cond}(\phi)$, and suppose $\phi \neq \mathbb{1}$. Then $\mu(\mathcal{L}_E) = 0$ and*

$$\lambda(\mathcal{L}_E) = \lambda(\mathcal{L}_\phi) + \lambda(\mathcal{L}_\psi) + \sum_{w \in S} \bigl\{ \lambda(\mathcal{P}_w(\phi)) + \lambda(\mathcal{P}_w(\psi)) - \lambda(\mathcal{P}_w(E)) \bigr\}.$$

Proof. Since K satisfies (Heeg) and (spl), the conductors of both ϕ and ψ are only divisible by primes split in K, and hence the vanishing of $\mu(\mathcal{L}_E)$ follows immediately from the congruence of Theorem 2.2.1 and Hida's result [Hid10] (note that the factors $\mathcal{P}_w(\phi)$ and $\mathcal{P}_w(\psi)$ also have vanishing μ-invariant, since again the primes w are split in K).

As for the equality between λ-invariants, note that the involution of Λ given by $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \Gamma$ preserves λ-invariants, and so

$$\lambda(\mathcal{P}_w(\theta)^2) = \lambda(\mathcal{P}_w(\theta)) + \lambda(\mathcal{P}_{\bar{w}}(\theta)),$$

using that complex conjugation acts as inversion on Γ. For the term $\mathcal{E}_{\phi,\psi}$ in Theorem 2.2.1 we thus have

$$\lambda((\mathcal{E}_{\phi,\psi}^{\iota})^2) = \lambda((\mathcal{E}_{\phi,\psi})^2) = \sum_{w | N_0 N_-} \lambda(\mathcal{P}_w(\phi)) + \sum_{w | N_0 N_+} \lambda(\mathcal{P}_w(\psi)),$$

where w runs over all divisors, not just the ones dividing $\mathfrak{N}$. Using the congruence relations in Theorem 2.2.1 (in particular, that $a_\ell \equiv 0 \pmod{p}$ for $\ell | N_0$) this can be rewritten as

$$\lambda((\mathcal{E}_{\phi,\psi}^{\iota})^2) = \sum_{w \in S} \bigl\{ \lambda(\mathcal{P}_w(\phi)) + \lambda(\mathcal{P}_w(\psi)) - \lambda(\mathcal{P}_w(E)) \bigr\}. \tag{2.10}$$

On the other hand, since $\psi = \phi^{-1}\omega$, the functional equation for the Katz p-adic L-function (see e.g. [Kri16, Thm. 27]) yields

$$\lambda(\mathcal{L}_\psi) = \lambda(\mathcal{L}_\phi). \tag{2.11}$$

The result now follows from Theorem 2.2.1 combined with (2.10) and (2.11). □

Together with the main result of §1, we arrive at the following.

Theorem 2.2.3. *Assume that $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ with $\phi|_{G_p} \neq \mathbb{1}, \omega$. Then $\mu(\mathcal{L}_E) = \mu(\mathfrak{X}_E) = 0$ and*

$$\lambda(\mathcal{L}_E) = \lambda(\mathfrak{X}_E).$$

Proof. The vanishing of $\mu(\mathfrak{X}_E)$ (resp. $\mu(\mathcal{L}_E)$) has been shown in Proposition 1.4.2 (resp. Theorem 2.2.2). On the other hand, Iwasawa's main conjecture for K (a theorem of Rubin [Rub91]) yields in particular the equalities $\lambda(\mathcal{L}_\phi) = \lambda(\mathfrak{X}_\phi)$ and $\lambda(\mathcal{L}_\psi) = \lambda(\mathfrak{X}_\psi)$. The combination of Theorem 1.5.1 and Theorem 2.2.2 therefore yields the result. □

3. A Kolyvagin system argument

The goal of this section is to prove Theorem 3.4.1 below, extending [How04a, Thm. 2.2.10] to the residually reducible setting. This result, which assumes the existence of a non-trivial Kolyvagin system, will be applied in §4 to a Kolyvagin system derived from Heegner points to prove one of the divisibilities towards Conjecture B.

3.1. **Selmer structures and Kolyvagin systems.** Let K be an imaginary quadratic field, let $(R,\mathfrak{m})$ be a complete Noetherian local ring with finite residue field of characteristic p, and let M be a topological $R[G_K]$-module such that the G_K-action is unramified outside a finite set of primes. We define a *Selmer structure* $\mathcal{F}$ on M to be a finite set $\Sigma=\Sigma(\mathcal{F})$ of places of K containing ∞, the primes above p, and the primes where M is ramified, together with a choice of R-submodules (called local conditions) $\mathrm{H}^1_{\mathcal{F}}(K_w,M)\subset\mathrm{H}^1(K_w,M)$ for every $w\in\Sigma$. The associated *Selmer group* is then defined by

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

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

Below we shall use the following local conditions. First, the *unramified* local condition is

$$\mathrm{H}^1_{\mathrm{ur}}(K_w,M):=\ker\bigl\{\mathrm{H}^1(K_w,M)\to\mathrm{H}^1(K_w^{\mathrm{ur}},M)\bigr\}.$$

If $w\mid p$ is a finite prime where M is unramified, we set $\mathrm{H}^1_{\mathrm{f}}(K_w,M):=\mathrm{H}^1_{\mathrm{ur}}(K_w,M)$, which is sometimes called the *finite* local condition. The *singular quotient* $\mathrm{H}^1_{\mathrm{s}}(K,M)$ is defined by the exactness of the sequence

$$0\to\mathrm{H}^1_{\mathrm{f}}(K_w,M)\to\mathrm{H}^1(K_w,M)\to\mathrm{H}^1_{\mathrm{s}}(K_w,M)\to 0.$$

Denote by $\mathscr{L}_0=\mathscr{L}_0(M)$ the set of rational primes $\ell\neq p$ such that

- ℓ is inert in K,
- M is unramified at ℓ.

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

$$\mathrm{H}^1_{\mathrm{tr}}(K_\lambda,T):=\ker\bigl\{\mathrm{H}^1(K_\lambda,T)\to\mathrm{H}^1(K[\ell]_{\lambda'},T)\bigr\},$$

where $K[\ell]_{\lambda'}$ is the completion of $K[\ell]$ at any prime λ' above λ.

As in [How04a], we call a *Selmer triple* $(M,\mathcal{F},\mathscr{L})$ the data of a Selmer structure $\mathcal{F}$ on M and a subset $\mathscr{L}\subset\mathscr{L}_0$ with $\mathscr{L}\cap\Sigma(\mathcal{F})=\emptyset$. Given a Selmer triple $(M,\mathcal{F},\mathscr{L})$ and pairwise coprime integers a,b,c divisible only by primes in $\mathscr{L}_0$, the modified Selmer group $\mathrm{H}^1_{\mathcal{F}_b^a(c)}(K,M)$ is the one defined by $\Sigma(\mathcal{F}_b^a(c))=\Sigma(\mathcal{F})\cup\{w|abc\}$ and the local conditions

$$\mathrm{H}^1_{\mathcal{F}_b^a(c)}(K_\lambda,T)=\begin{cases}\mathrm{H}^1(K_\lambda,T) & \text{if } \lambda|a,\\ 0 & \text{if } \lambda|b,\\ \mathrm{H}^1_{\mathrm{tr}}(K_\lambda,T) & \text{if } \lambda|c,\\ \mathrm{H}^1_{\mathcal{F}}(K_w,T) & \text{if } \lambda\nmid abc.\end{cases}$$

Let T be a compact R-module equipped with a continuous linear G_K-action that is unramified outside a finitely set of primes. For each $\lambda|\ell\in\mathscr{L}_0=\mathscr{L}_0(T)$, let I_ℓ be the smallest ideal containing $\ell+1$ for which the Frobenius element $\mathrm{Frob}_\lambda\in G_{K_\lambda}$ acts trivially on $T/I_\ell T$. By class field theory, the prime λ splits completely in the Hilbert class field of K, and the p-Sylow subgroups of $G_\ell:=\mathrm{Gal}(K[\ell]/K[1])$ and $k_\lambda^\times/\mathbb{F}_\ell^\times$ are identified via the Artin symbol, where k_λ is the residue field of λ. Hence by [MR04, Lem. 1.2.1] there is a *finite-singular comparison isomorphism*

$$\phi_\lambda^{\mathrm{fs}}:\mathrm{H}^1_{\mathrm{f}}(K_\lambda,T/I_\ell T)\simeq T/I_\ell T\simeq\mathrm{H}^1_{\mathrm{s}}(K_\lambda,T/I_\ell T)\otimes G_\ell. \tag{3.1}$$

Given a subset $\mathscr{L}\subset\mathscr{L}_0$, we let $\mathscr{N}=\mathscr{N}(\mathscr{L})$ be the set of square-free products of primes $\ell\in\mathscr{L}$, and for each $n\in\mathscr{N}$ define

$$I_n=\sum_{\ell|n}I_n\subset R,\quad G_n=\bigotimes_{\ell|n}G_\ell,$$

with the convention that $1\in\mathscr{N}$, $I_1=0$, and $G_1=\mathbb{Z}$.

Definition 3.1.1. A *Kolyvagin system* for a Selmer triple $(T,\mathcal{F},\mathscr{L})$ is a collection of classes

$$\kappa=\{\kappa_n\in\mathrm{H}^1_{\mathcal{F}(n)}(K,T/I_nT)\otimes G_n\}_{n\in\mathscr{N}}$$

such that $(\phi_\lambda^{\mathrm{fs}}\otimes 1)(\mathrm{loc}_\lambda(\kappa_n))=\mathrm{loc}_\lambda(\kappa_{n\ell})$ for all $n\ell\in\mathscr{N}$.

We denote by $\mathbf{KS}(T,\mathcal{F},\mathscr{L})$ the R-module of Kolyvagin systems for $(T,\mathcal{F},\mathscr{L})$.

3.2. **Bounding Selmer groups.** Here we state our main result on bounding Selmer groups of anticyclotomic twists of Tate modules of elliptic curves, whose proof is given in the next section. The reader mostly interested in the Iwasawa-theoretic consequences of this result might wish to proceed to §3.4 after reading the statement of Theorem 3.2.1.

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

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

As before, let $\Gamma=\mathrm{Gal}(K_\infty/K)$ be the Galois group of the anticyclotomic $\mathbb{Z}_p$-extension of K. Let $\alpha:\Gamma\to R^\times$ be a character with values in the ring of integers R of a finite extension $\Phi/\mathbb{Q}_p$. Let

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

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

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

where $R(\alpha)$ is the free R-module of rank one on which G_K acts the projection $G_K\twoheadrightarrow\Gamma$ composed with α, and the G_K-action on T_α is via $\rho_\alpha=\rho_E\otimes\alpha$.

Let $\mathfrak{m}\subset R$ be the maximal ideal, with uniformizer $\pi\in\mathfrak{m}$, and let $\bar{T}:=T_\alpha\otimes R/\mathfrak{m}$ be the residual representation associated to T_α. Note that

$$\bar{T}\simeq E[p]\otimes R/\mathfrak{m} \tag{3.2}$$

as G_K-modules, since $\alpha\equiv 1\pmod{\mathfrak{m}}$. In particular, (h1) implies that $\bar{T}^{G_K}=0$.

For $w|p$ a prime of K above p, set

$$\mathrm{Fil}_w^+(T_pE):=\ker\{T_pE\to T_p\tilde{E}\},$$

where $\tilde{E}$ is the reduction of E at w, and put

$$\mathrm{Fil}_w^+(T_\alpha):=\mathrm{Fil}_w^+(T_pE)\otimes_{\mathbb{Z}_p}R(\alpha),\quad \mathrm{Fil}_w^+(V_\alpha):=\mathrm{Fil}_w^+(T_\alpha)\otimes_R\Phi.$$

Following [CG96], define the *ordinary* Selmer structure $\mathcal{F}_{\rm ord}$ on V_α by taking $\Sigma(\mathcal{F}_{\rm ord})=\{w\mid pN\}$ and

$$\mathrm{H}^1_{\mathcal{F}_{\rm ord}}(K_w,V_\alpha):=\begin{cases}\mathrm{im}\big\{\mathrm{H}^1(K_w,\mathrm{Fil}_w^+(V_\alpha))\to\mathrm{H}^1(K_w,V_\alpha)\big\} & \text{if } w|p,\\ \mathrm{H}^1_{\rm ur}(K_w,V_\alpha) & \text{else.}\end{cases}$$

Let $\mathcal{F}_{\rm ord}$ also denote the Selmer structure on T_α and A_α obtained by propagating $\mathrm{H}^1_{\mathcal{F}_{\rm ord}}(K_w,V_\alpha)$ under the maps induced by the exact sequence $0\to T_\alpha\to V_\alpha\to A_\alpha\to 0$.

Let $\gamma\in\Gamma$ be a topological generator, and let

$$C_\alpha:=\begin{cases}v_p(\alpha(\gamma)-\alpha^{-1}(\gamma)) & \alpha\neq\alpha^{-1},\\ 0 & \alpha=\alpha^{-1},\end{cases} \tag{3.3}$$

where v_p is the p-adic valuation normalized so that $v_p(p)=1$. Finally, let

$$\mathscr{L}_E:=\{\ell\in\mathscr{L}_0(T_pE)\ :\ a_\ell\equiv\ell+1\equiv 0\ (\mathrm{mod}\ p)\},$$

where $a_\ell=\ell+1-|\tilde{E}(\mathbb{F}_\ell)|$, and $\mathscr{N}=\mathscr{N}(\mathscr{L}_E)$.

Theorem 3.2.1. *Suppose $\alpha\neq 1$ and there is a Kolyvagin system $\kappa_\alpha=\{\kappa_{\alpha,n}\}_{n\in\mathscr{N}}\in\mathbf{KS}(T_\alpha,\mathcal{F}_{\rm ord},\mathscr{L}_E)$ with $\kappa_{\alpha,1}\neq 0$. Then $\mathrm{H}^1_{\mathcal{F}_{\rm ord}}(K,T_\alpha)$ has rank one, and there is a finite R-module M_α such that*

$$\mathrm{H}^1_{\mathcal{F}_{\rm ord}}(K,A_\alpha)\simeq(\Phi/R)\oplus M_\alpha\oplus M_\alpha$$

with

$$\mathrm{length}_R(M_\alpha)\leqslant\mathrm{length}_R\big(\mathrm{H}^1_{\mathcal{F}_{\rm ord}}(K,T_\alpha)/R\cdot\kappa_{\alpha,1}\big)+E_\alpha$$

for some constant $E_\alpha\in\mathbb{Z}_{\geqslant 0}$ depending only on C_α, T_pE, and $\mathrm{rank}_{\mathbb{Z}_p}(R)$.

When $\rho_E|_{G_K}:G_K\to\mathrm{End}_{\mathbb{Z}_p}(T_pE)$ is surjective, Theorem 3.2.1 (with $E_\alpha=0$) can be deduced from [How04a, Thm. 1.6.1], but the proof of Theorem 3.2.1 assuming only (h1) requires new ideas, some of which were inspired by Nekovář's work [Nek07].

3.3. **Proof of Theorem 3.2.1.** To ease notation, let $(T,\mathcal{F},\mathscr{L})$ denote the Selmer triple $(T_\alpha,\mathcal{F}_{\mathrm{ord}},\mathscr{L}_E)$, and let $\rho=\rho_\alpha$. For any $k\geqslant 0$, let

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

and let $\mathscr{N}^{(k)}$ be the set of square-free products of primes $\ell\in\mathscr{L}^{(k)}$.

We begin by recalling two preliminary results from [MR04] and [How04a].

Lemma 3.3.1. *For every $n\in\mathscr{N}^{(k)}$ and $0\leqslant i\leqslant k$ there are natural isomorphisms*

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

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

Proof. The proof of [MR04, Lem. 3.5.4] carries over, since it only requires the vanishing of $\bar{T}^{G_K}$. □

Proposition 3.3.2. *For every $n\in\mathscr{N}^{(k)}$ there is an $R^{(k)}$-module $M^{(k)}(n)$ and an integer ϵ such that*

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

Moreover, ϵ can be taken to be $\epsilon\in\{0,1\}$ and is independent of k and n.

Proof. This is shown in [How04a, Prop. 1.5.5], whose proof makes use of hypothesis (h1) and hypotheses (H.3) and (H.4) in *op. cit.*, the latter two being satisfied in our setting by [MR04, Lem. 3.7.1] and [MR04, Lem. 2.2.1], respectively. We note that the independence of ϵ follows from the fact that, by Lemma 3.3.1, we have

$$\epsilon\equiv\dim_{R/\mathfrak{m}}\mathrm{H}^1_{\mathcal{F}(n)}(K,\bar{T})\pmod 2,$$

and the right dimension is independent of k and n by the "parity lemma" of [How04a, Lem. 1.5.3], whose proof is also given under just the aforementioned hypotheses. □

3.3.1. *The Čebotarev argument.* For any finitely-generated torsion R-module M and $x\in M$, write

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

When ρ_E has large image, a standard application of the Čebotarev density theorem can be used to show that, given R-linearly independent classes $c_1,\dots,c_s\in\mathrm{H}^1(K,T^{(k)})$, there exist infinitely many primes $\ell\in\mathscr{L}$ such that $\mathrm{ord}(\mathrm{loc}_\ell(c_i))=\mathrm{ord}(c_i)$, $i=1,\dots,s$ (see [McC91, Cor. 3.2]). Assuming only hypothesis (h1), one can obtain a similar result with "error terms". Our version of this is Proposition 3.3.6 below, which provides the key technical input for our proof of Theorem 3.2.1. Before proving this proposition we define the error terms that appear in its statement.

For any field $F\subset\overline{\mathbb{Q}}$ let $F(E[p^\infty])$ be the fixed field of the kernel of $\rho_E|_{G_F}$. Since $(D_K,Np)=1$, and therefore E does not have CM by K, and p is odd by hypothesis, $\mathbb{Q}(E[p^\infty])\cap K_\infty=\mathbb{Q}$, as any subfield of K_∞ that is Galois over $\mathbb{Q}$ is either $\mathbb{Q}$ or contains K. Hence the natural projection $\mathrm{Gal}(K_\infty(E[p^\infty])/K_\infty)\to\mathrm{Gal}(\mathbb{Q}(E[p^\infty])/\mathbb{Q})$ is an isomorphism and so $\rho_E(G_{K_\infty})=\rho_E(G_\mathbb{Q})$.

The first error term comes from the following.

Lemma 3.3.3. *The intersection $U=\mathbb{Z}_p^\times\cap\mathrm{im}(\rho_E|_{G_{K_\infty}})$ is an open subgroup of $\mathbb{Z}_p^\times$ such that $U\subset\mathrm{Im}(\rho)\subset\mathrm{Aut}_R(T)$ for all characters α.*

Proof. By [Nek07, Prop. (6.1.1)(i)], $U=\mathbb{Z}_p^\times\cap\mathrm{im}(\rho_E)\subset\mathrm{Aut}_{\mathbb{Z}_p}(T_pE)\simeq\mathrm{GL}_2(\mathbb{Z}_p)$ is an open subgroup of $\mathbb{Z}_p^\times$. Since $\mathrm{im}(\rho_E|_{G_{K_\infty}})=\mathrm{im}(\rho_E)$, $U=\mathbb{Z}_p^\times\cap\mathrm{im}(\rho_E|_{G_{K_\infty}})$. As α is trivial on G_{K_∞} the claim for all characters α follows. □

For $U=\mathbb{Z}_p^\times\cap\mathrm{im}(\rho_E)$ as in Lemma 3.3.3, let

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

Since U is an open subgroup of $\mathbb{Z}_p^\times$, $0\leqslant C_1<\infty$.

To define the second error term, note that $\mathrm{End}_{\mathbb{Z}_p}(T_pE)/\rho_E(\mathbb{Z}_p[G_\mathbb{Q}])$ is a torsion $\mathbb{Z}_p$-module, as ρ_E is irreducible. Hence there exists $m\in\mathbb{Z}_{\geq 0}$ such that $p^m(\mathrm{End}_{\mathbb{Z}_p}(T_pE)/\rho_E(\mathbb{Z}_p[G_\mathbb{Q}]))=0$. Then

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

is such that $0\leqslant C_2<\infty$.

Lemma 3.3.4. *For any α, p^{C_2} annihilates $\mathrm{End}_R(T)/\rho(R[G_{K_\infty}])$.*

Proof. Since $\rho(G_{K_\infty}) = \rho_E(G_{K_\infty}) = \rho_E(G_{\mathbb{Q}})$ (using that E does not have CM by K), it follows that

$$\mathrm{End}_R(T)/\rho(R[G_{K_\infty}]) = \mathrm{End}_R(T)/\rho_E(R[G_{\mathbb{Q}}]) = (\mathrm{End}_{\mathbb{Z}_p}(T_pE)/\rho_E(\mathbb{Z}_p[G_{\mathbb{Q}}])) \otimes_{\mathbb{Z}_p} R$$

is annihilated by p^{C_2}. □

Remark 3.3.5. If ρ_E is surjective, then clearly $C_1 = 0$. Similarly, if $E[p]$ is irreducible, then $C_2 = 0$. In particular, if ρ_E is surjective, then $C_1 = 0 = C_2$.

The third error term is given by the quantity C_α defined before.

Proposition 3.3.6. *Suppose $\alpha \neq 1$. Let $c_1, c_2, c_3 \in \mathrm{H}^1(K, T^{(k)})$. Suppose $Rc_1 + Rc_2$ contains a submodule isomorphic to $\mathfrak{m}^{d_1}R^{(k)} \oplus \mathfrak{m}^{d_2}R^{(k)}$ for some $d_1, d_2 \geqslant 0$. Then there exist infinitely many primes $\ell \in \mathscr{L}^{(k)}$ such that*

$$\mathrm{ord}(\mathrm{loc}_\ell(c_3)) \geqslant \mathrm{ord}(c_3) - r(C_1 + C_2 + C_\alpha),$$

and $R\,\mathrm{loc}_\ell(c_1) + R\,\mathrm{loc}_\ell(c_2) \subset \mathrm{H}^1(K_\ell, T^{(k)})$ contains a submodule isomorphic to

$$\mathfrak{m}^{d_1+d_2+2r(C_1+C_2+C_\alpha)}(R^{(k)} \oplus R^{(k)}).$$

Proof. Let $m_i = \max\{0, \mathrm{ord}(c_i) - r(C_1+C_2+C_\alpha)\}$. Note that since $Rc_1 + Rc_2$ contains a submodule isomorphic to $\mathfrak{m}^{d_1}R^{(k)} \oplus \mathfrak{m}^{d_2}R^{(k)}$, it must be that $\max\{\mathrm{ord}(c_1), \mathrm{ord}(c_2)\} \geqslant k - d_1, k - d_2$ and hence if $m_1 = m_2 = m_3 = 0$, then the lemma is trivially true. So we suppose $\max\{m_1, m_2, m_3\} > 0$.

Let $K_\alpha \subset K_\infty$ be such that $\alpha|_{G_{K_\alpha}} \equiv 1 \mod \mathfrak{m}^k$. Let $L = K_\alpha(E[p^k])$ be the fixed field of the kernel of the action of G_{K_α} on $E[p^k]$ (so in particular, G_L acts trivially on $T^{(k)}$). Then ρ induces an injection

$$\rho : \mathrm{Gal}(L/K) \hookrightarrow \mathrm{Aut}(T^{(k)}).$$

Let $u \in \mathbb{Z}_p^\times \cap \mathrm{im}(\rho_E|_{G_{K_\infty}})$ such that $\mathrm{ord}_p(u-1) = C_1$. Then $u = \rho(g)$ for some $g \in \mathrm{Gal}(L/K)$. Let $T_E^{(k)} = T_pE \otimes_{\mathbb{Z}_p} R/\mathfrak{m}^k$. It follows from Sah's lemma that $g - 1$ annihilates $\mathrm{H}^1(\mathrm{Gal}(L/K), T^{(k)})$, and therefore the kernel of the restriction map

$$\mathrm{H}^1(K, T^{(k)}) \to \mathrm{H}^1(L, T^{(k)}) = \mathrm{H}^1(L, T_E^{(k)})^{(\alpha)} = \mathrm{Hom}(G_L, T_E^{(k)})^{(\alpha)}$$

is annihilated by p^{C_1} and hence by π^{rC_1} (cf. [Nek07, Prop. (6.1.2)]). Here and in the following we denote by $(-)^{(\alpha)}$ the submodule on which $\mathrm{Gal}(L/K)$ acts via the character α. The restriction of the c_i to G_L therefore yields homomorphisms $f_i \in \mathrm{Hom}(G_L, T_E^{(k)})^{(\alpha)}$ such that

$$\mathrm{ord}(f_i) \geqslant \mathrm{ord}(c_i) - rC_1, i = 1, 2, 3,$$

and $Rf_1 + Rf_2 \subset \mathrm{Hom}(G_L, T_E^{(k)})^{(\alpha)}$ contains a submodule isomorphic to $\mathfrak{m}^{d_1+rC_1}R^{(k)} \oplus \mathfrak{m}^{d_2+rC_1}R^{(k)}$.

Note that the complex conjugation τ acts naturally on $\mathrm{Hom}(G_L, T_E^{(k)})$, and that this action maps an element $f \in \mathrm{Hom}(G_L, T_E^{(k)})^{(\alpha)}$ to an element $\tau \cdot f \in \mathrm{Hom}(G_L, T_E^{(k)})^{(\alpha^{-1})}$. The intersection $\mathrm{Hom}(G_L, T_E^{(k)})^{(\alpha)} \cap \mathrm{Hom}(G_L, T_E^{(k)})^{(\alpha^{-1})}$ is annihilated by $\gamma - \alpha^{\pm 1}(\gamma)$ and so by $\alpha(\gamma) - \alpha^{-1}(\gamma)$, for all $\gamma \in \mathrm{Gal}(L/K)$. Since

$$\{\alpha(\gamma) - \alpha^{-1}(\gamma) \bmod \mathfrak{m}^k \ : \ \gamma \in \mathrm{Gal}(L/K)\} = \{\alpha(\gamma) - \alpha^{-1}(\gamma) \bmod \mathfrak{m}^k \ : \ \gamma \in \Gamma\}$$

and since $\alpha \neq \alpha^{-1}$ (as $\alpha \neq 1$ and p is odd), it follows from the definition of C_α that $\mathrm{Hom}(G_L, T_E^{(k)})^{(\alpha)} \cap \mathrm{Hom}(G_L, T_E^{(k)})^{(\alpha^{-1})}$ is annihilated by π^{rC_α}. This implies that $f_i^\pm = (1 \pm \tau) \cdot f_i$ satisfies

$$\mathrm{ord}(f_i^\pm) \geqslant \mathrm{ord}(f_i) - rC_\alpha \geqslant \mathrm{ord}(c_i) - r(C_1 + C_\alpha), \quad i = 1, 2, 3,$$

and that $Rf_1^\pm + Rf_2^\pm = (1 \pm \tau) \cdot (Rf_1 + Rf_2)$ contains a submodule isomorphic to $\mathfrak{m}^{d_1+r(C_1+C_\alpha)}R^{(k)} \oplus \mathfrak{m}^{d_2+r(C_1+C_\alpha)}R^{(k)}$. Note that since $\max\{m_1, m_2, m_3\} > 0$, it follows that for some j both f_j^+ and f_j^- are non-zero.

The R-module spanned by the image of $f_i^\pm$ contains $R[G_{K_\infty}] \cdot f_i^\pm(G_L)$. By Lemma 3.3.4, the latter contains $p^{C_2}(\mathrm{End}_{\mathbb{Z}_p}(T_pE) \otimes_{\mathbb{Z}_p} R) \cdot f_i^\pm(G_L) \subset T_E^{(k)}$. Since $f_i^\pm$ has order at least $\mathrm{ord}(f_i) - rC_\alpha$, $f_i^\pm(G_L)$ contains an element of order at least $\mathrm{ord}(f_i) - rC_\alpha$ and hence $\pi^{k-\mathrm{ord}(f_i)+r(C_2+C_\alpha)}T_E^{(k)} \subset p^{C_2}(\mathrm{End}_{\mathbb{Z}_p}(T_pE) \otimes_{\mathbb{Z}_p} R) \cdot f_i^\pm(G_L)$. In particular, the R-module spanned by the image of $f_i^\pm$ contains $\mathfrak{m}^{k-m_i}T_E^{(k)}$.

Let $H \subset G_L$ be the intersection of the kernels of the $f_i^\pm$. Since some $f_j^\pm$ is non-zero, $H \neq G_L$ and $Z = G_L/H$ is a non-zero torsion $\mathbb{Z}_p$-module. The subgroup H is stable under the action of complex conjugation and hence this action descends to Z, which then decomposes as $Z = Z^+ \oplus Z^-$ with respect to this action. Each $f_i^\pm$

can be viewed as an element of $\mathrm{Hom}(Z, T_E^{(k)})$. Let $g_i^\pm$ be the composition of $f_i^\pm$ with the projection of $T_E^{(k)}$ to $(T_E^{(k)})^\pm$. Fix an $R^{(k)}$-basis $u_\pm$ of $(T_E^{(k)})^\pm$. Since the R-span of the image of $f_i^\pm$ contains $\mathfrak{m}^{k-m_i}T_E^{(k)}$, the R-span of the image of $g_i^\pm$ contains $\mathfrak{m}^{k-m_i}R^{(k)}u_\pm$. Moreover, since $f_i^\pm \in \mathrm{Hom}(Z, T_E^{(k)})^\pm$, $g_i^\pm(Z^-) = 0$ and so $g_i^\pm(Z) = g_i^\pm(Z^+)$. Since $\max\{m_1, m_2, m_3\} > 0$, it follows that Z^+ is nontrivial.

Let $W^\pm = \sum_{i=1}^3 Rf_i^\pm \subset \mathrm{Hom}(G_L, T_E^{(k)})^\pm$ and let $W = W^+ \oplus W^- \subset \mathrm{Hom}(G_L, T_E^{(k)})$. Each $f \in W$ can be viewed as a homomorphism from Z to $T_E^{(k)}$, and evaluation at $z \in Z$ yields an injection

$$Z \hookrightarrow \mathrm{Hom}_R(W, T_E^{(k)}).$$

Furthermore, this injection is equivariant with respect to the action of complex conjugation, so the restriction to Z^+ is an injection

$$Z^+ \hookrightarrow \mathrm{Hom}_R(W, T_E^{(k)})^+ = \mathrm{Hom}_R(W^+, (T_E^{(k)})^+) \oplus \mathrm{Hom}_R(W^-, (T_E^{(k)})^-).$$

Let $X^+ \subset \mathrm{Hom}_R(W, T_E^{(k)})^+$ be the R-span of the image of Z^+. It follows from [Nek07, Cor. (6.3.4)] and Lemma 3.3.4 that

$$p^{C_2}\,\mathrm{Hom}_R(W, T_E^{(k)})^+ \subset X^+. \tag{3.4}$$

Given $(\phi^+, \phi^-) \in \mathrm{Hom}_R(W^+, (T_E^{(k)})^+) \oplus \mathrm{Hom}_R(W^-, (T_E^{(k)})^-)$, define

$$q(\phi^+, \phi^-) = \det\begin{pmatrix} \beta(\phi^+(f_1^+)) & \beta(\phi^-(f_1^-)) \\ \beta(\phi^+(f_2^+)) & \beta(\phi^-(f_2^-)) \end{pmatrix}, \quad \phi^\pm(-) = \beta(\phi^\pm(-))u_\pm \in R^{(k)}u_\pm = (T_E^{(k)})^\pm.$$

The restriction of q to X^+ defines an $R^{(k)}$-valued quadratic form on X^+ that we denote by $q(x)$. Since W^+ contains $Rf_1^+ + Rf_2^+$, which in turn contains a submodule isomorphic to $\mathfrak{m}^{d_1+r(C_1+C_\alpha)}R^{(k)} \oplus \mathfrak{m}^{d_2+r(C_1+C_\alpha)}R^{(k)}$, there exists $\psi^+ \in \mathrm{Hom}_R(W^+, (T_E^{(k)})^+)$ and $j \in \{1, 2\}$ such that $\beta(\psi^+(f_j^+)) \in \pi^{\max d_1, d_2 + r(C_1+C_\alpha)}(R^{(k)})^\times$. Similarly, there exists $\psi^- \in \mathrm{Hom}_R(W^-, (T_E^{(k)})^-)$ such that $\beta(\psi^-(f_{3-j}^-)) \in \pi^{\min d_1, d_2 + r(C_1+C_\alpha)}(R^{(k)})^\times$ and $\beta(\psi^-(f_j^-)) = 0$. For such a pair (ψ^+, ψ^-),

$$q(\psi^+, \psi^-) \in \pi^{d_1+d_2+2r(C_1+C_\alpha)}(R^{(k)})^\times.$$

From (3.4) it follows that $p^{C_2}(\psi^+, \psi^-) = x_\psi$ for some $x_\psi \in X^+$, and

$$q(x_\psi) = p^{2C_2}q(\psi^+, \psi^-) \in \pi^{d_1+d_2+2r(C_1+C_2+C_\alpha)}(R^{(k)})^\times.$$

It then follows from [Nek07, Lem. (6.6.1)(ii)] that

$$q(Z^+) \not\subset \mathfrak{m}^{d_1+d_2+2r(C_1+C_2+C_\alpha)+1}R^{(k)}. \tag{3.5}$$

If $m_3 > 0$, let $Z_3 \subset Z^+$ be the submodule such that $g_3^+(Z_3) = \mathfrak{m}^{k-m_3+1}R^{(k)}u_+$. Otherwise, let $Z_3 = 0$. Then Z_3 is a proper $\mathbb{Z}_p$-submodule of Z^+. It then follows from [Nek07, Lem. (6.6.1)(iii)] and (3.5) that

$$\text{there exists } z \in Z^+ \text{ such that } z \notin Z_3 \text{ and } q(z) \notin \mathfrak{m}^{d_1+d_2+2r(C_1+C_2+C_\alpha)+1}R^{(k)}. \tag{3.6}$$

Let M be the fixed field of the subgroup $H \subset G_L$, so $\mathrm{Gal}(M/L) = Z$. Let $g = \tau z \in \mathrm{Gal}(M/\mathbb{Q})$, and let $\ell \nmid pND_K$ be any prime such that each c_i is unramified at ℓ and $\mathrm{Frob}_\ell = g$ in $\mathrm{Gal}(M/\mathbb{Q})$ (there are infinitely many such ℓ: this is the application of the Čebotarev Density Theorem). Since G_L fixes $E[p^k]$ and K, Frob_ℓ acts as τ on K and $E[p^k]$. This means that ℓ is inert in K and that $a_\ell(E) \equiv \ell + 1 \equiv 0 \mod p^k$. That is, $\ell \in \mathscr{L}^{(k)}$.

Since ℓ is inert in K, the Frobenius element for K_ℓ is Frob_ℓ^2. Consider the restriction of c_i to K_ℓ. Since c_i is unramified at ℓ, $\mathrm{loc}_\ell(c_i) \in \mathrm{H}^1_{\mathrm{ur}}(K_\ell, T^{(k)})$. Evaluation at Frob_ℓ^2 is an isomorphism

$$\mathrm{H}^1_{\mathrm{ur}}(K_\ell, T^{(k)}) \xrightarrow{\sim} T^{(k)}/(\mathrm{Frob}_\ell^2 - 1)T^{(k)} = T^{(k)} = T_E^{(k)},$$

where the last equality is because Frob_ℓ^2 acts as $\tau^2 = 1$ on $T^{(k)}$ by the choice of ℓ. This means that $\mathrm{loc}_\ell(c_i)$ is completely determined by $c_i(\mathrm{Frob}_\ell^2)$. Furthermore, since $\mathrm{Frob}_\ell^2 = g^2 = z^2 \in \mathrm{Gal}(M/L)$, $c_i(\mathrm{Frob}_\ell^2) = f_i(z^2)$. Hence

$$c_i(\mathrm{Frob}_\ell^2) = f_i(z^2) = 2f_i(z) = f_i^+(z) + f_i^-(z) = (g_i^+(z), g_i^-(z)) \in T_E^{(k)} = (T_E^{(k)})^+ \oplus (T_E^{(k)})^-, \tag{3.7}$$

since the projection of $f_i^\pm$ to $(T_E^{(k)})^\mp$ vanishes on Z^+.

From (3.7) we see that $\operatorname{ord}(\operatorname{loc}_\ell(c_3)) = \operatorname{ord}(c_3(\operatorname{Frob}_\ell^2) = \operatorname{ord}(f_3(z^2)) \geqslant \operatorname{ord}(g_3^+(z))$. Since $z \notin Z_3$ by (3.6),

$$\operatorname{ord}(\operatorname{loc}_\ell(c_3)) \geqslant m_3,$$

which shows that ℓ satisfies the first condition of the theorem.

From (3.7) we also see that

$$R\operatorname{loc}_\ell(c_1) + R\operatorname{loc}_\ell(c_2) \xrightarrow{\sim} R(g_1^+(z), g_1^-(z)) + R(g_2^+(z), g_2^-(z)) \subset T_E^{(k)} = (T_E^{(k)})^+ \oplus (T_E^{(k)})^-.$$

Write $g_i^\pm(z) = \beta_i^\pm(z)u_\pm$. Then

$$q(z) = \det\begin{pmatrix} \beta_1^+(z) & \beta_1^-(z) \\ \beta_2^+(z) & \beta_2^-(z) \end{pmatrix}.$$

Since $q(z) \notin \mathfrak{m}^{d_1+d_2+2r(C_1+C_2+C_\alpha)+1}R^{(k)}$ by (3.6), it follows from the above expression for $q(z)$ that the module $R(g_1^+(z), g_1^-(z)) + R(g_2^+(z), g_2^-(z))$ contains a submodule isomorphic to $\mathfrak{m}^{d_1+d_2+2r(C_1+C_2+C_\alpha)}(R^{(k)} \oplus R^{(k)})$, which shows that ℓ also satisfies the second condition of the theorem. □

Corollary 3.3.7. *Suppose $\alpha \neq 1$. Let $c_1, c_2 \in \mathrm{H}^1(K, T^{(k)})$. Suppose $Rc_1 + Rc_2$ contains a submodule isomorphic to $\mathfrak{m}^{d_1}R^{(k)} \oplus \mathfrak{m}^{d_2}R^{(k)}$ for some $d_1, d_2 \geqslant 0$. Then there exist infinitely many primes $\ell \in \mathscr{L}^{(k)}$ such that $\operatorname{ord}(\operatorname{loc}_\ell(c_1)) \geqslant \operatorname{ord}(c_1) - r(C_1+C_2+C_\alpha)$ and $R\operatorname{loc}_\ell(c_1) + R\operatorname{loc}_\ell(c_2) \subset \mathrm{H}^1(K_\ell, T^{(k)})$ contains a submodule isomorphic to*

$$\mathfrak{m}^{k-\operatorname{ord}(c_1)+r(C_1+C_2+C_\alpha)}R^{(k)} \oplus \mathfrak{m}^{d_1+d_2+2r(C_1+C_2+C_\alpha)}R^{(k)}.$$

Proof. We apply Proposition 3.3.6 with $c_3 = c_1$. Then $R\operatorname{loc}_\ell(c_1) = R\operatorname{loc}_\ell(c_3)$ contains a submodule isomophic to $\mathfrak{m}^{k-\operatorname{ord}(c_3)+r(C_1+C_2+C_\alpha)}R^{(k)} = \mathfrak{m}^{k-\operatorname{ord}(c_1)+r(C_1+C_2+C_\alpha)}R^{(k)}$, and $R\operatorname{loc}_\ell(c_1) + R\operatorname{loc}_\ell(c_2)$ contains a submodule isomorphic to $\mathfrak{m}^{d_1+d_2+2r(C_1+C_2+C_\alpha)}(R^{(k)} \oplus R^{(k)})$, whence the conclusion of the corollary. □

With Proposition 3.3.6 – and especially Corollary 3.3.7 – in hand, we next prove the following theorem, which implies the first statement of Theorem 3.2.1 and will be used in the next section to prove the bound on the length of M_α.

Theorem 3.3.8. *Suppose $\alpha \neq 1$. If $\kappa_{\alpha,1} \in \mathrm{H}^1(K, T)$ is non-zero, then $\epsilon = 1$ and for $k \gg 0$, every element in $M^{(k)}(1)$ has order strictly less than k. In particular, $\mathrm{H}^1_{\mathcal{F}}(K, T) \simeq R$.*

Proof. Suppose $\kappa_1 := \kappa_{\alpha,1} \neq 0$. The assumption $\bar{T}^{G_K} = 0$ implies that $\mathrm{H}^1_{\mathcal{F}}(K, T)$ is torsion-free, so $\epsilon \geqslant 1$.

If $k \gg 0$, then the image of κ_1 in $\mathrm{H}^1_{\mathcal{F}}(K, T^{(k)})$, still denoted by κ_1 by abuse of notation, is non-zero and $\operatorname{ind}(\kappa_1, \mathrm{H}^1_{\mathcal{F}}(K, T)) = \operatorname{ind}(\kappa_1, \mathrm{H}^1_{\mathcal{F}}(K, T^{(k)}))$, where by the index $\operatorname{ind}(c, M)$ for M a finitely generated R-module and $c \in M$ we mean the smallest integer $m \geqslant 0$ such that c has non-zero image in $M/\mathfrak{m}^{m+1}M$ (equivalently, $c \in \mathfrak{m}^m M$). Let $s = \operatorname{ind}(\kappa_1, \mathrm{H}^1_{\mathcal{F}}(K, T))$. Let $e = r(C_1 + C_2 + C_\alpha)$. Suppose k also satisfies

$$k > s + 3e. \tag{3.8}$$

By the definition of s, there exist $c_1 \in \mathrm{H}^1_{\mathcal{F}}(K, T^{(k)})$ such that the image of c_1 in $\mathrm{H}^1_{\mathcal{F}}(K, T^{(k)})/\mathfrak{m}\mathrm{H}^1_{\mathcal{F}}(K, T^{(k)})$ is non-zero and $\kappa_1 = \pi^s c_1$. The assumption $\bar{T}^{G_K} = 0$ implies that $\mathrm{H}^1_{\mathcal{F}}(K, T)$ is torsion-free, so $Rc_1 \simeq R^{(k)}$. Suppose $c_2 \in \mathrm{H}^1_{\mathcal{F}}(K, T^{(k)})$ is such that $c_2 \notin Rc_1$. We will show that $\pi^{s+3e}c_2 \in Rc_1$. By (3.8) this implies that $\mathrm{H}^1_{\mathcal{F}}(K, T^{(k)})/Rc_1$ is annihilated by π^{k-1} and hence that $\epsilon \leqslant 1$. It then follows that $\epsilon = 1$ and every element in $M^{(k)}(1)$ has order strictly less than k. This in turn implies $\mathrm{H}^1_{\mathcal{F}}(K, T) \simeq R$, since $\mathrm{H}^1_{\mathcal{F}}(K, T)$ is torsion-free.

Let d be the order of the image of c_2 in $\mathrm{H}^1_{\mathcal{F}}(K, T^{(k)})/Rc_1$. Then $Rc_1 + Rc_2$ contains a submodule isomorphic to $R^{(k)} \oplus \mathfrak{m}^{k-d}R^{(k)}$. By Corollary 3.3.7, there exists $\ell \in \mathscr{L}^{(k)}$ such that $\operatorname{ord}(\operatorname{loc}_\ell(c_1)) \geqslant k - e$ and

$$R\operatorname{loc}_\ell(c_1) + R\operatorname{loc}_\ell(c_2) \text{ contains a submodule isomorphic to } \mathfrak{m}^e R^{(k)} \oplus \mathfrak{m}^{k-d+2e}R^{(k)}. \tag{3.9}$$

We now make use of the assumption that κ_1 belongs to a Kolyvagin system. The finite-singular relation of the definition of a Kolyvagin system implies that the image of $\kappa_\ell := \kappa_{\alpha,\ell}$ in $\mathrm{H}^1_{\mathcal{F}}(K, T^{(k)})$, which we also denote by κ_ℓ, satisfies

$$\operatorname{ord}(\operatorname{loc}_{\ell,\mathrm{s}}(\kappa_\ell)) = \operatorname{ord}(\operatorname{loc}_\ell(\kappa_1)) = \operatorname{ord}(\operatorname{loc}_\ell(\pi^s c_1)) \geqslant k - s - e, \tag{3.10}$$

where by $\operatorname{loc}_{\ell,\mathrm{s}}$ we mean the composition of loc_ℓ with the projection to $\mathrm{H}^1_{\mathrm{s}}(K_\ell, T^{(k)})$.

By global duality, the images of

$$\mathrm{H}^1_{\mathcal{F}}(K, T_\alpha^{(k)}) \xrightarrow{\operatorname{loc}_\ell} \mathrm{H}^1_{\mathrm{ur}}(K_\ell, T_\alpha^{(k)}) \quad \text{and} \quad \mathrm{H}^1_{\mathcal{F}^\ell}(K, T_{\alpha^{-1}}^{(k)}) \xrightarrow{\operatorname{loc}_{\ell,\mathrm{s}}} \mathrm{H}^1_{\mathrm{s}}(K_\ell, T_{\alpha^{-1}}^{(k)})$$

are mutual annihilators under local duality. Since $\tau\cdot\kappa_\ell\in \mathrm{H}^1_{\mathcal{F}^\ell}(K,T^{(k)}_{\alpha^{-1}})$, we easily conclude from (3.8), (3.9), and (3.10) that

$$k-s-e\leqslant k-d+2e.$$

That is, $d\leqslant s+3e$, as claimed. □

3.3.2. *Some simple algebra.* Our adaptation of Kolyvagin's arguments relies on the following simple results about finitely-generated torsion R-modules. For a finitely-generated torsion R-module M we write

$$\exp(M):=\min\{n\geqslant 0:\pi^nM=0\}=\max\{\mathrm{ord}(m):m\in M\}.$$

Lemma 3.3.9. *Let $N\subset M$ be finitely-generated torsion R-modules. Suppose $N\simeq\oplus_{i=1}^r R/\mathfrak{m}^{d_i(N)}$, $d_1(N)\geqslant\cdots\geqslant d_r(N)$, and $M\simeq\oplus_{i=1}^s R/\mathfrak{m}^{d_i(M)}$, $d_1(M)\geqslant\cdots\geqslant d_s(M)$. Then $r\leqslant s$ and*

$$d_i(N)\leqslant d_i(M),\quad i=1,\dots,r.$$

Proof. We have $r=\dim_{R/\mathfrak{m}}N[\pi]\leqslant\dim_{R/\mathfrak{m}}M[\pi]=s$, which proves the first claim.

We prove the second claim by induction on r. Let $d=d_r(N)$. Since $N[\pi^d]=N\cap M[\pi^d]$, the inclusion $N\subset M$ induces an inclusion

$$N'=N/N[\pi^d]\subset M/M[\pi^d]=M'.$$

Clearly, $N'\simeq\oplus_{i=1}^{r'}R/\mathfrak{m}^{d_i(N)-d}$, where r' is the smallest integer such that $d_i(N)=d$ for $r'+1\leqslant i\leqslant r$. Similarly, $M'\simeq\oplus_{i=1}^{s'}R/\mathfrak{m}^{d_i(M)-d}$. Since $r'<r$, the induction hypothesis implies that $d_i(M)\geqslant d_i(N)$ for $i=1,\dots,r'$. To complete the induction step we just need to show that at least r of the $d_i(M)$'s are $\geqslant d$. But this is clear from the injection $N[\pi^d]/N[\pi^{d-1}]\hookrightarrow M[\pi^d]/M[\pi^{d-1}]$, from which it follows that

$$r=\dim_{R/\mathfrak{m}}N[\pi^d]/N[\pi^{d-1}]\leqslant\dim_{R/\mathfrak{m}}M[\pi^d]/M[\pi^{d-1}].$$

□

Next we consider two short exact sequences of finitely-generated torsion R-modules

$$0\to X\to R/\mathfrak{m}^k\oplus M\xrightarrow{\alpha}R/\mathfrak{m}^{k-a}\oplus R/\mathfrak{m}^b\to 0 \tag{3.11}$$

and

$$0\to X\to R/\mathfrak{m}^k\oplus M'\xrightarrow{\beta}R/\mathfrak{m}^{a'}\oplus R/\mathfrak{m}^{k-b'}\to 0 \tag{3.12}$$

satisfying:

$$k>\exp(M)+2a\quad\text{and}\quad a'\leqslant a. \tag{3.13}$$

We further assume that both M and M' are the direct sum of two isomorphic R-modules. Let $2s:=\dim_{R/\mathfrak{m}}M[\pi]$, $2s':=\dim_{R/\mathfrak{m}}M'[\pi]$ and $d_1(M),\dots,d_{2s}(M)$ be the lengths of the R-summands in a decomposition of M as a direct sum of cyclic R-modules, ordered so that

$$d_1(M)=d_2(M)\geqslant d_3(M)=d_4(M)\geqslant\cdots\geqslant d_{2s-1}(M)=d_{2s}(M).$$

Note that $d_1(M)=\exp(M)$. Fix a decomposition

$$M=\oplus_{i=1}^{2s}M_i,\quad M_i\simeq R/\mathfrak{m}^{d_i(M)}.$$

Let $d_1(M'),\dots,d_{2s'}(M')$ be similarly defined for M'.

Lemma 3.3.10. *The following hold:*

(i) $s-1\leqslant s'\leqslant s+1$,
(ii) $b\leqslant\exp(M)$,
(iii) $\exp(X)\leqslant\exp(M)+a$.

Proof. Let $r(-)$ denote the minimal number of R-generators of $(-)$. Then from (3.11) it follows that $r(M)-1\leqslant r(X)\leqslant r(M)+1$ (see Lemma 3.3.9). Similarly, it follows from (3.12) that $r(M')-1\leqslant r(X)\leqslant r(M')+1$. From this we conclude that $r(M)-1\leqslant r(M')+1$ and $r(M')-1\leqslant r(M)+1$. Since $r(M)=2s$ and $r(M')=2s'$, this implies $2s\leqslant 2s'+2$ and $2s'\leqslant 2s+2$. That is, $s-1\leqslant s'\leqslant s+1$, as claimed in part (i).

For part (ii) we note that since $k-a>\exp(M)$ by (3.13), the image under α of the summand $R/\mathfrak{m}^k$ in the middle of (3.11) must be isomorphic to $R/\mathfrak{m}^{\max\{k-a,b\}}$ (else $\exp(\mathrm{im}(\alpha))\leqslant\max\{k-a,b\}-1$). It follows that α induces a surjection $M\twoheadrightarrow(R/\mathfrak{m}^{k-a}\oplus R/\mathfrak{m}^b)/\alpha(R/\mathfrak{m}^k)\simeq R/\mathfrak{m}^{\min\{k-a,b\}}$. In particular, $\min\{k-a,b\}\leq\exp(M)$. As $k-a>\exp(M)$, this implies part (ii).

For part (iii) we note that (3.11) induces an inclusion

$$X/(X \cap R/\mathfrak{m}^k) \hookrightarrow (R/\mathfrak{m}^k \oplus M)/(R/\mathfrak{m}^k) \simeq M.$$

It follows that $\exp(X) \leqslant \exp(M) + \exp(X \cap R/\mathfrak{m}^k)$. As noted in the proof of part (ii), $\alpha(R/\mathfrak{m}^k) \simeq R/\mathfrak{m}^{k-a}$ so $X \cap R/\mathfrak{m}^k \simeq R/\mathfrak{m}^a$. Part (iii) follows. □

Proposition 3.3.11. *The following hold:*

(i) *There exists $1 \leqslant i_0 \leqslant 2s$ such that there is an inclusion $\oplus_{i=1, i\neq i_0}^{2s} M_i \hookrightarrow X$.*
(ii) *There exists an inclusion $X \hookrightarrow M' \oplus R/\mathfrak{m}^{\exp(X)}$.*
(iii) *$d_i(M') \geqslant d_{i+2}(M)$, for $i = 1, \dots, 2s-2$.*

Proof. As explained in the proof of Lemma 3.3.10(ii), the image under α of the $R/\mathfrak{m}^k$ summand in the middle of (3.11) has exponent $k-a$. In particular, we may assume that the $R/\mathfrak{m}^{k-a}$ summand on the right in (3.11) is the image under α of the $R/\mathfrak{m}^k$-summand in the middle.

Let $1 \leqslant i_0 \leqslant 2s$ be such that $\mathrm{im}(\alpha) = R/\mathfrak{m}^{k-a} + \alpha(M_{i_0})$. It follows from (3.11) that there is a surjection

$$X \twoheadrightarrow (R/\mathfrak{m}^k \oplus M)/(R/\mathfrak{m}^k \oplus M_{i_0}) \simeq \oplus_{i=1, i\neq i_0}^{2s} M_i.$$

Taking duals we deduce the existence of an inclusion $\oplus_{i=1, i\neq i_0}^{2s} M_i \hookrightarrow X$, proving (i). (Here and in the following we are using that the (Pontryagin) dual of a torsion R-module is isomorphic to itself as an R-module.)

For (ii), we first claim that $\beta(R/\mathfrak{m}^k) \simeq R/\mathfrak{m}^{k-b'}$. Suppose that $\beta(R/\mathfrak{m}^k) \simeq R/\mathfrak{m}^{k-b''}$ for some $b'' > b'$. This would imply that there exists $m' \in M$ such that $\beta(1 \oplus m') \in R/\mathfrak{m}^{a'} \oplus 0 \subset R/\mathfrak{m}^{a'} \oplus R/\mathfrak{m}^{k-b'}$. In particular, we would have $\pi^{a'}(1 \oplus m') \in X$. But since $\mathrm{ord}(\pi^{a'}(1 \oplus m')) = k - a'$ this would mean that X contains a submodule isomorphic to $R/\mathfrak{m}^{k-a'}$. But since $k - a' > \exp(M) + a \geqslant \exp(X)$ by (3.13) and Lemma 3.3.10(iii), we reach a contradiction. Thus we may assume that the $R/\mathfrak{m}^{k-b'}$ summand on the right in (3.12) is the image under β of the $R/\mathfrak{m}^k$-summand in the middle.

Let $M'' \subset M'$ be the submodule such that $\beta(M'') \subseteq R/\mathfrak{m}^{k-b'}$. Then (3.12) implies that there is an exact sequence

$$0 \to X \to R/\mathfrak{m}^k \oplus M'' \to \beta(R/\mathfrak{m}^k) \to 0.$$

From this it follows that there is an exact sequence

$$0 \to X \cap R/\mathfrak{m}^k \to X \to M'' \to 0.$$

Taking duals we conclude that there exists a short exact sequence

$$0 \to M'' \to X \xrightarrow{\gamma} X \cap R/\mathfrak{m}^k \to 0.$$

Note that $X \cap R/\mathfrak{m}^k$ is a cyclic R-module. Let $R/\mathfrak{m}^d \subset X$ be an R-summand that surjects onto $X \cap R/\mathfrak{m}^k$ via γ. Then there is a surjection $M'' \oplus R/\mathfrak{m}^d \twoheadrightarrow X$. Taking duals we deduce the existence of inclusions

$$X \hookrightarrow M'' \oplus R/\mathfrak{m}^d \hookrightarrow M' \oplus R/\mathfrak{m}^{\exp(X)}.$$

This proves (ii).

Let $d_1(X) \geqslant d_2(X) \geqslant \cdots \geqslant d_t(X)$ be the lengths of the summands in a decomposition of X as a direct sum of cyclic R-modules. Note that $d_1(X) = \exp(X)$. From part (i) we see that $t \geqslant 2s-1$. From part (i) and Lemma 3.3.9 we also easily conclude that $d_i(X) \geqslant d_{i+1}(M)$. Similarly, from part (ii) we conclude that $d_i(M') \geqslant d_{i+1}(X)$. Combining these yields (iii). □

3.3.3. *Finishing the proof of Theorem 3.2.1.* We now have all the pieces needed to prove Theorem 3.2.1.

Since the character α is fixed, for the rest of the proof we denote $\kappa_n := \kappa_{\alpha,n}$ for all $n \in \mathcal{N}$. In particular, our assumption is that $\kappa_1 \neq 0$. Let

$$\mathrm{ind}(\kappa_1) = \max\{m \ : \ \kappa_1 \in \mathfrak{m}^m \mathrm{H}^1_{\mathcal{F}}(K,T)\}.$$

We can write $\mathrm{H}^1_{\mathcal{F}}(K,A) = (\Phi/R)^n \oplus M$, for $n \geq 0$ and M a finite R-module. Since $\mathrm{H}^1_{\mathcal{F}}(K,A) = \varinjlim_k \mathrm{H}^1_{\mathcal{F}}(K,T^{(k)})$, it follows from Lemma 3.3.1 that

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

Recall that by Theorem 3.3.8 (and its proof), $\mathrm{H}^1_{\mathcal{F}}(K,T)$ has R-rank one and for $k \gg 0$

$$(R/\mathfrak{m}^k)^n \oplus M[\mathfrak{m}^k] \simeq R/\mathfrak{m}^k \oplus M^{(k)}(1) \oplus M^{(k)}(1),$$

with $\exp(M^{(k)}(1)) < k$ and hence

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

for some finitely-generated torsion R-module M_0 such that $M_0 \simeq M^{(k)}(1)$ for $k \gg 0$.

Let $r(M)$ be the minimal number of R-generators of M and let

$$e = (C_1 + C_2 + C_\alpha)\mathrm{rank}_{\mathbb{Z}_p}(R).$$

We will show that

$$\mathrm{ind}(\kappa_1) + \frac{3}{2}r(M)e \geqslant \mathrm{length}_R(M_0). \tag{3.14}$$

Since by Lemma 3.3.1 and (3.2) we have

$$r(M) + 1 = \dim_{R/\mathfrak{m}} \mathrm{H}^1_{\mathcal{F}}(K, T^{(k)})[\mathfrak{m}] = \dim_{R/\mathfrak{m}} \mathrm{H}^1_{\mathcal{F}}(K, \bar{T}) = \dim_{\mathbb{F}_p} \mathrm{H}^1_{\mathcal{F}}(K, E[p]),$$

it follows that (3.14) yields the inequality in Theorem 3.2.1 with an error term $E_\alpha = r(M)e$ that depends only on C_α, T_pE, and $\mathrm{rank}_{\mathbb{Z}_p}(R)$.

Let $s = r(M)/2$ and fix an integer $k > 0$ such that

$$k/2 > \mathrm{length}_R(M_0) + \mathrm{ind}(\kappa_1) + (r(M)+1)e \tag{3.15}$$

and $M_0 \simeq M^{(k)}(1)$. Our proof of (3.14) relies on making a good choice of integers in $\mathscr{N}^{(k)}$, which in turn relies on a good choice of primes in $\mathscr{L}^{(k)}$.

Let $n \in \mathscr{N}^{(k)}$. By Proposition 3.3.2 and Theorem 3.3.8, there exists a finite $R^{(k)}$-module $M(n)_0$ such that

$$\mathrm{H}^1_{\mathcal{F}(n)}(K, T^{(k)}) \simeq R^{(k)} \oplus M(n), \quad M(n) \simeq M(n)_0 \oplus M(n)_0.$$

Let $r(M(n))$ be the minimal number of R-generators of $M(n)$ and let

$$d_1(n) = d_2(n) \geqslant d_3(n) = d_4(n) \geqslant \cdots \geqslant d_{r(M(n))-1}(n) = d_{r(M(n))}(n)$$

be the lengths of the cyclic R-modules appearing in an expression for $M(n)$ as a direct sum of such modules. Let $s(n) = r(M(n))/2$. In particular, $s(1) = r(M)/2 = s$. In what follows we write, in an abuse of notation, κ_n to mean its image in $\mathrm{H}^1(K, T^{(k)})$.

Suppose we have a sequence of integers $1 = n_0, n_1, n_2, \ldots, n_s \in \mathscr{N}^{(k)}$ satisfying

(a) $s(n_j) \geqslant s(n_{j-1}) - 1$,
(b) $d_t(n_j) \geqslant d_{t+2}(n_{j-1})$, $t = 1, \ldots, s(n_{j-1}) - 1$,
(c) $\mathrm{length}_R(M(n_j)_0) \leqslant \mathrm{length}_R(M(n_{j-1})_0) - d_1(n_{j-1}) + 3e$,
(d) $\mathrm{ord}(\kappa_{n_j}) \geqslant \mathrm{ord}(\kappa_{n_{j-1}}) - e$, and
(e) $\mathrm{ord}(\kappa_{n_{j-1}}) \leqslant \mathrm{ord}(\kappa_{n_j}) - d_1(n_{j-1}) + 3e$,

for all $1 \leqslant j \leqslant s$. Since $\mathrm{H}^1_{\mathcal{F}}(K,T)$ is torsion free, $\mathrm{ind}(\kappa_1) = k - \mathrm{ord}(\kappa_1)$, and so repeated combination of (b) and (e) yields

$$\begin{aligned}\mathrm{ind}(\kappa_1) = k - \mathrm{ord}(\kappa_{n_0}) &\geqslant d_1(n_0) + d_3(n_0) + \cdots + d_{2s-1}(n_0) - 3se + (k - \mathrm{ord}(\kappa_{n_s})) \\ &\geqslant \mathrm{length}_R(M(n_0)_0) - 3se.\end{aligned}$$

Since $M(n_0)_0 = M(1)_0 \simeq M^{(k)}(1)_0 \simeq M_0$ by the choice of k and $3se = \frac{3}{2}r(M)e$, this means (3.14) holds. So to complete the proof of the theorem it suffices to find such a sequence of n_j's. In the following we will define such a sequence by making repeated use of Corollary 3.3.7 to choose suitable primes in $\mathscr{L}^{(k)}$. Note that if $s = 0$ then there is nothing to prove, so we assume $s > 0$.

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

From (a), $s(n_i) \geqslant s - i > 0$, so $d_1(n_i) > 0$. Let $c_1, c_2 \in \mathrm{H}^1_{\mathcal{F}(n_i)}(K, T^{(k)})$ be such that c_1 generates an $R^{(k)}$-summand complementary to $M(n_i)$ and $Rc_2 \simeq R/\mathfrak{m}^{d_1(n_i)} = \mathfrak{m}^{k-d_1(n_i)}R^{(k)}$ is a direct summand of $M(n_i) = M(n_i)_0 \oplus M(n_i)_0$. Then $Rc_1 + Rc_2 \subset \mathrm{H}^1_{\mathcal{F}(n_i)}(K, T^{(k)})$ contains a submodule isomorphic to $R^{(k)} \oplus \mathfrak{m}^{k-d_1(n_i)}R^{(k)}$. Let $\ell \in \mathscr{L}^{(k)}$ be a prime as in Corollary 3.3.7 that does not divide $n_1 \cdots n_i$. In particular,

$$\mathrm{ord}(\mathrm{loc}_\ell(c_1)) \geqslant k - e$$

and

$$R\operatorname{loc}_\ell(c_1) + R\operatorname{loc}_\ell(c_2) \text{ contains a submodule isomorphic to } \mathfrak{m}^e R^{(k)} \oplus \mathfrak{m}^{k-d_1(n_i)+2e}R^{(k)}.$$

It follows that there is a short exact sequence

$$(3.16)\qquad 0 \to \mathrm{H}^1_{\mathcal{F}(n_i)_\ell}(K,T^{(k)}) \to \mathrm{H}^1_{\mathcal{F}(n_i)}(K,T^{(k)}) \xrightarrow{\operatorname{loc}_\ell} R/\mathfrak{m}^{k-a} \oplus R/\mathfrak{m}^b \to 0, \quad e \geqslant a,\ b \geqslant d_1(n_i) - 2e.$$

Global duality then implies that there is another exact sequence

$$(3.17)\qquad 0 \to \mathrm{H}^1_{\mathcal{F}(n_i)_\ell}(K,T^{(k)}) \to \mathrm{H}^1_{\mathcal{F}(n_i\ell)}(K,T^{(k)}) \xrightarrow{\operatorname{loc}_\ell} R/\mathfrak{m}^{a'} \oplus R/\mathfrak{m}^{k-b'} \to 0, \quad e \geqslant a \geqslant a',\ b' \geqslant b.$$

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

Combining (c) for $1 \leqslant j \leqslant i$ yields

$$\operatorname{length}_R(M(n_i)_0) \leqslant \operatorname{length}_R(M(n_0)_0) + 3ie.$$

From this, together with $r(M) = 2s$, $i < s$, and the assumption (3.15), we find

$$k > 2\operatorname{length}_R(M(n_0)_0) + 2r(M)e \geqslant 2\operatorname{length}_R(M(n_i)_0) + 2r(M)e - 3ie > \operatorname{length}_R(M(n_i)) + 2e.$$

It follows that (3.16) and (3.17) satisfy the hypotheses (3.13) for (3.11) and (3.12) with

$$X = \mathrm{H}^1_{\mathcal{F}(n_i)_\ell}(K,T^{(k)}), \quad M = M(n_i), \quad M' = M(n_i\ell).$$

Let $n_{i+1} = n_i\ell$. Then (a) for $j = i+1$ follows from Lemma 3.3.10(i) while (b) for $j = i+1$ follows from Proposition 3.3.11(iii). To see that (c) holds we observe that by (3.16) and (3.17)

$$\operatorname{length}_R(M(n_{i+1})) = \operatorname{length}_R(M(n_i)) - (b+b') + (a+a') \leqslant \operatorname{length}_R(M(n_i)) - 2d_1(n_i) + 6e.$$

To verify (d) for $j = i+1$ we first observe that by the Kolyvagin system relations under the finite singular map

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

So (d) holds for $j = i+1$ if we can show that $\operatorname{ord}(\operatorname{loc}_\ell(\kappa_{n_i})) \geqslant \operatorname{ord}(\kappa_{n_i}) - e$. To check that this last inequality holds, we first note that $\operatorname{ord}(\kappa_{n_i}) \geqslant \operatorname{ord}(\kappa_{n_0}) - ie$ by (d) for $1 \leqslant j \leqslant i$. But $\operatorname{ord}(\kappa_{n_0}) = \operatorname{ord}(\kappa_1) = k - \operatorname{ind}(\kappa_1)$ by the choice of k (and the fact that $\mathrm{H}^1_{\mathcal{F}}(K,T)$ is torsion-free), and so by (3.15) and repeated application of (c) for $1 \leqslant j \leqslant i$ we have

$$\begin{aligned}\operatorname{ord}(\kappa_{n_i}) \geqslant k - \operatorname{ind}(\kappa_1) - ie &> 4\cdot\operatorname{length}_R(M(n_0)_0) + (4s - i + 2)e\\ &> 3\cdot\operatorname{length}_R(M(n_0)_0) + \operatorname{length}_R(M(n_i)_0) + (4s - 4i + 2)e\\ &> \operatorname{length}_R(M(n_i)_0) + 2e.\end{aligned}$$

Write $\kappa_{n_i} = xc_1 + m$ with $x \in R^{(k)}$ and $m \in M(n_i)$. Since $\operatorname{ord}(\kappa_{n_i}) > \exp(M(n_i)_0)$, it follows that $x = \pi^t u$ for $t = k - \operatorname{ord}(\kappa_{n_i})$ and some $u \in R^\times$. Let $n = \exp(M(n_i))$. It follows that

$$\pi^n \operatorname{loc}_\ell(\kappa_{n_i}) = \pi^{n+t}u\operatorname{loc}_\ell(c_1).$$

By the choice of ℓ, $\operatorname{ord}(\operatorname{loc}_\ell(c_1)) \geqslant k - e$. Since $n + t = k - \operatorname{ord}(\kappa_{n_i}) + \exp(M(n_i)_0) < k - 2e$, it then follows that

$$\operatorname{ord}(\operatorname{loc}_\ell(\kappa_{n_i})) = \operatorname{ord}(\operatorname{loc}_\ell(c_1)) - t \geqslant k - e - t = \operatorname{ord}(\kappa_{n_i}) - e.$$

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

$$\operatorname{ord}(\operatorname{loc}_\ell(\kappa_{n_i})) = \operatorname{ord}(\operatorname{loc}_\ell(c_1)) - g \quad\text{and}\quad \operatorname{ord}(\operatorname{loc}_\ell(\kappa_{n_{i+1}})) = \operatorname{ord}(\operatorname{loc}_\ell(c)) - h.$$

From the Kolyvagin system relations under the finite singular map it then follows that

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

We refer again to the exact sequences (3.16) and (3.17). By the choice of ℓ, $\operatorname{ord}(\operatorname{loc}_\ell(c_1)) \geqslant k - e > \exp(M(n_i)_0) \geq b$, the last inequality by Lemma 3.3.10(ii). Hence we must have $\operatorname{ord}(\operatorname{loc}_\ell(c_1)) = k - a$. As shown in the proof of Proposition 3.3.11 (ii), we also must have $\operatorname{ord}(\operatorname{loc}_\ell(c)) = k - b'$. Hence we find

$$h - g = (k - b') - (k - a) = a - b' \leqslant 3e - d_1(n_{j-1}).$$

Since $h-g=\mathrm{ord}(\kappa_{n_i})-\mathrm{ord}(\kappa_{n_{i+1}})$, this proves (e) holds for $j=i+1$ and so concludes the proof of Theorem 3.2.1.

3.4. **Iwasawa theory.** Let E, p, and K be as in §3.2. Let $\Lambda=\mathbb{Z}_p[\![\Gamma]\!]$ be the anticyclotomic Iwasawa algebra, and consider the Λ-modules

$$M_E:=(T_pE)\otimes_{\mathbb{Z}_p}\Lambda^\vee,\quad \mathbf{T}:=M_E^\vee(1)\simeq(T_pE)\otimes_{\mathbb{Z}_p}\Lambda,$$

where the G_K-action on $\Lambda^\vee$ is given by the inverse Ψ^{-1} of the tautological character $\Psi:G_K\twoheadrightarrow\Gamma\hookrightarrow\Lambda^\times$.

For w a prime of K above p, put

$$\mathrm{Fil}_w^+(M_E):=\mathrm{Fil}_w^+(T_pE)\otimes_{\mathbb{Z}_p}\Lambda^\vee,\quad \mathrm{Fil}_w^+\mathbf{T}:=\mathrm{Fil}_w^+(T_pE)\otimes_{\mathbb{Z}_p}\Lambda.$$

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

$$\mathrm{H}^1_{\mathcal{F}_\Lambda}(K_w,M_E):=\begin{cases}\mathrm{im}\{\mathrm{H}^1(K_w,\mathrm{Fil}_w^+(M_E))\to\mathrm{H}^1(K_w,M_E)\} & \text{if } w|p,\\ 0 & \text{else,}\end{cases}$$

and

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

Denote by

$$\mathcal{X}=\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,M_E)^\vee=\mathrm{Hom}_{\mathrm{cts}}(\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,M_E),\mathbb{Q}_p/\mathbb{Z}_p)$$

the Pontryagin dual of the associated Selmer group $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,M_E)$, and let $\mathscr{L}_E\subset\mathscr{L}_0$ be as in §3.2.

Recall that $\gamma\in\Gamma$ is a topological generator. Then $\mathfrak{P}_0:=(\gamma-1)\subset\Lambda$ is a height one prime independent of the choice of γ.

Theorem 3.4.1. *Suppose there is a Kolyvagin system $\kappa\in\mathbf{KS}(\mathbf{T},\mathcal{F}_\Lambda,\mathscr{L}_E)$ with $\kappa_1\neq0$. Then $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$ has Λ-rank one, and there is a finitely generated torsion Λ-module M such that*

(i) $\mathcal{X}\sim\Lambda\oplus M\oplus M$,
(ii) $\mathrm{char}_\Lambda(M)$ *divides* $\mathrm{char}_\Lambda\big(\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})/\Lambda\kappa_1\big)$ *in* $\Lambda[1/p,1/(\gamma-1)]$.

Proof. This follows by applying Theorem 3.2.1 for the specializations of $\mathbf{T}$ at height one primes of Λ, similarly as in the proof of [How04a, Thm. 2.2.10]. We only explain how to deduce the divisibility in part (ii), since part (i) is shown exactly as in [How04a, Thm. 2.2.10].

For any height one prime $\mathfrak{P}\neq p\Lambda$ of Λ, let $S_\mathfrak{P}$ be the integral closure of $\Lambda/\mathfrak{P}$ and consider the G_K-module

$$T_\mathfrak{P}:=\mathbf{T}\otimes_\Lambda S_\mathfrak{P},$$

where G_K acts on $S_\mathfrak{P}$ via $\alpha_\mathfrak{P}:\Gamma\hookrightarrow\Lambda^\times\to S_\mathfrak{P}^\times$. Note that $T_\mathfrak{P}$ is a G_K-module of the type considered in §3.2. In particular, $S_\mathfrak{P}$ is the ring of integers of a finite extension of $\mathbb{Q}_p$, and $T_\mathfrak{P}=T_pE\otimes_{\mathbb{Z}_p}S_\mathfrak{P}(\alpha_\mathfrak{P})$, where $\alpha_\mathfrak{P}=\Psi^{-1}\bmod\mathfrak{P}$.

Fix $\mathfrak{P}$ as above, write $\mathfrak{P}=(g)$, and set $\mathfrak{Q}:=(g+p^m)$ for some integer m. For $m\gg0$, $\mathfrak{Q}$ is also a height one prime of Λ. As explained in [How04a, p. 1463], there is a specialization map

$$\mathbf{KS}(\mathbf{T},\mathcal{F}_\Lambda,\mathscr{L}_E)\to\mathbf{KS}(T_\mathfrak{Q},\mathcal{F}_{\mathrm{ord}},\mathscr{L}_E).$$

Writing $\kappa^{(\mathfrak{Q})}$ for the image of κ under this map, the hypothesis $\kappa_1\neq0$ implies that $\kappa_1^{(\mathfrak{Q})}$ generates an infinite $S_\mathfrak{Q}$-submodule of $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ord}}}(K,T_\mathfrak{Q})$ for $m\gg0$. By Theorem 3.2.1, it follows that X and $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$ have both Λ-rank one, and letting f_Λ be a characteristic power series for $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})/\Lambda\kappa_1$ we see as in [How04a, p. 1463] that the equalities

$$\mathrm{length}_{\mathbb{Z}_p}\big(\mathrm{H}^1_{\mathcal{F}_\mathfrak{Q}}(K,T_\mathfrak{Q})/S_\mathfrak{Q}\kappa_1^{(\mathfrak{Q})}\big)=md\,\mathrm{ord}_\mathfrak{P}(f_\Lambda)$$

and

$$2\,\mathrm{length}_{\mathbb{Z}_p}(M_\mathfrak{Q})=md\,\mathrm{ord}_\mathfrak{P}\big(\mathrm{char}_\Lambda(\mathcal{X}_{\mathrm{tors}})\big)$$

hold up to $O(1)$ as m varies, where $d=\mathrm{rank}_{\mathbb{Z}_p}(\Lambda/\mathfrak{P})$ and X_{tors} denotes the Λ-torsion submodule of X.

On the other hand, Theorem 3.2.1 yields the inequality

$$\mathrm{length}_{\mathbb{Z}_p}(M_{\alpha_\mathfrak{Q}})\leqslant\mathrm{length}_{\mathbb{Z}_p}\big(\mathrm{H}^1_{\mathcal{F}_\mathfrak{Q}}(K,T_\mathfrak{Q})/S_\mathfrak{Q}\kappa_1^{(\mathfrak{Q})}\big)+E_{\alpha_\mathfrak{Q}}.$$

If $\mathfrak{P} \neq \mathfrak{P}_0$, then the error term $E_{\alpha_{\mathfrak{Q}}}$ is bounded independently of m, since $\mathrm{rank}_{\mathbb{Z}_p}(S_{\mathfrak{Q}}) = \mathrm{rank}_{\mathbb{Z}_p}(S_{\mathfrak{P}})$ and the term $C_{\alpha_{\mathfrak{Q}}}$ in (3.3) satisfies $C_{\alpha_{\mathfrak{Q}}} = C_{\alpha_{\mathfrak{P}}}$ for $m \gg 0$. Letting $m \to \infty$ we thus deduce

$$\mathrm{ord}_{\mathfrak{P}}\big(\mathrm{char}_\Lambda(\mathcal{X}_{\mathrm{tors}})\big) \leqslant 2\,\mathrm{ord}_{\mathfrak{P}}(f_\Lambda),$$

for $\mathfrak{P} \neq (p), \mathfrak{P}_0$, yielding the divisibility in part (ii). □

Corollary 3.4.2. *Let the hypotheses be as in Theorem 3.4.1. Assume also that* $\mathrm{H}^1_{\mathcal{F}}(K, E[p^\infty])$ *has* $\mathbb{Z}_p$*-corank one (equivalently,* $\mathrm{H}^1_{\mathcal{F}}(K, T_pE)$ *has* $\mathbb{Z}_p$*-rank one). Then* $\mathrm{char}_\Lambda(M)$ *divides* $\mathrm{char}_\Lambda\big(\mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})/\Lambda\kappa_1\big)$ *in* $\Lambda[1/p]$.

Proof. The assumption that $\mathrm{H}^1_{\mathcal{F}}(K, E[p^\infty])$ has $\mathbb{Z}_p$-corank one implies that $X_{\mathrm{tors}}/\mathfrak{P}_0 X_{\mathrm{tors}}$ is a torsion $\mathbb{Z}_p$-module and hence that $\mathrm{ord}_{\mathfrak{P}_0}(\mathrm{char}_\Lambda(X_{\mathrm{tors}})) = 0$. □

4. Proof of Theorem C and Corollary D

4.1. **Preliminaries.** Let E, p, and K be as in §3.2, and assume in addition that hypotheses (Heeg) and (disc) hold. Fix an integral ideal $\mathfrak{N} \subset \mathcal{O}_K$ with $\mathcal{O}_K/\mathfrak{N} = \mathbb{Z}/N\mathbb{Z}$. For each positive integer m prime to N, let $K[m]$ be the ring class field of K of conductor m, and set

$$G[m] = \mathrm{Gal}(K[m]/K[1]), \qquad \mathcal{G}[m] = \mathrm{Gal}(K[m]/K).$$

Let also $\mathcal{O}_m = \mathbb{Z} + m\mathcal{O}_K$ be the order of K of conductor m.

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

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

defines a point $x_m \in X_0(N)(K[m])$, and fixing a modular parameterization $\pi : X_0(N) \to E$ we define the *Heegner point* of conductor m by

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

Building on this construction, one can prove the following result.

Theorem 4.1.1. *Assume* $E(K)[p] = 0$*. Then there exists a Kolyvagin system* $\kappa^{\mathrm{Hg}} \in \mathbf{KS}(\mathbf{T}, \mathcal{F}_\Lambda, \mathscr{L}_E)$ *such that* $\kappa_1^{\mathrm{Hg}} \in \mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ *is nonzero.*

Proof. Under the additional hypotheses that $p \nmid h_K$, the class number of K, and the representation $G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(T)$ is surjective, this is [How04a, Thm. 2.3.1]. In the following paragraphs, we explain how to adapt Howard's arguments to our situation.

We begin by briefly recalling the construction of κ^{Hg} in [How04a, §2.3]. Let K_k be the subfield of K_∞ with $[K_k\colon K] = p^k$. For each $n \in \mathcal{N}$ set

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

where $d(k) = \min\{d \in \mathbb{Z}_{\geqslant 0}\colon K_k \subset K[p^{d(k)}]\}$, and $K_k[n]$ denotes the compositum of K_k and $K[n]$. Letting $H_k[n] \subset E(K_k[n]) \otimes \mathbb{Z}_p$ be the $\mathbb{Z}_p[\mathrm{Gal}(K_k[n]/K)]$-submodule generated by $P[n]$ and $P_j[n]$ for $j \leqslant k$, it follows from the Heegner point norm relations [PR87, §3.1] that one can form the $\mathcal{G}(n)$-module

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

By [How04a, Lem. 2.3.3], there is a family

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

such that

$$Q_0[n] = \Phi P[n], \quad \text{where } \Phi = \begin{cases} (p - a_p\sigma_p + \sigma_p^2)(p - a_p\sigma_p^* + \sigma_p^{*2}) & \text{if } p \text{ splits in } K, \\ (p+1)^2 - a_p^2 & \text{if } p \text{ is inert in } K, \end{cases} \tag{4.1}$$

with σ_p and σ_p^* the Frobenius elements at the primes above p in the split case, and

$$\mathrm{Norm}_{K_\infty[n\ell]/K_\infty[n]} Q[n\ell] = a_\ell Q[n]$$

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

$$\tilde{\kappa}_n := \sum_{s \in S} s D_n Q[n] \in \mathbf{H}[n] \tag{4.2}$$

under the composite map

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

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

The proof that the classes κ_n land in $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$ and can be modified to a system $\kappa^{\mathrm{Hg}} = \{\kappa_n^{\mathrm{Hg}}\}_{n\in\mathscr{N}}$ satisfying the Kolyvagin system relations is the same as in [How04a, Lem. 2.3.4] *et seq.*, noting that the arguments proving Lemma 2.3.4 (in the case $v|p$) apply almost *verbatim* in the case when p divides the class number of K. Finally, that κ_1^{Hg} is nonzero follows from the works of Cornut and Vatsal [Cor02, Vat03]. □

Applying Theorem 3.4.1 and Corollary 3.4.2 to the Kolyvagin system κ^{Hg} of Theorem 4.1.1, we thus obtain the following.

Theorem 4.1.2. *Assume $E(K)[p]=0$. Then the module $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$ has Λ-rank one, and there is a finitely generated torsion Λ-module M such that*

(i) *$\mathcal{X}\sim\Lambda\oplus M\oplus M$,*

(ii) *$\mathrm{char}_\Lambda(M)$ divides $\mathrm{char}_\Lambda\big(\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})/\Lambda\kappa_1^{\mathrm{Hg}}\big)$ in $\Lambda[1/p,1/(\gamma-1)]$.*

Moreover, if $\mathrm{H}^1_{\mathcal{F}}(K,E[p^\infty])$ has $\mathbb{Z}_p$-corank one, then $\mathrm{char}_\Lambda(M)$ divides $\mathrm{char}_\Lambda\big(\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})/\Lambda\kappa_1^{\mathrm{Hg}}\big)$ in $\Lambda[1/p]$.

Remark 4.1.3. For our later use, we compare the class $\kappa_1^{\mathrm{Hg}}\in\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$ from Theorem 4.1.1 with the Λ-adic class constructed in [CH18, §5.2] (taking for f the newform associated with E).

Denote by α the p-adic unit root of x^2-a_px+p. With the notations introduced in the proof of Theorem 4.1.1, define the *α-stabilized Heegner point* $P[p^k]_\alpha\in E(K[p^k])\otimes\mathbb{Z}_p$ by

$$P[p^k]_\alpha := \begin{cases} P[p^k]-\alpha^{-1}P[p^{k-1}] & \text{if } k\geqslant 1,\\ u_K^{-1}\big(1-\alpha^{-1}\sigma_p\big)\big(1-\alpha^{-1}\sigma_p^*\big)P[1] & \text{if } k=0 \text{ and } p \text{ splits in } K,\\ u_K^{-1}\big(1-\alpha^{-2}\big)P[1] & \text{if } k=0 \text{ and } p \text{ is inert in } K.\end{cases} \tag{4.3}$$

Using the Heegner point norm relations, a straightforward calculation shows that the points $\alpha^{-k}P[p^k]_\alpha$ are norm-compatible. Letting $\delta : E(K_k)\otimes\mathbb{Z}_p\to\mathrm{H}^1(K_k,T_pE)$ be the Kummer map, we may therefore set

$$\kappa_\infty := \varprojlim_k \delta(\kappa_k) \in \varprojlim_k \mathrm{H}^1(K_k,T_pE)\simeq\mathrm{H}^1(K,\mathbf{T}),$$

where $\kappa_k=\alpha^{-d(k)}\mathrm{Norm}_{K[p^{d(k)}]/K_k}(P[p^{d(k)}]_\alpha)$. The inclusion $\kappa_\infty\in\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$ follows immediately from the construction. For the comparison with κ_1^{Hg}, note that by (4.2) the projection $\mathrm{pr}_K(\kappa_1^{\mathrm{Hg}})$ of κ_1^{Hg} to $\mathrm{H}^1(K,T_pE)$ is given by the Kummer image of $\mathrm{Norm}_{K[1]/K}(Q_0[1])$, while κ_0 is the Kummer image of $\mathrm{Norm}_{K[1]/K}(P[1]_\alpha)$. Thus comparing (4.1) and (4.3) we see that

$$\mathrm{pr}_K(\kappa_1^{\mathrm{Hg}}) = \begin{cases} u_K\alpha^2(\beta-1)^2\cdot\kappa_0 & \text{if } p \text{ splits in } K,\\ u_K\alpha^2(\beta^2-1)\cdot\kappa_0 & \text{if } p \text{ is inert in } K,\end{cases} \tag{4.4}$$

where $\beta=p\alpha^{-1}$. In particular, κ_∞ and κ_1^{Hg} generate the same Λ-submodule of $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$.

4.2. Proof of the Iwasawa main conjectures.

Let $\kappa_\infty\in\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$ be the Λ-adic Heegner class introduced in Remark 4.1.3, and put $\Lambda_{\mathrm{ac}}=\Lambda\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$. Let $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K,\mathbf{T})$ be defined just as $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K,M_E)$ but with $\mathbf{T}$ replacing M_E and the conditions on v and $\bar{v}$ switched.

Proposition 4.2.1. *Assume that $p=v\bar{v}$ splits in K and that $E(K)[p]=0$. Then the following statements are equivalent:*

(i) *Both $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$ and $\mathcal{X}=\mathrm{H}^1_{\mathcal{F}_\Lambda}(K,M_E)^\vee$ have Λ-rank one, and the divisibility*

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

holds in Λ_{ac}.

(ii) *Both $\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K,\mathbf{T})$ and $\mathfrak{X}_E=\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(K,M_E)^\vee$ are Λ-torsion, and the divisibility*

$$\mathrm{char}_\Lambda(\mathfrak{X}_E)\Lambda^{\mathrm{ur}}\supset(\mathcal{L}_E)$$

holds in $\Lambda^{\mathrm{ur}}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$.

Moreover, the same result holds for the opposite divisibilities.

Proof. See [BCK21, Thm. 5.2], whose proof still applies after inverting p. □

We can now conclude the proof of Theorem C in the introduction.

Theorem 4.2.2. *Suppose K satisfies hypotheses* (Heeg), (spl), (disc), *and* (Sel), *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 $\mathfrak{X}_E$ is Λ-torsion, and*

$$\mathrm{char}_\Lambda(\mathfrak{X}_E)\Lambda^{\mathrm{ur}} = (\mathcal{L}_E)$$

as ideals in Λ^{ur}.

Proof. By Theorem 4.1.2, the modules $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ and $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K, M_E)^\vee$ have both Λ-rank one, with

$$\mathrm{char}_\Lambda\big(\mathrm{H}^1_{\mathcal{F}_\Lambda}(K, M_E)^\vee_{\mathrm{tors}}\big) \supset \mathrm{char}_\Lambda\big(\mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})/\Lambda\kappa_1^{\mathrm{Hg}}\big)^2$$

as ideals in $\Lambda_{\mathrm{ac}} = \Lambda[1/p]$. Since by Remark 4.1.3 the classes κ_1^{Hg} and κ_∞ generate the same Λ-submodule of $\mathrm{H}^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$, by Proposition 4.2.1 it follows that $\mathfrak{X}_E$ is Λ-torsion, with

$$\mathrm{char}_\Lambda(\mathfrak{X}_E)\Lambda^{\mathrm{ur}} \supset (\mathcal{L}_E)$$

as ideals in $\Lambda_{\mathrm{ac}}\hat{\otimes}_{\mathbb{Z}_p}\mathbb{Z}_p^{\mathrm{ur}}$. This divisibility, together with the equalities $\mu(\mathfrak{X}_E) = \mu(\mathcal{L}_E) = 0$ and $\lambda(\mathfrak{X}_E) = \lambda(\mathcal{L}_E)$ in Theorem 2.2.3, yields the result. □

As a consequence, we can also deduce the first cases of Perrin-Riou's Heegner point main conjecture [PR87] in the residually reducible case. More precisely, together with Theorem 4.1.2, the following yields Corollary D in the introduction.

Corollary 4.2.3. *Suppose K satisfies hypotheses* (Heeg), (spl), (disc), *and* (Sel), *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 Λ-rank one, and*

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

as ideals in Λ_{ac}.

Proof. In light of Remark 4.1.3, this is the combination of Theorem 4.2.2 and Proposition 4.2.1. □

Remark 4.2.4. If the Heeger point $P_K = \mathrm{Norm}_{K[1]/K}(P[1]) \in E(K)$ is non-torsion, then (Sel) holds by the main results of [Kol88]. In particular, this is so if the image $\mathrm{pr}_K(\kappa_1^{\mathrm{Hg}})$ of κ_1^{Hg} (equivalently, the class κ_0) in $\mathrm{H}^1_{\mathcal{F}}(K, T_p(E))$ is non-zero (as $\mathrm{H}^1_{\mathcal{F}}(K, T_p(E))$ is non-torsion since $E(K)[p] = 0$).

5. Proof of Theorem E and Theorem F

5.1. **Preliminaries.** Here we collect the auxiliary results we shall use in the next sections to deduce Theorems E and F in the introduction from our main result, Theorem 4.2.2.

5.1.1. *Anticyclotomic control theorem.* Assume that $p = v\bar{v}$ splits in K, and as in [JSW17, §2.2.3], define the *anticyclotomic Selmer group* of $W = E[p^\infty]$ by

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{ac}}}(K, W) = \ker\bigg\{\mathrm{H}^1(K^\Sigma/K, W) \rightarrow \prod_{w \in \Sigma} \mathrm{H}^1(K_w, W) \times \frac{\mathrm{H}^1(K_v, W)}{\mathrm{H}^1(K_v, W)_{\mathrm{div}}} \times \mathrm{H}^1(K_{\bar{v}}, W)\bigg\},$$

where $\mathrm{H}^1(K_v, W)_{\mathrm{div}} \subset \mathrm{H}^1(K_v, W)$ denotes the maximal divisible submodule and $\Sigma = \{w : \ w | N\}$.

The following result is a special case of the "anticyclotomic control theorem" of [JSW17, §3].

Theorem 5.1.1. *Assume that*

- $E(\mathbb{Q}_p)[p] = 0$,
- $\mathrm{rank}_{\mathbb{Z}} E(K) = 1$,
- $\#Ш(E/K)[p^\infty] < \infty$.

Then $\mathfrak{X}_E$ is a torsion Λ-module, and letting $\mathcal{F}_E \in \Lambda$ be a generator of $\mathrm{char}_\Lambda(\mathfrak{X}_E)$, we have

$$\#\mathbb{Z}_p/\mathcal{F}_E(0) = \#Ш(E/K)[p^\infty] \cdot \left(\frac{\#(\mathbb{Z}_p/(\frac{1-a_p+p}{p}) \cdot \log_{\omega_E} P)}{[E(K) : \mathbb{Z} \cdot P]_p}\right)^2 \cdot \prod_{w|N} c_w(E/K)_p,$$

where

- *$P \in E(K)$ is any point of infinite order,*
- *$\log_{\omega_E} : E(K_v)_{/\mathrm{tors}} \to \mathbb{Z}_p$ is the formal group logarithm associated to a Néron differential ω_E,*
- *$[E(K) : \mathbb{Z} \cdot P]_p$ denotes the p-part of the index $[E(K) : \mathbb{Z} \cdot P]$,*
- *$c_w(E/K)_p$ is the p-part of the Tamagawa number of E/K_w.*

Proof. This follows from the combination of Theorem 3.3.1 and equation (3.5.d) in [JSW17, (3.5.d)], noting that the arguments in the proof of those results apply without change with the G_K-irreducibility of $E[p]$ assumed in *loc. cit.* replaced by the weaker hypothesis that $E(K)[p] = 0$, which is implied by the hypothesis $E(\mathbb{Q}_p)[p] = 0$ since p splits in K. □

5.1.2. *Gross–Zagier formulae.* Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and fix a parametrization

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

Let K be an imaginary quadratic field satisfying the Heegner hypothesis relative to N, and fix an integral ideal $\mathfrak{N} \subset \mathcal{O}_K$ with $\mathcal{O}_K/\mathfrak{N} = \mathbb{Z}/N\mathbb{Z}$. Let $x_1 = [\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathfrak{N}^{-1}] \in X_0(N)$ be the Heegner point of conductor 1 on $X_0(N)$, which is defined over the Hilbert class field $H = K[1]$ of K, and set

$$P_K = \sum_{\sigma \in \mathrm{Gal}(H/K)} \pi(x_1)^\sigma \in E(K).$$

Let $f \in S_2(\Gamma_0(N))$ be the newform associated with E, so that $L(f, s) = L(E, s)$, and consider the differential $\omega_f := 2\pi i f(\tau) d\tau$ on $X_0(N)$. Let also ω_E be a Néron differential on E, and let $c_E \in \mathbb{Z}$ be the associated *Manin constant*, so that $\pi^*(\omega_E) = c_E \cdot \omega_f$.

Theorem 5.1.2. *Under the above hypotheses, $L(E/K, 1) = 0$ and*

$$L'(E/K, 1) = u_K^{-2} c_E^{-2} \cdot \sqrt{|D_K|}^{-1} \cdot \|\omega_E\|^2 \cdot \hat{h}(P_K),$$

where $u_K = \#(\mathcal{O}_K^\times/\pm 1)$, $\hat{h}(P_K)$ is the canonical height of P_K, and $\|\omega_E\|^2 = \iint_{E(\mathbb{C})} |\omega_E \wedge \bar{\omega}_E|$.

Proof. This is [GZ86, Thm. V.2.1]. □

Theorem 5.1.3. *Under the above hypotheses, let $p > 2$ be a prime of good reduction for E such that $p = v\bar{v}$ splits in K. Then*

$$\mathcal{L}_E(0) = c_E^{-2} \cdot \left(1 - a_p p^{-1} + p^{-1}\right)^2 \cdot \log_{\omega_E}(P_K)^2.$$

where $\log_{\omega_E} : E(K_v) \to K_v$ is the formal group logarithm associated to ω_E.

Proof. Let $J_0(N)$ be the Picard variety of $X_0(N)$, and set $\Delta_1 = (x_1) - (\infty) \in J_0(N)(H)$. By [BDP13, Thm. 5.13] specialized to the case $k = 2$, $r = j = 0$, and $\chi = \mathbf{N}_K^{-1}$, we have

$$\mathcal{L}_E(0) = \left(1 - a_p p^{-1} + p^{-1}\right)^2 \cdot \left(\sum_{\sigma \in \mathrm{Gal}(H/K)} \log_{\omega_f}(\Delta_1^\sigma)\right)^2,$$

where $\log_{\omega_f} : J_0(N)(H_v) \to H_v$ is the formal group logarithm associated to ω_f. Since $\log_{\omega_f}(\Delta_1) = c_E^{-1} \cdot \log_{\omega_E}(\pi(\Delta_1))$, this yields the result. □

5.1.3. *A result of Greenberg–Vatsal.*

Theorem 5.1.4. *Let $A/\mathbb{Q}$ be an elliptic curve, and let $p > 2$ be a prime of good ordinary reduction for A. Assume that A admits a cyclic p-isogeny with kernel Φ_A, with the $G_\mathbb{Q}$-action on Φ_A given by a character which is either ramified at p and even, or unramified at p and odd. If $L(A, 1) \neq 0$ then*

$$\mathrm{ord}_p\left(\frac{L(A,1)}{\Omega_A}\right) = \mathrm{ord}_p\left(\frac{\#\text{Ш}(A/\mathbb{Q}) \cdot \mathrm{Tam}(A/\mathbb{Q})}{\#(A(\mathbb{Q})_{\mathrm{tors}})^2}\right),$$

where $\mathrm{Tam}(A/\mathbb{Q}) = \prod_\ell c_\ell(A/\mathbb{Q})$ is the product over the bad primes ℓ of A of the Tamagawa numbers of $A/\mathbb{Q}_\ell$.

Proof. By [Kol88], if $L(A, 1) \neq 0$ then $\mathrm{rank}_\mathbb{Z} A(\mathbb{Q}) = 0$ and $\#\text{Ш}(A/\mathbb{Q}) < \infty$; in particular, $\#\mathrm{Sel}_{p^\infty}(A/\mathbb{Q}) = \#\text{Ш}(A/\mathbb{Q})[p^\infty] < \infty$. Letting $\Lambda_{\mathrm{cyc}} = \mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]\!]$ be the cyclotomic Iwasawa algebra, by [Gre99, Thm. 4.1] we therefore have

$$\#\mathbb{Z}_p/\mathcal{F}_A(0) = \frac{\#\left(\mathbb{Z}_p/(1 - a_p(A) + p)^2 \cdot \#\text{Ш}(A/\mathbb{Q}) \cdot \mathrm{Tam}(A/\mathbb{Q})\right)}{\#\left(\mathbb{Z}_p/(A(\mathbb{Q})_{\mathrm{tors}})^2\right)}, \tag{5.1}$$

where $\mathcal{F}_A \in \Lambda_{\rm cyc}$ is a generator of the characteristic ideal of the dual Selmer group $Sel_{\mathbb{Q}_\infty}(T_pA, T_p^+A)^\vee$ in the notations of [SU14, §3.6.1]. Under the given assumptions, the cyclotomic main conjecture for A, i.e., the equality

$$(\mathcal{F}_A) = (\mathcal{L}_A) \subset \Lambda_{\rm cyc} \tag{5.2}$$

where $\mathcal{L}_A$ is the p-adic L-function of Mazur–Swinnerton-Dyer, follows from the combination of [Kat04, Thm. 12.5] and [GV00, Thm. 1.3]. By the interpolation property of $\mathcal{L}_A$,

$$\mathcal{L}_A(0) = \left(1-\alpha_p^{-1}\right)^2 \cdot \frac{L(A,1)}{\Omega_A}, \tag{5.3}$$

where $\alpha_p \in \mathbb{Z}_p^\times$ is the unit root of $x^2 - a_p(A)x + p$. Noting that ${\rm ord}_p(1-a_p(A)+p) = {\rm ord}_p(1-\alpha_p^{-1})$, the result thus follows from the combination of (5.1), (5.2), and (5.3). □

5.2. **Proof of the p-converse.** The next result is Theorem E in the introduction. Note that a result for $r=0$ can be obtained from the cyclotomic main conjecture proved by combining [GV00, Thm. 1.3] and Kato's divisibility in [Kat04]. However, our assumptions are less restrictive, since in [GV00] the character ϕ is assumed to be ramified at p and even or unramified at p and odd.

Theorem 5.2.1. *Assume that $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ with $\phi|_{G_p} \neq \mathbb{1}, \omega$. Let $r \in \{0,1\}$. Then*

$$\operatorname{corank}_{\mathbb{Z}_p}{\rm Sel}_{p^\infty}(E/\mathbb{Q}) = r \quad \Longrightarrow \quad {\rm ord}_{s=1}L(E,s) = r,$$

and so ${\rm rank}_{\mathbb{Z}}E(\mathbb{Q}) = r$ *and* $\#Ш(E/\mathbb{Q}) < \infty$.

Proof. The proof of this result is a consequence of Corollary 4.2.3 for suitable choices of a quadratic imaginary field K depending on $r \in \{0,1\}$.

First we suppose $\operatorname{corank}_{\mathbb{Z}_p}{\rm Sel}_{p^\infty}(E/\mathbb{Q}) = 1$. It follows from [Mon96, Theorem 1.5] that the root number $w(E/\mathbb{Q}) = -1$. Choose an imaginary quadratic field K of discriminant D_K such that

(a) $D_K < -4$ is odd,
(b) every prime ℓ dividing N splits in K,
(c) p splits in K, say $p = v\bar{v}$,
(d) $L(E^K,1) \neq 0$.

The existence of such K (in fact, of an infinitude of them) is ensured by [FH95, Thm. B.1], since (a), (b), and (c) impose only a finite number of congruence conditions on D_K, and any K satisfying (b) is such that E/K has root number $w(E/K) = w(E/\mathbb{Q})w(E^K/\mathbb{Q}) = -1$, and therefore $w(E^K/\mathbb{Q}) = +1$. By work of Kolyvagin [Kol88] (or alternatively, Kato [Kat04]), the non-vanishing of $L(E^K,1)$ implies that ${\rm Sel}_{p^\infty}(E^K/\mathbb{Q})$ is finite and therefore

$$\operatorname{corank}_{\mathbb{Z}_p}{\rm Sel}_{p^\infty}(E/K) = 1,$$

and hence E satisfies (Sel). In particular, all the hypotheses of Corollary 4.2.3 hold. As in the proof of Corollary 3.4.2, the condition that $\operatorname{corank}_{\mathbb{Z}_p}{\rm Sel}_{p^\infty}(E/K) = 1$ easily implies that ${\rm ord}_{\mathfrak{P}_0}(X_{\rm tors}) = 0$, and so it then follows from Corollary 4.2.3 that the image of κ_1 in ${\rm H}^1(K, T_pE)$ is non-zero. This implies that the Heegner point $P_K \in E(K)$ is non-torsion and hence, by the Gross–Zagier formula that ${\rm ord}_{s=1}L(E/K,s) = 1$. Since $L(E/K,s) = L(E,s)L(E^K,s)$ and ${\rm ord}_{s=1}L(E^K,s) = 0$ by the choice of K, it follows that ${\rm ord}_{s=1}L(E,s) = 1$.

We now assume $\operatorname{corank}_{\mathbb{Z}_p}{\rm Sel}_{p^\infty}(E/\mathbb{Q}) = 0$. The result of Monsky used above implies in this case that $w(E/\mathbb{Q}) = +1$. We now choose an imaginary quadratic field K satisfying the same conditions (a), (b), (c) as above, in addition to the condition

(d') ${\rm ord}_{s=1}L(E^K,1) = 1$.

The existence of infinitely many such K follows from [FH95, Thm. B.2], since any K satisfying (b) is such that $w(E^K/\mathbb{Q}) = -1$. The Gross–Zagier–Kolyvagin theorem implies that $\operatorname{corank}_{\mathbb{Z}_p}{\rm Sel}_{p^\infty}(E^K/\mathbb{Q}) = 1$ and therefore

$$\operatorname{corank}_{\mathbb{Z}_p}{\rm Sel}_{p^\infty}(E/K) = 1.$$

Thus, as above, E satisfies (Sel), and we can apply Corollary 4.2.3 and the Gross–Zagier formula to obtain ${\rm ord}_{s=1}L(E/K,s) = 1$, which implies by our choice of K that $L(E,1) \neq 0$. □

Since the hypotheses of Theorem 5.2.1 imply $E(\mathbb{Q})[p] = 0$, we see that ${\rm Sel}_{p^\infty}(E/\mathbb{Q})[p] = {\rm Sel}_p(E/\mathbb{Q})$, whence the following mod p version of the theorem.

Corollary 5.2.2. *Suppose E is as in Theorem 5.2.1 and $r \in \{0,1\}$. Then*

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/\mathbb{Q}) = r \quad \Longrightarrow \quad \mathrm{ord}_{s=1}L(E,s) = r,$$

and so $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}) = r$ *and* $\#\text{Ш}(E/\mathbb{Q}) < \infty$.

For $p = 3$, Corollary 5.2.2 together with the work of Bhargava–Klagsbrun–Lemke Oliver–Shnidman [BKLOS19] on the average 3-Selmer rank in quadratic twist families, leads to the following result in the direction of Goldfeld's conjecture [Gol79].

Corollary 5.2.3. *Let E be an elliptic curve over $\mathbb{Q}$ with a rational 3-isogeny. Then a positive proportion of quadratic twists of E have algebraic and analytic rank equal to 1 and a positive proportion of quadratic twists of E have algebraic and analytic rank equal to 0.*

Proof. Denote by $\phi : G_{\mathbb{Q}} \to \mathbb{F}_3^\times = \mu_2$ the character giving the Galois action on the kernel of a rational 3-isogeny of E. As the condition $\phi|_{G_p} \neq \mathbb{1}, \omega$ can be arranged by a quadratic twist, combining [BKLOS19, Thm. 2.6] and Corollary 5.2.2, the result follows. □

Remark 5.2.4. The qualitative result of Corollary 5.2.3 was first obtained by Kriz–Li (see [KL19, Thm. 1.5]), but thanks to [BKLOS19] (see esp. [*op. cit.*, p. 2957]) our result can lead to better lower bounds on the proportion of rank 1 twists. In particular the proportions provided by [BKLOS19, Thm. 2.5] are the largest when the parity of the logarithmic Selmer ratios is equidistributed in quadratic families. The elliptic curve of smallest conductor over $\mathbb{Q}$ for which this happens is the elliptic curve having Cremona label $19a3$ given by the affine equation $y^2 + y = x^3 + x^2 + x$. The explicit bounds of [BKLOS19] and our result give that at least 41.6% of its quadratic twists have analytic and algebraic rank equal to 1 and at least 25% have analytic and algebraic rank equal to 0.

5.3. **Proof of the p-part of BSD formula.**

The following is Theorem F in the introduction.

Theorem 5.3.1. *Let $E/\mathbb{Q}$ be an elliptic curve, and let $p > 2$ be a prime of good ordinary reduction for E. Assume that E admits a cyclic p-isogeny with kernel $C = \mathbb{F}_p(\phi)$, with $\phi : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ such that*

- *$\phi|_{G_p} \neq \mathbb{1}, \omega$,*
- *ϕ is either ramified at p and odd, or unramified at p and even.*

If $\mathrm{ord}_{s=1}L(E,s) = 1$, *then*

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

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

Proof. Suppose $\mathrm{ord}_{s=1}L(E,s) = 1$ and choose, as in the proof of Theorem 5.2.1, an imaginary quadratic field K of discriminant D_K such that

(a) $D_K < -4$ is odd,
(b) every prime ℓ dividing N splits in K,
(c) p splits in K, say $p = v\bar{v}$,
(d) $L(E^K, 1) \neq 0$.

Then $\mathrm{ord}_{s=1}L(E/K,s) = 1$, which by Theorem 5.1.2 implies that the Heegner point $P_K \in E(K)$ has infinite order, and therefore $\mathrm{rank}_{\mathbb{Z}}E(K) = 1$ and $\#\text{Ш}(E/K) < \infty$ by [Kol88]. In particular, (Sel) holds, and so all the hypotheses of Theorem 4.2.2 are satisfied. Thus there is a p-adic unit $u \in (\mathbb{Z}_p^{\mathrm{ur}})^\times$ for which

$$\mathcal{F}_E(0) = u \cdot \mathcal{L}_E(0), \tag{5.4}$$

where $\mathcal{F}_E \in \Lambda$ is a generator of $\mathrm{char}_\Lambda(\mathfrak{X}_E)$. The hypotheses on ϕ imply that $E(K)[p] = 0$, and so Theorem 5.1.1 applies with $P = P_K$, which combined with Theorem 5.1.3 and the relations (4.4) and (5.4) yields the equality

$$\mathrm{ord}_p\big(\#\text{Ш}(E/K)\big) = 2\,\mathrm{ord}_p\big(c_E^{-1}u_K^{-1} \cdot [E(K) : \mathbb{Z}.P_K]\big) - \sum_{w \in S} \mathrm{ord}_p\big(c_w(E/K)\big), \tag{5.5}$$

On the other hand, the Gross–Zagier formula of Theorem 5.1.2 can be rewritten (see [GZ86, p. 312]) as

$$L'(E/K,1) = 2^t c_E^{-2} u_K^{-2} \cdot \hat{h}(P_K) \cdot \Omega_E \cdot \Omega_{E^K},$$

where the power of 2 is given by the number of connected components $[E(\mathbb{R}) : E(\mathbb{R})^0]$. This, together with the relations $L(E/K,s) = L(E,s) \cdot L(E^K,s)$ and

$$\hat{h}(P_K) = [E(K) : \mathbb{Z} \cdot P_K]^2 \cdot \mathrm{Reg}(E/K) = [E(K) : \mathbb{Z} \cdot P_K]^2 \cdot \mathrm{Reg}(E/\mathbb{Q}),$$

using that $\mathrm{rank}_{\mathbb{Z}} E^K(\mathbb{Q}) = 0$ for the last equality, amounts to the formula

$$\frac{L'(E,1)}{\mathrm{Reg}(E/\mathbb{Q}) \cdot \Omega_E} \cdot \frac{L(E^K,1)}{\Omega_{E^K}} = 2^t c_E^{-2} u_K^{-2} \cdot [E(K) : \mathbb{Z} \cdot P_K]^2. \tag{5.6}$$

Note that $u_K = 1$, since $D_K < -4$. Since $Ш(E/K)[p^\infty] \simeq Ш(E/\mathbb{Q})[p^\infty] \oplus Ш(E^K/\mathbb{Q})[p^\infty]$ as p is odd, and

$$\sum_{w|\ell} \mathrm{ord}_p(c_w(E/K)) = \mathrm{ord}_p(c_\ell(E/\mathbb{Q})) + \mathrm{ord}_p(c_\ell(E^K/\mathbb{Q}))$$

for any prime ℓ (see [SZ14, Cor. 9.2]), combining (5.5) and (5.6) we arrive at

$$\begin{aligned} &\mathrm{ord}_p\left(\frac{L'(E,1)}{\mathrm{Reg}(E/\mathbb{Q}) \cdot \Omega_E \cdot \prod_\ell c_\ell(E/\mathbb{Q})}\right) - \mathrm{ord}_p(\#Ш(E/\mathbb{Q})) \\ &\qquad = \mathrm{ord}_p\left(\frac{L(E^K,1)}{\Omega_{E^K} \cdot \prod_\ell c_\ell(E^K/\mathbb{Q})}\right) - \mathrm{ord}_p\big(\#Ш(E^K/\mathbb{Q})\big). \end{aligned} \tag{5.7}$$

Finally, by our hypotheses on ϕ the curve E^K satisfies the hypotheses of Theorem 5.1.4, and hence the right-hand side of (5.7) vanishes, concluding the proof of Theorem 5.3.1. □

References

[BBV16] Andrea Berti, Massimo Bertolini, and Rodolfo Venerucci. Congruences between modular forms and the Birch and Swinnerton-Dyer conjecture. In *Elliptic curves, modular forms and Iwasawa theory*, volume 188 of *Springer Proc. Math. Stat.*, pages 1–31. Springer, Cham, 2016.

[BCK21] A. Burungale, F. Castella, and C.-H. Kim. A proof of Perrin-Riou's Heegner point main conjecture. *Algebra Number Theory, to appear*, 2021. arXiv:1908.09512.

[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.

[Ber95] Massimo Bertolini. Selmer groups and Heegner points in anticyclotomic $\mathbf{Z}_p$-extensions. *Compositio Math.*, 99(2):153–182, 1995.

[BKLOS19] Manjul Bhargava, Zev Klagsbrun, Robert J. Lemke Oliver, and Ari Shnidman. 3-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field. *Duke Math. J.*, 168(15):2951–2989, 2019.

[BPS18] Kâzim Büyükboduk, Robert Pollack, and Shu Sasaki. p-adic Gross-Zagier formula at critical slope and a conjecture of Perrin-Riou. 2018. preprint, arXiv:1811.08216.

[Bra11] Miljan Brakočević. Anticyclotomic p-adic L-function of central critical Rankin-Selberg L-value. *Int. Math. Res. Not. IMRN*, (21):4967–5018, 2011.

[BT20] Ashay A. Burungale and Ye Tian. p-converse to a theorem of Gross–Zagier, Kolyvagin and Rubin. *Invent. Math.*, 220(1):211–253, 2020.

[Cas13] Francesc Castella. *On the p-adic variation of Heegner points*. 2013. Thesis (Ph.D.)–McGill University.

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

[Cas18] Francesc Castella. On the p-part of the Birch-Swinnerton-Dyer formula for multiplicative primes. *Camb. J. Math.*, 6(1):1–23, 2018.

[CCL18] Li Cai, Yihua Chen, and Yu Liu. Heegner points on modular curves. *Trans. Amer. Math. Soc.*, 370(5):3721–3743, 2018.

[CG96] J. Coates and R. Greenberg. Kummer theory for abelian varieties over local fields. *Invent. Math.*, 124(1-3):129–174, 1996.

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

[CLTZ15] John Coates, Yongxiong Li, Ye Tian, and Shuai Zhai. Quadratic twists of elliptic curves. *Proc. Lond. Math. Soc. (3)*, 110(2):357–394, 2015.

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

[Edi92] Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594, 1992.

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

[Gol79] Dorian Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, volume 751 of *Lecture Notes in Math.*, pages 108–118. Springer, Berlin, 1979.

[Gre77] Ralph Greenberg. On p-adic L-functions and cyclotomic fields. II. *Nagoya Math. J.*, 67:139–158, 1977.

[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.

[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.

[Hid93] Haruzo Hida. *Elementary theory of L-functions and Eisenstein series*, volume 26 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1993.

[Hid10] H. Hida. The Iwasawa μ-invariant of p-adic Hecke L-functions. *Ann. of Math. (2)*, 172(1):41–137, 2010.

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

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

[How05] Benjamin Howard. The Iwasawa theoretic Gross-Zagier theorem. *Compos. Math.*, 141(4):811–846, 2005.

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

[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.

[KL19] Daniel Kriz and Chao Li. Goldfeld's conjecture and congruences between Heegner points. *Forum Math. Sigma*, 7:e15, 80, 2019.

[Kol88] Victor Kolyvagin. The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves (Russian). *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 52(6):1154–1180, 1327, 1988. translation in Mathematics of the USSR-Izvestiya **33** (1989), no. 3, 473–499.

[Kri16] Daniel Kriz. Generalized Heegner cycles at Eisenstein primes and the Katz p-adic L-*function*. *Algebra Number Theory*, 10(2):309–374, 2016.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

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

[Mon96] P. Monsky. Generalizing the Birch-Stephens theorem. I. Modular curves. *Math. Z.*, 221(3):415–420, 1996.

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

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

[PR87] Bernadette Perrin-Riou. Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner. *Bull. Soc. Math. France*, 115(4):399–456, 1987.

[PW11] Robert Pollack and Tom Weston. On anticyclotomic μ-invariants of modular forms. *Compos. Math.*, 147(5):1353–1381, 2011.

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

[Ski20] Christopher Skinner. A converse to a theorem of Gross, Zagier, and Kolyvagin. *Ann. of Math. (2)*, 191(2):329–354, 2020.

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

[SZ14] Christopher Skinner and Wei Zhang. Indivisibility of Heegner points in the multiplicative case. 2014. preprint, arXiv:1407.1099.

[Tia14] Ye Tian. Congruent numbers and Heegner points. *Camb. J. Math.*, 2(1):117–161, 2014.

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

[Ven16] Rodolfo Venerucci. On the p-converse of the Kolyvagin-Gross-Zagier theorem. *Comment. Math. Helv.*, 91(3):397–444, 2016.

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

[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) Institut Galilée, Université Sorbonne Paris Nord, 93430 Villetaneuse, FRANCE
Email address: grossi@math.univ-paris13.fr

(J. Lee) KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea
Email address: jaehoon.lee900907@gmail.com

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