ON THE 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 $p$ a 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 following the method of Greenberg–Vatsal [GV00]. As a result of our study, we obtain a proof under mild hypotheses of Perrin-Riou’s Heegner point main conjecture, as well as 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 1
1. Algebraic side 5
1.1. Local cohomology groups of characters 5
1.2. Selmer groups of characters 6
1.3. Local cohomology groups of $E$ 9
1.4. Selmer groups of $E$ 9
1.5. Comparison I: Algebraic Iwasawa invariants 11
2. Analytic side 11
2.1. $p$-adic $L$-functions 11
2.2. Comparison II: Analytic Iwasawa invariants 12
3. A Kolyvagin system argument 14
3.1. Selmer groups and Kolyvagin systems 14
3.2. Bounding Selmer groups I 15
3.3. Bounding Selmer groups II 18
3.4. Iwasawa theory 20
4. Proof of Theorem C and Corollary D 21
4.1. Preliminaries 21
4.2. Proof of the Iwasawa main conjectures 22
5. Proof of Theorem E and Theorem F 23
5.1. Preliminaries 23
5.2. Proof of the $p$-converse 26
5.3. Proof of the $p$-part of BSD formula 26
References 27

Introduction

0.1. Statement of the main results. Let $E/\mathbb{Q}$ be an elliptic curve, and $p$ a prime of good reduction for $E$. We say that $p$ is an Eisenstein prime (for $E$) if the $G_{\mathbb{Q}}$-module $E[p]$ is reducible, where $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is the absolute Galois group of $\mathbb{Q}$. 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 $p \in \{3, 5, 7, 13, 37\}$. In this paper, we study the anticyclotomic Iwasawa theory of $E$ at Eisenstein primes $p$ over an imaginary quadratic field in which $p$ splits. We restrict to the

Date: May 3, 2020.
elliptic curve case largely for simplicity, and it should be noted that our methods apply more generally to the case of elliptic modular forms.

Thus let \( p \) be an Eisenstein prime for \( E \), and let \( K \) be an imaginary quadratic field such that

\[
p = vu \text{ splits in } K.
\]

Denoting by \( N \) the conductor of \( E \), assume also that \( K \) satisfies the following Heegner hypothesis:

(Heeg)

every prime \( \ell | N \) splits in \( K \).

Let \( \Gamma = \text{Gal}(K_{\infty}/K) \) be the Galois group of the anticyclotomic \( \mathbb{Z}_\wp \)-extension of \( K \), and set

\[
\Lambda := \mathbb{Z}_p[[\Gamma]], \quad \Lambda^{ur} := \Lambda \hat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p^{ur},
\]

where \( \mathbb{Z}_p^{ur} \) denotes the completion of the ring of integers of the maximal unramified extension of \( \mathbb{Q}_p \). Under these hypotheses, the anticyclotomic Iwasawa main conjecture for \( E \) can be formulated in two different guises.

To recall the formulations, fix a modular parametrization

\[
Z
\]

where

\[
N
\]

and for any \( \pi \), the Kummer images of Heegner points on \( X_0(N) \) over the ring class of \( K \) of \( p \)-power conductor give rise of a class \( \kappa_1^{\text{Hg}} \in S \), where

\[
S := \varprojlim_n \varinjlim_m \text{Sel}_{p^m}(E/K_n),
\]

which is known to be not \( \Lambda \)-torsion by Cornut–Vatsal. Let \( X \), the Pontryagin dual of \( \text{Sel}_{\infty}(E/K_{\infty}) \).

The first formulation of the anticyclotomic main conjecture for \( E \) was given by Perrin-Riou [PR87]. Let \( f \in S_2(\Gamma_0(N)) \) be the newform associated to \( E \), so that \( L(f, s) = L(E, s) \), and let \( c_E \in \mathbb{Z} \) be such that

\[
\pi^*(\omega_E) = c_E \cdot 2\pi i f(\tau) \frac{d\tau}{\tau}, \text{ for } \omega_E \text{ a Néron differential on } E.
\]

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

\[
\text{char}_\Lambda(X_{\text{tors}}) = \frac{1}{c_E^2 u_K} \cdot \text{char}_\Lambda(S/\Lambda^{\text{Hg}}_1)^2,
\]

where \( X_{\text{tors}} \) denote the \( \Lambda \)-torsion submodule of \( X \), and \( u_K = \#(\mathcal{O}_K^\times)/2 \).

Note that Conjecture A allows \( p \) to be inert or ramified in \( K \). On the other hand, if both (Heeg) and (spl) hold, and also

\[
(\text{disc}) \quad \text{the discriminant } D_K \text{ of } K \text{ is odd and } D_K \neq -3,
\]

following the work of Bertolini–Darmon–Prasanna [BDP13], there is a \( p \)-adic \( L \)-function \( L_E \in \Lambda^{ur} \) defined by the interpolation of central critical values of \( f/K \) twisted by certain characters of \( \Gamma \). Let \( \mathfrak{X}_E \) be the Pontryagin dual of the Selmer group obtained from \( \text{Sel}_{\infty}(E/K_{\infty}) \subset \text{H}^1(K_{\infty}, E[p^\infty]) \) by relaxing (resp. imposing triviality) at the places above \( v \) (resp. \( \bar{v} \)), where \( v \) is the prime of \( K \) above \( p \) induced by a fixed embedding \( \overline{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}_p^\times \). A second formulation of the anticyclotomic Iwasawa main conjectures for \( E \) then arises as a special case of the Greenberg’s main conjectures [Gre94].

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

\[
\text{char}_\Lambda(\mathfrak{X}_E) \Lambda^{ur} = (L_E)
\]

as ideals in \( \Lambda^{ur} \).

To state our main results on Conjectures A and B for Eisenstein primes \( p \), write

\[
E[p]^{ss} = E_p(\phi) \oplus E_p(\psi),
\]

where \( \phi, \psi : G_\mathbb{Q} \rightarrow \mathbb{F}_p^\times \) are character. It follows from the Weil pairing that \( \psi = \omega \phi^{-1} \), where \( \omega \) is the Teichmüller character. Let \( G_p \subset G_\mathbb{Q} \) be a decomposition group at \( p \).

**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), and (disc). Assume in addition that
under the same hypotheses the implication
\( p \) or unramified at \( F \)
In other words, Conjecture A holds.

**Corollary D.** Under the hypotheses of Theorem C, both \( S \) and \( X \) have \( \Lambda \)-rank one, and
\[
\text{char}_\Lambda(X_{\text{tors}}) = \frac{1}{c_E^2 \mu^2_K} \cdot \text{char}_\Lambda(S/\Lambda \kappa_{E_1}^H)^2.
\]
In other words, Conjecture A holds.

With a judicious choice of \( K, \) Theorem C also has applications to the arithmetic over \( \mathbb{Q} \) of rational elliptic curves. Specifically, for Eisenstein primes \( p, \) we obtain converse to the celebrated theorem
\[
(0.1) \quad \text{ord}_{s=1} L(E, s) = 1 \implies \text{rank}_\mathbb{Z} E(\mathbb{Q}) = 1 \text{ and } \# \mathbb{III}(E/\mathbb{Q})[p^\infty] < \infty,
\]
of Gross–Zagier and Kolyvagin, as well as Theorem F below on the \( p \)-part of the Birch–Swinnerton-Dyer formula for \( E \) in the case of analytic rank 1. Note that Eisenstein primes \( p \) eluded the methods of [Ski19,Zha14,JSW17], where it is assumed that \( E[p] \) is absolutely irreducible.

**Theorem F.** 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 \( \phi|_{G_{K_p}} \neq 1, \omega. \) Then the following implication holds:
\[
\text{rank}_\mathbb{Z} E(\mathbb{Q}) = 1 \quad \# \mathbb{III}(E/\mathbb{Q})[p^\infty] < \infty \quad \implies \quad \text{ord}_{s=1} L(E, s) = 1.
\]

In fact, similarly as in [Wan14], in Corollary 5.2.2 below we prove a stronger version of Theorem E, showing under the same hypotheses the implication
\[
\text{corank}_\mathbb{Z} \text{Sel}_{p^{ss}}(E/\mathbb{Q}) = 1 \implies \text{ord}_{s=1} L(E, s) = 1,
\]
and deducing the finiteness of \( \# \mathbb{III}(E/\mathbb{Q}) \) as a consequence of (0.1). Another application of Theorem C is the following.

**Theorem F.** Under the hypotheses of Theorem E, assume in addition that \( \phi \) is either ramified at \( p \) and odd, or unramified at \( p \) and even. If \( \text{ord}_{s=1} L(E, s) = 1, \) then
\[
\text{ord}_p \left( \frac{L'(E, 1)}{\text{Reg}(E/\mathbb{Q}) \cdot \Omega_E} \right) = \text{ord}_p \left( \# \mathbb{III}(E/\mathbb{Q}) \prod_\ell \zeta_{\ell}(E/\mathbb{Q}) \right),
\]
where
- \( \text{Reg}(E/\mathbb{Q}) \) is the regulator of \( E(\mathbb{Q}), \)
- \( \Omega_E = \int_{E(\mathbb{R})} |\omega_E| \) is the Néron period associated to the Néron differential \( \omega_E, \)
- \( c_\ell(E) \) is the Tamagawa number of \( E \) at the prime \( \ell. \)

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

### 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. The starting point here 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 \( \Sigma \) any finite set of non-archimedean primes of \( K \) not containing any of the primes above \( p, \) this translates into the expectation that the Selmer group \( \zeta(E_{\Sigma}) \) at the primes \( w \in \Sigma, \) is \( \Lambda \)-torsion with
\[
(0.2) \quad \text{char}_\Lambda(X_{\Sigma}^E)^{\Lambda^w} = (L_{E_1}^\Sigma)
\]
as ideals in \( \Lambda^w, \) where \( L_{E_1}^\Sigma := L_E \cdot \prod_{w \in \Sigma} \mathbb{P}_w(E) \) for certain elements in \( \mathbb{P}_w(E) \in \Lambda \) interpolating (for varying characters of \( \Gamma \)) the Euler factor of \( L(E/K, s) \) at \( w \) evaluated \( s = 1. \)

A key advantage of the imprimitive main conjecture (0.2) is that (unlike the original conjecture), for suitable choices of \( \Sigma, \) its associated Iwasawa invariants are well-behaved with respect to congruences mod \( p. \) Identifying
Λ with the power series ring \( \mathbb{Z}_p[[T]] \) 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 \( u \in \Lambda^\times \), \( \mu = \mu(g) \in \mathbb{Z}_{\geq 0} \), and \( Q(T) \in \mathbb{Z}_p[T] \) a distinguished polynomial of degree \( \lambda(g) \). The constants \( \lambda \) and \( \mu \) are the so-called Iwasawa invariants of \( g \). For a torsion \( \Lambda \)-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 \( \mathcal{L} \in \Lambda^ur \) we let \( \lambda(\mathcal{L}) \) and \( \mu(\mathcal{L}) \) be the Iwasawa invariants of any element of \( \Lambda \) generating the same \( \Lambda^ur \)-ideal as \( \mathcal{L} \). With these conventions, in §1 we deduce from the \( G_\mathbb{Q} \)-module isomorphism \( E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi) \) that, taking \( \Sigma \) 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 \( \Lambda \)-torsion with

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

where \( \mathfrak{X}_E^\Sigma \) and \( \mathfrak{X}_E^\psi \) are anticyclotomic Selmer groups for the Teichmüller lifts of \( \phi \) and \( \psi \), respectively. The proof of (0.3) uses Rubin’s work [Rub91] on the Iwasawa main conjecture for imaginary quadratic fields and Hida’s work [Hid10] on the vanishing of the \( \mu \)-invariant of \( p \)-adic Hecke \( L \)-functions.

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

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

where \( \mathcal{L}_E^\Sigma \) and \( \mathcal{L}_E^\psi \) are \( \Sigma \)-imprimitive anticyclotomic Katz \( p \)-adic \( L \)-functions attached to \( \phi \) and \( \psi \).

With equalities (0.3) and (0.4) in hand, it follows easily that to prove the equality of characteristic ideals in Conjecture B it suffices to prove one of the predicted divisibilities. In §3, by an extension of Howard’s Kolvyagin system arguments [How04a] to the residually reducible setting, we prove one of the divisibilities in Conjecture A, which by the aforementioned connection with Conjecture B yields a corresponding divisibility in (0.2), and therefore the proof of Theorem C. The details of the final argument, and the deduction of Corollary D, are given in §4.

Finally, the proofs of Theorem E and Theorem F are given in §5, and they are both obtained as an application of Theorem C for a suitable chosen of \( K \). In particular, for the proof of the latter we need to know the \( p \)-part of the Birch–Swinnerton-Dyer formula for the quadratic twist \( E^K \) in analytic rank 0; this is deduced in Theorem 5.1.6 from the results of Greenberg–Vatsal [GV00], and is responsible for the additional hypotheses on \( \phi \) 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 \( J[5]^{ss} = \mathbb{Z}/5\mathbb{Z} \oplus \mu_5 \) as \( G_\mathbb{Q} \)-modules ( \( J \) has a rational 5-torsion point). If \( \psi \) is an even quadratic character such that \( \psi(5) = -1 \), corresponding to a real quadratic field \( \mathbb{Q}(\sqrt{5}) \) in which 5 is inert, then the twist \( E = J_5 \) of \( J \) by \( \psi \) satisfies the hypotheses of Theorem E with \( p = 5 \). Since the root of 5 is \(-1 \) (begin of analytic rank one), by [FH95, Thm. B.2] we can find infinitely many \( \psi \) as above for which the associated twist \( E = J_5 \) 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 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).

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, which combined with Kato’s divisibility [Kat04] 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. The ensuing applications to the \( p \)-converse of the Gross–Zagier–Kolyvagin theorem and to the \( p \)-part of the Birch–Swinnerton-Dyer formula in analytic rank 1 covers primes \( p \) that were either left untouched by the recent works in these directions [Ski19,Ven16,BBV16,Zha14,SZ14,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).
0.5. **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. During the preparation of this paper, F.C. was partially supported by the NSF grant DMS-1946136.

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 $E[p]^{new} = \mathbb{F}_p(\phi) \oplus \mathbb{F}(\psi)$ to the anticyclotomic Iwasawa invariants of the characters $\phi$ and $\psi$.

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

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

1.1. **Local cohomology groups of characters.** Let

$$\theta : G_K \rightarrow \mathbb{F}_p^\times$$

be a character whose conductor is only divisible by primes which are split in $K$. Via the Teichmüller lift $\mathbb{F}_p^\times \hookrightarrow \mathbb{Z}_p^\times$, we shall also view $\theta$ as taking values in $\mathbb{Z}_p^\times$. Set

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

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

In this section, we study the local cohomology of $M_\theta$ 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 $K$, let $I_w \subset \Gamma_w \subset \Gamma$ denote the corresponding inertia and decomposition groups. Let $\gamma_w \in \Gamma_w$ be a Frobenius element at $w$, and set

$$(1.1) \quad P_w(\theta) = P_w(\ell^{-1}\gamma_w) \in \Lambda,$$

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

**Lemma 1.1.1.** Let $w \nmid p$ be a prime split in $K$. Then the module $H^1(K_w, M_{\theta})^\vee$ is $\Lambda$-torsion with

$$\text{char}_\Lambda(H^1(K_w, M_{\theta})^\vee) = (P_w(\theta)).$$

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

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

1.1.2. $w \mid p$ split in $K$. 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 $\Lambda$-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 $\Lambda$-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

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

Thus $K/TK = 0$, and so $K = 0$ by Nakayama’s lemma. \qed

Let $w$ be the prime of $K$ above $p$, and denote by $I_w \subset G_w \subset G_K$ the inertia and decomposition groups of $w$.

**Proposition 1.1.3.** Let $w$ be a prime of $K$ above $p$, and assume that $\theta|_{G_w} \neq 1, \omega$. Then:
(i) The restriction map \( r_w : H^1(K_w, M_\theta) \to H^1(I_w, M_\theta)^{G_w/I_w} \) is an isomorphism.

(ii) \( H^1(K_w, M_\theta) \) is \( \Lambda \)-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, \( \ker(r_w) \cong M_\theta^I/(\text{Frob}_w - 1)M_\theta^I \), where \( \text{Frob}_w \) is a Frobenius element at \( w \). Taking Pontryagin duals to the exact sequence

\[
0 \to M_\theta^G \to M_\theta^I \xrightarrow{\text{Frob}_w - 1} M_\theta^I/(\text{Frob}_w - 1)M_\theta^I \to 0
\]

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

\[
(M_\theta^I)^w \to (M_\theta^I)^w,
\]

hence an isomorphism (by the Noetherian property of \( \Lambda \)); since the kernel of (1.2) is isomorphic to \( \ker(r_w)^V \), the proof of (i) follows.

For (ii), in light of Lemma 1.1.2, letting

\[
X := H^1(K_w, M_\theta)^V,
\]

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

\[
\frac{H^1(K_w, M_\theta)}{TH^1(K_w, M_\theta)} = 0, \quad H^1(K_w, \mathbb{Q}_p/\mathbb{Z}_p(\theta)) \cong H^1(K_w, M_\theta)[T],
\]

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

\[
\frac{H^1(K_w, \mathbb{Q}_p/\mathbb{Z}_p(\theta))}{pH^1(K_w, \mathbb{Q}_p/\mathbb{Z}_p(\theta))} \cong H^2(K_w, \mathbb{F}_p(\theta)) = 0,
\]

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

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 only divisible by primes split in \( K \).

Let \( \Sigma \) be a finite set of places of \( K \) containing \( \infty \) and the primes dividing \( p \) or the conductor of \( \theta \). We choose \( \Sigma \) so that every finite place in \( \Sigma \) is split in \( K \), and denote by \( K^\Sigma \) the maximal extension of \( K \) unramified outside \( \Sigma \).

**Definition 1.2.1.** The Selmer group of \( \theta \) is

\[
H^1_{\Sigma \Sigma}(K, M_\theta) := \ker\left\{ H^1(K^\Sigma/K, M_\theta) \to \prod_{w \in \Sigma, w \mid p} H^1(K_w, M_\theta) \times H^1(K_{\bar{w}}, M_\theta) \right\},
\]

and letting \( S = \Sigma \setminus \{ v, \bar{v}, \infty \} \), we define the \( S \)-imprimitive Selmer group of \( \theta \) by

\[
H^1_{\Sigma \Sigma}(K, M_\theta) := \ker\left\{ H^1(K^\Sigma/K, M_\theta) \to H^1(K_{\bar{v}}, M_\theta) \right\}.
\]

Replacing \( M_\theta \) by \( M_\theta[p] \) in the above definitions, we obtain the residual Selmer group \( H^1_{\Sigma \Sigma}(K, M_\theta[p]) \) and its \( S \)-imprimitive variant \( H^1_{\Sigma \Sigma}(K, M_\theta[p]) \).

It is well-known that the above Selmer groups are cofinitely over the corresponding Iwasawa algebra (\( \Lambda \) and \( \Lambda/p \)), and that they are independent of the choice of the set \( \Sigma \) as above.

Our definition of these Selmer groups is slightly different than those considered [GV00] (where the unramified, rather than strict, local condition is imposed), and is more convenient for our applications. Nonetheless, as we exploit in the next result, one can show that both definitions give rise to the same Selmer groups under mild hypotheses on \( \theta \) by building on the local results in the preceding section.
The following result combining work of Rubin and Hida will play a key role in the proof of our results.

**Theorem 1.2.2** (Rubin, Hida). Assume that \( \theta | G_\theta \neq 1, \omega \). Then \( H^1_{\text{Gr}}(K, M_\theta)^\vee \) is a torsion \( \Lambda \)-module with \( \mu \)-invariant zero.

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

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

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

\[
(1.4) \quad H^1(K^{\Sigma}/K_\theta, M_\theta) \simeq \text{Hom}_{cts}(\mathcal{X}^{\Sigma}_\infty^\theta, \mathbb{Q}_p/\mathbb{Z}_p),
\]

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

Now, by [PW11, Rem. 3.2] (since the primes \( \nu \) \( p \) in \( \Sigma \) are finitely decomposed in \( K_\infty/K \)) and Proposition 1.1.3(i), the Selmer group \( H^1_{\text{Gr}}(K, M_\theta) \) is the same as the one defined by the unramified local conditions, i.e., as

\[
\ker\left\{ H^1(K^{\Sigma}/K, M_\theta) \to \prod_{\nu \in \Sigma, \nu \nmid p} H^1(I_\nu, M_\theta)^{G_\nu/I_\nu} \times H^1(I_{\overline{\nu}}, M_\theta)^{G_{\overline{\nu}}/I_{\overline{\nu}}} \right\},
\]

and so under the identification (1.4) we obtain

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

where \( \mathcal{X}_\infty = \text{Gal}(\mathcal{M}_\infty/K_\infty K_\theta) \) is the Galois group of the maximal abelian pro-\( p \) extension of \( K_\infty K_\theta \) unramified outside \( \nu \). Thus from the works of Rubin [Rub91] and Hida [Hid10], proving the Iwasawa main conjecture for imaginary quadratic fields and the vanishing of the \( \mu \)-invariant of \( p \)-adic Hecke \( L \)-functions, respectively, we obtain the result.

**Remark 1.2.3.** Following the notations introduced in the proof of Theorem 1.2.2, and letting \( \mathcal{X}^{\Sigma}_\infty = \text{Gal}(\mathcal{M}^{\Sigma}_\infty/K_\infty K_\theta) \) 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 \( v \) split completely, Proposition 1.1.3(i) shows \( \mathcal{X}^{\Sigma}_\infty = (\mathcal{X}^{\Sigma}_\infty)^\theta \).

The next result will be used to understand the Iwasawa invariants of the \( p \)-adic Selmer group of \( \theta \) in terms of the residual Selmer group.

**Lemma 1.2.4.** Assume that \( \theta | G_\theta \neq 1 \). Then

\[
H^1_{\text{Gr}}(K, M_\theta[p]) \simeq H^1_{\text{Gr}}(K, M_\theta)[p].
\]

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

\[
H^1(K, M_\theta[p]) \to H^1(K, M_\theta)[p]
\]

induced by multiplication by \( p \) on \( M_\theta \) is an isomorphism. Thus to conclude it suffices to check that the natural map \( r_v : H^1(K_v, M_\theta[p]) \to H^1(K_v, M_\theta)[p] \) is an injection, but since \( H^0(K_v, \mathbb{F}_p(\theta)) = 0 \) by our hypothesis, the same argument as above shows that \( r_v \) is an isomorphism.

Denote by

\[
\mathcal{X}^\theta := H^1_{\text{Gr}}(K, M_\theta)^\vee, \quad \mathcal{X}_\theta := H^1_{\text{Gr}}(K, M_\theta)^\vee
\]

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

**Proposition 1.2.5.** Assume that \( \theta | G_\theta \neq 1, \omega \). Then \( \mathcal{X}^\theta \) is a torsion \( \Lambda \)-module with \( \mu \)-invariant zero and

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

Moreover, \( H^1_{\text{Gr}}(K, M_\theta[p]) \) is finite and

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

\begin{equation}
0 \to H^1_{\mathcal{F}_G}(K, M_\theta) \to H^1(K^\Sigma/K, M_\theta) \to \prod_{w \in \Sigma, w \neq p} H^1(K_w, M_\theta) \times H^1(K_v, M_\theta) \to 0
\end{equation}

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

\begin{equation}
0 \to H^1_{\mathcal{F}_G}(K, M_\theta) \to H^1_{\mathcal{F}_G}(K, M_\theta) \to \prod_{w \in S} H^1(K_w, M_\theta) \to 0,
\end{equation}

which combined this Theorem 1.2.2 and Lemma 1.1.1 gives the first part of the Proposition.

For the second part, note that $H^2(K^\Sigma/K, M_\theta) = 0$. (Indeed, by the Euler characteristic formula, the $\Lambda$-cotorsionness of $H^1_{\mathcal{F}_G}(K, M_\theta)$ implies that $H^2(K^\Sigma/K, M_\theta)$ is $\Lambda$-cotorsion; being $\Lambda$-cofree, as follows immediately from the fact that $\text{Gal}(K^\Sigma/K)$ 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

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

Since $H^2(K^\Sigma/K, \mathbb{Q}_p/\mathbb{Z}_p(\theta))$ is $\mathbb{Z}_p$-cofree (because $\text{Gal}(K^\Sigma/K)$ has cohomomogical dimension 2), it follows that $H^1(K^\Sigma/K, M_\theta)^\vee$ has no nonzero pseudo-null $\Lambda$-submodules, and since (1.5) and (1.6) readily imply that

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

as $\Lambda$-modules, by Proposition 1.1.3 and [GV00, Lem. 2.6] we conclude that also $X^S_\theta$ has no nonzero pseudo-null $\Lambda$-submodules. Finally, since $X^S_\theta$ is $\Lambda$-torsion with $\mu$-invariant zero by Theorem 1.2.2, the finiteness of $H^1_{\mathcal{F}_G}(K, M_\theta)[p]$ (and therefore of $H^1_{\mathcal{F}_G}(K, M_\theta[p])$ by Lemma 1.2.4) follows from the structure theorem. It also follows that $X^S_\theta$ is a finitely generated $\mathbb{Z}_p$-module, and since $X^S_\theta$ has no nonzero pseudo-null $\Lambda$-submodules, we conclude that $H^1_{\mathcal{F}_G}(K, M_\theta)$ is divisible, so

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

where $\lambda = \lambda(X^S_\theta)$, which clearly implies the last formula for the $\lambda$-invariant. \hfill \Box

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

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

$$0 \to H^1_{\mathcal{F}_G}(K, M_\theta[p]) \to H^1(K^\Sigma/K, M_\theta[p]) \to H^1(K_v, M_\theta[p]) \to 0$$

is exact.

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

\begin{equation}
\frac{H^1(K^\Sigma/K, M_\theta)}{pH^1(K^\Sigma/K, M_\theta)} \simeq H^2(K^\Sigma/K, M_\theta[p]).
\end{equation}

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

\begin{equation}
0 \to H^1_{\mathcal{F}_G}(K, M_\theta) \to H^1(K^\Sigma/K, M_\theta) \to H^1(K_v, M_\theta) \to 0.
\end{equation}

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

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

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

For the second claim, consider the commutative diagram
which together with the second isomorphism in (1.10) shows that
\[ X/TX \]
(1.9) 0
\[ \](1.9) 0
\at
\[ p \]

1.4. Selmer groups of \( E \). Fix a finite set \( \Sigma \) of places of \( K \) containing \( \infty \) and the primes above \( Np \), and assume that the finite places in \( \Sigma \) are all split in \( K \).

Similarly as in §1.2, we define Selmer group of \( E \) by
\[ \]
\[ H^1_{\text{Gr}}(K, M_E) := \ker \left\{ H^1(K^\Sigma/K, M_E) \to \prod_{w \in \Sigma, w \mid p} H^1(K_w, M_E) \times H^1(K_{\bar{w}}, M_E) \right\}, \]
and the \( S \)-imprimitive Selmer group of \( \theta \), where \( S = \Sigma \setminus \{ v, \bar{v}, \infty \} \), by
\[ \]
\[ H^1_{\text{Gr}}(K, M_E) := \ker \left\{ H^1(K^\Sigma/K, M_E) \to H^1(K_{\bar{v}}, M_E) \right\}. \]

The residual Selmer groups \( H^1_{\text{Gr}}(K, M_E[p]) \) and \( H^1_{\text{Gr}}(K, M_E[p]) \) are defined in the same manner.
Proof. Assume that the last claim of Proposition 1.2.5.

\(\text{lemma applied to this diagram yields the exact sequence in the statement. The last claim now follows from}
\]

vertical maps are given by restriction. Since the left vertical arrow is surjective by Corollary 1.2.6, the snake

\[\phi \]


this completes the proof.

Now we can relate the imprimitive residual and \(p\)-adic Selmer groups. Set

\[X^S_E := H^1_{\mathcal{F}_{Gr}}(K, M_E)^\vee,\]

and similarly \(X_E := H^1_{\mathcal{F}_{Gr}}(K, M_E)[p]\) for the primitive Selmer group.

Proposition 1.4.2. Assume that \(\phi|_{G_p} \neq 1, \omega\). Then

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

Moreover, the modules \(X^S_E\) and \(X_E\) are both \(\Lambda\)-torsion with \(\mu = 0\).

Proof. Since \(\psi = \omega \phi^{-1}\), our assumption on \(\phi\) implies that \(E(K_\psi)[p] = 0\), and therefore \(H^0(K_\psi, M_E) = 0\). Thus the same argument as in the proof of Lemma 1.2.4 yields the isomorphism in the statement. By Corollary 1.4.1, it follows that \(H^1_{\mathcal{F}_{Gr}}(K, M_E)[p]\) is finite, and so \(X^S_E\) is \(\Lambda\)-cotorsion with \(\mu = 0\). Since \(X_E\) is a quotient of \(X^S_E\), 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 \(\phi|_{G_p} \neq 1, \omega\). Then \(X^S_E\) has no non-trivial finite \(\Lambda\)-submodules, and

\[\lambda(X^S_E) = \dim_{\Lambda}(H^1_{\mathcal{F}_{Gr}}(K, M_E)[p]).\]

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

\[0 \rightarrow H^1_{\mathcal{F}_{Gr}}(K, M_E) \rightarrow H^1(K^\Sigma/K, M_E) \rightarrow \prod_{w \in \Sigma, w \neq p} H^1(K_w, M_E) \times H^1(K_\psi, M_E) \rightarrow 0\]

is exact. Proceeding as in the proof of Proposition 1.2.5, we see that the \(\Lambda\)-torsionness of \(X_E\) implies that

\(H^2(K^\Sigma/K, M_E) = 0\) and that \(H^1(K^\Sigma/K, M_E)^\vee\) has no nonzero pseudo-null \(\Lambda\)-submodules. The exactness of (1.12) readily a \(\Lambda\)-module isomorphism

\[X^S_E \simeq H^1(K^\Sigma/K, M_E)^\vee / H^1(K_\psi, M_E)^\vee.\]

Since \(H^1(K_\psi, M_E)\) is \(\Lambda\)-cofree by Lemma 1.3.1, we thus conclude from [GV00, Lem. 2.6] that \(X^S_E\) has no nonzero finite \(\Lambda\)-submodules. Together with the isomorphism \(H^1_{\mathcal{F}_{Gr}}(K, M_E[p]) \simeq H^1_{\mathcal{F}_{Gr}}(K, M_E)[p]\) of Proposition 1.4.2, the last claim in the statement 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 $H^1(K_w, M_E) \cong \Lambda$-torsion, with characteristic ideal generated by the element 
\[
P_w(E) = P_w(\ell^{-1}v_w) \in \Lambda,
\]
where $P_w = \det(1 - \text{Frob}_w X|V_{Iw})$, for $V = T \otimes \mathbb{Q}_p$, is the Euler factor at $w$ of $L$-function of $E$.

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

**Theorem 1.5.1.** Assume that $\phi|_{G_p} \not\equiv 1, \omega$. Then the module $\mathfrak{x}_E$ is $\Lambda$-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(P_w(\phi)) + \lambda(P_w(\psi)) - \lambda(P_w(E)) \).
\]

**Proof.** That $\mathfrak{x}_E$ is $\Lambda$-torsion with $\mu$-invariant zero is part of Proposition 1.4.2. For the $\lambda$-invariant, combining Corollary 1.4.3 and the last claim of Proposition 1.4.1 we obtain 
\[
(1.13) \quad \lambda(\mathfrak{x}_E^S) = \lambda(\mathfrak{x}_\phi^S) + \lambda(\mathfrak{x}_\psi^S).
\]

On the other hand, from (1.12) we deduce the exact sequence 
\[
0 \to H^1_{\text{Gr}}(K, M_E) \to H^1_{\text{Gr}}(K, M_E) \to \prod_{w \in S} H^1(K_w, M_E) \to 0,
\]
and therefore the relation $\lambda(\mathfrak{x}_E^S) = \lambda(\mathfrak{x}_E) + \sum_{w \in S} \lambda(P_w(E))$. This, combined with the second part of Proposition 1.2.5 shows that (1.13) reduces to equality of $\lambda$-invariants in the statement. 

2. Analytic side

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

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

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

Following the conventions in [BDP13], we say that an algebraic Hecke character $\psi : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{C}^\times$ has infinity type $(m, n)$ if $\psi_\infty(z) = z^{-m} \bar{z}^{-n}$ for all $z \in (K \otimes \mathbb{R})^\times \simeq \mathbb{C}^\times$, where $\psi_\infty$ is the component of $\psi$ at $\infty$.

2.1.1. The Bertolini–Darmon–Prasanna $p$-adic $L$-functions. Fix an integral ideal $\mathfrak{N} \subset \mathcal{O}_K$ with 
\[
(2.1) \quad \mathcal{O}_K/\mathfrak{N} \simeq \mathbb{Z}/N\mathbb{Z}.
\]

Following [BDP13], one has the following result, where we let $f$ be the newform associated with $E$.

**Theorem 2.1.1.** There exists an element $L_E \in \Lambda^ur$ such that for every character $\xi$ of $\Gamma$ crystalline at both $v$ and $\hat{v}$ 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 
\[
L_E(\xi) = \Omega_p^{4n} \cdot \frac{\Gamma(n+1)\Gamma(n)\xi^{-1}(\mathfrak{N})}{4\pi^{2n+1}\sqrt{D_K}^{2n-1}} \cdot (1 - a_p(\psi)^{-1} + \xi(\bar{v})^2 p^{-1}) \cdot \frac{L(f/K, \xi, 1)}{\Omega_\infty^{4n}},
\]
where $\Omega_p$ and $\Omega_\infty$ are CM periods attached to $K$.

**Proof.** See [CH18, §3.3], extending the original construction in [BDP13, §5.2] as a continuous function of $\xi$. 


2.1.2. **Katz $p$-adic L-functions.** Let $\theta : G_K \to \mathbb{F}_p^\times$ be a character. We shall view $\theta$ as valued in $\mathbb{Z}_p^\times$ via the Teichmüller lift. As it will suffice for our application, we assume that the conductor $\mathcal{E} \subset \mathcal{O}_K$ of $\theta$ is prime to $p$, and only divisible by primes which are split in $K$.

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

**Theorem 2.1.2.** There exist elements $\mathcal{L}_{v,\theta}, \mathcal{L}_{\bar{v},\theta} \in \Lambda^{ur}$ such that for every character $\xi$ of $\Gamma$ crystalline at both $v$ and $\bar{v}$ and corresponding to a Hecke character of $K$ of infinity type $(n, -n)$ (resp. $(-n, n)$) with $n \in \mathbb{Z}_{\geq 0}$ and $n \equiv 0 \pmod{p-1}$, we have

\[
\mathcal{L}_{v,\theta}(\xi^{-1}) = \Omega_{p^n} \cdot \frac{\Gamma(n)2^{n+2}\pi^n}{\sqrt{D_K}} \cdot (1 - \xi^{-1}(\bar{v}))(1 - \xi(v)p) \cdot \prod_{w|\mathcal{E}}(1 - \xi^{-1}(w)) \cdot L(\xi^{-1}, 0) \frac{L(\xi^{-1}, 0)}{\Omega_{p^n}},
\]

and the same for $\mathcal{L}_{\bar{v},\xi}(\xi^{-1})$ with the roles of $v$ and $\bar{v}$ reversed.

**Proof.** The character $\theta$ defines a projection

\[
\pi_\theta : \mathcal{Z}_p^{ur}[\mathrm{Gal}(K(\mathcal{O}_p^\infty)/K)] \to \Lambda^{ur},
\]

where $K(\mathcal{O}_p^\infty)$ is the ray class field of $K$ of conductor $\mathcal{O}_p^\infty$. The element $\mathcal{L}_{v,\theta}$ is then obtained by applying $\pi_\theta$ to the $p$-adic $L$-function described in [Kri16, Thm. 27], and $\mathcal{L}_{\bar{v},\theta}$ is obtained by reversing the roles of $v$ and $\bar{v}$. \(\square\)

In the following, we set $\mathcal{L}_\theta := \mathcal{L}_{v,\theta}$.

2.2. **Comparison II: Analytic Iwasawa invariants.** The following theorem follows from the main result of [Kri16]. Following the notations in loc.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).

We denote by $\lambda'$ the image of an element $\lambda \in \Lambda$ under the involution of $\Lambda$ given by $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \Gamma$.

**Theorem 2.2.1.** Assume that $E[p]^\times \simeq \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ as $G_Q$-modules. Then there is a factorization $N/N_0 = N_+N_-$ with

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

such that the following congruence holds

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

where

\[
\mathcal{E}_{\phi,\psi} = \prod_{\ell \mid N_0N_-} \mathcal{P}_w(\phi)^2 \cdot \prod_{\ell \mid N_0N_+} \mathcal{P}_w(\psi)^2,
\]

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

**Proof.** Since both $\mathcal{L}_E$ and $\mathcal{L}_\psi$ are elements in $\Lambda^{ur}$, to prove the desired congruence it suffices to show that

\[
\mathcal{L}_E(\xi) \equiv \mathcal{E}_{\phi,\psi}(\xi) \cdot \mathcal{L}_\psi(\xi^{-1}) \pmod{p\mathbb{Z}_p^{ur}}
\]

for $\xi$ any character of $\Gamma$ crystalline at both $v$ and $\bar{v}$ and corresponding to a Hecke character of $K$ of infinity type $(n, -n)$ for some $n \geq 0$ with $n \equiv 0 \pmod{p-1}$. (That this is enough follows essentially from the Weierstrass preparation theorem, cf. [Vat03, Thm. 1.10].)

Letting $\xi$ denote any such character of $\Gamma$, from [Kri16, p. 353] (taking $\chi = \xi N_K^{-1}, \psi_1 = \phi, \psi_2 = \phi^{-1} = \psi^{-1}$ in the notations of loc.cit., so in particular $j = n - 1$) we can extract the congruence

\[
\mathcal{L}_E(\xi) \equiv \left(\left(\frac{\Omega_p}{\Omega_\infty}\right)^{2n} \cdot \frac{\Gamma(n+1)\phi^{-1}(\sqrt{D_K})^{-1}(i)t}{(2\pi i)^{n+1}g(\phi)\sqrt{D_K}^{-1}} \times \Xi_{N_K^{-1}}(\phi, \psi^{-1}, N_+, N_-, p^2N_0) \cdot L(\phi K N_K(\xi \circ \sigma)^{-1}, 0)\right)^2 \pmod{p\mathbb{Z}_p^{ur}},
\]
where
\[
\Xi_{\mathbb{N}^2}(\phi, \psi^{-1}, N_+, N_-, p^2 N_0) = \prod_{\ell \mid N_-} (1 - \phi(\bar{\ell}) \ell^{-1} \xi^{-1}(\bar{\ell})) \cdot \prod_{\ell \mid N_+} (1 - \psi(\bar{\ell}) \ell^{-1} \xi^{-1}(\bar{\ell})) \times \prod_{\ell \mid p^2 N_0} (1 - \phi(\bar{\ell}) \ell^{-1} \xi^{-1}(\bar{\ell}))(1 - \psi(\bar{\ell}) \ell^{-1} \xi^{-1}(\bar{\ell}))
\]
and \( \xi \circ \sigma \) is the composition of \( \xi \) with the action of complex conjugation.

Recall that our \( L_\phi \) and \( L_\psi \) are obtained from the Katz \( p \)-adic \( L \)-function with \( p \)-adic CM type \( \{ \nu \} \). Denoting these temporarily by \( L_{\nu, \phi} \) and \( L_{\nu, \psi} \) (for distinction with \( L_{v, \phi} \) and \( L_{v, \psi} \)), we see from the interpolation property for \( L_{v, \phi} \) that the above congruence can be rewritten as
\[
L_{E}(\xi) \equiv \phi^{-1}(D_K) \left( \frac{\xi^{-1}(t)}{4g(\phi)} \cdot \Xi_{\mathbb{N}^2}(\phi, \psi^{-1}, N_+, N_-, N_0) \cdot L_{v, \phi}(\mathbb{N}_K \xi) \right)^2 \quad (\text{mod } p\mathbb{Z}_p^{nr}),
\]
where we used that \( \xi \circ \sigma = \xi^{-1} \), since \( \xi \) is a character of \( \Gamma \). But it also follows from the interpolation property and functional equation of Katz’s \( p \)-adic \( L \)-functions (using \( \phi^{-1} \omega = \psi \)) that
\[
L_{v, \phi}(\mathbb{N}_K \xi) \equiv L_{v, \psi}(\xi^{-1}) \quad (\text{mod } p\mathbb{Z}_p^{nr})
\]
(see [BCG+19, Lem. 3.3.2(b)]). Moreover, noting that \( \gamma_w = \gamma_w^{-1} \), we see that
\[
\mathcal{E}_{\phi, \psi}(\xi) = \Xi_{\mathbb{N}^2}(\phi, \psi^{-1}, N_+, N_-, N_0),
\]
and therefore (2.2) follows from (2.3) and (2.4), as desired.

**Corollary 2.2.2.** If \( E[p] = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi) \) as \( G_Q \)-modules with \( \phi|_{G_p} \neq 1, \omega \), then \( \mu(L_E) = 0 \) and
\[
\lambda(L_E) = \lambda(L_\phi) + \lambda(L_\psi) + \sum_{w \in S} \{ \lambda(P_w(\phi)) + \lambda(P_w(\psi)) - \lambda(P_w(E)) \}.
\]

**Proof.** Since \( K \) satisfies (Heeg), the conductors of both \( \phi \) and \( \psi \) are only divisible by primes split in \( K \), and hence the vanishing of \( \mu(L_E) \) follows immediately from the congruence of Theorem 2.2.1 and Hida’s result [Hid10] (note that the factors \( P_w(\phi) \) and \( P_w(\psi) \) also have vanishing \( \mu \)-invariant, since again the primes \( w \) are split in \( K \)).

As for the equality between \( \lambda \)-invariants, we note that the involution on \( \Lambda \) given by \( \gamma \mapsto \gamma^{-1} \) for \( \gamma \in \Gamma \) preserves \( \lambda \)-invariants, and so
\[
\lambda(P_w(\phi)^2) = \lambda(P_w(\theta)^2) + \lambda(P_w(\theta)),
\]
using that complex conjugation as inversion on \( \Gamma \). For the term \( \mathcal{E}_{\phi, \psi} \) in Theorem 2.2.1 the thus have
\[
\lambda(\mathcal{E}_{\phi, \psi}) = \sum_{w \mid N_0 N_-} \lambda(P_w(\phi)) + \sum_{w \mid N_0 N_+} \lambda(P_w(\psi)),
\]
where \( w \) runs over all divisors, not just the one dividing \( \mathfrak{m} \), which using the congruence relations in Theorem 2.2.1 (in particular, that \( a_\ell \equiv 0 \pmod{p} \) for \( \ell \mid N_0 \)) can be rewritten as
\[
\lambda(\mathcal{E}_{\phi, \psi}) = \sum_{w \in S} \{ \lambda(P_w(\phi)) + \lambda(P_w(\psi)) - \lambda(P_w(E)) \}.
\]

One the other hand, since \( \psi = \phi^{-1} \omega \), the functional equation for the Katz \( p \)-adic \( L \)-function yields
\[
\lambda(L_\psi) = \lambda(L_\phi).
\]
The result now follows from Theorem 2.2.1 combined with (2.5) and (2.6).

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

**Theorem 2.2.3.** Assume that \( \phi|_{G_p} \neq 1, \omega \). Then \( \mu(L_E) = \mu(\mathcal{X}_E) = 0 \) and
\[
\lambda(L_E) = \lambda(\mathcal{X}_E).
\]

**Proof.** The vanishing of the \( \mu \)-invariant of \( \mathcal{X}_E \) (resp. \( L_E \)) has been shown in Proposition 1.4.2 (resp. Corollary 2.2.2). On the other hand, Iwasawa’s main conjecture for \( K \) (a theorem of Rubin [Rub91]) yields in particular the equalities \( \lambda(L_\phi) = \lambda(\mathcal{X}_\phi), \lambda(L_\psi) = \lambda(\mathcal{X}_\psi) \). The combination of Theorem 1.5.1 and Corollary 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. The result assumes that existence of a non-trivial Kolyvagin system, and in will be later applied in §4 using the system of Heegner points to prove first one of the divisibilities towards Conjecture A (up to powers of \( p \)), and then the full conjecture building on the results in the previous sections.

3.1. Selmer groups 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 finitely generated \( R \)-module equipped with a continuous linear action of \( G_K \) unramified outside a finite set of primes. Following [MR04, Ch. 2], we define a Selmer structure \( \mathcal{F} \) on \( M \) to be a finite set \( \Sigma = \Sigma(\mathcal{F}) \) of places of \( K \) containing \( \infty \), the primes above \( p \), and the primes where \( M \) is ramified, together with a choice of \( R \)-submodules (local conditions) \( H^1_w(K_w, M) \subset H^1(K_w, M) \) for every \( w \in \Sigma \). The associated Selmer group is then defined by

\[
H^1_{\mathcal{F}}(K, M) := \ker \left\{ H^1(K^\Sigma/K, M) \to \prod_{w \in \Sigma} H^1(K_w, M) \right\},
\]

where \( K^\Sigma \) is the maximal extension of \( K \) unramified outside \( \Sigma \).

In particular, we shall consider the unramified (or finite if \( w \nmid p \) is a prime where \( M \) is unramified) local condition

\[
H^1_{\mathcal{F}}(K, M) := \ker \{ H^1(K, M) \to H^1(K^{\text{unr}}, M) \},
\]

and for \( \lambda \) a prime inert in \( K \) lying above \( \ell \neq p \), the transverse local condition

\[
H^1_{\mathcal{F}}(K, M) := \ker \{ H^1(K, M) \to H^1(K[\ell], M) \},
\]

where \( K[\ell] \) is the ring class field of \( K \) of conductor \( \ell \). The singular quotient \( H^1_{\mathcal{F}}(K, M) \) is defined by the exactness of the sequence

\[
0 \to H^1_{\mathcal{F}}(K, M) \to H^1(K, M) \to H^1_{\mathcal{F}}(K, M) \to 0.
\]

Denote by \( \mathcal{L}_0 \) be the set of rational primes \( \ell \neq p \) such that

- \( \ell \) is inert in \( K \),
- \( T \) is unramified at \( \ell \).

As in [How04a], we shall often identify a prime \( \ell \in \mathcal{L}_0 \) with the prime \( \lambda \) of \( K \) above \( \ell \), and occasionally write \( \ell|\lambda \in \mathcal{L}_0 \). For each \( \ell \in \mathcal{L}_0 \), we let \( I_\ell \) be the smallest ideal containing \( \ell+1 \) for which the Frobenius element \( \text{Fr}_\lambda \) acts trivially on \( T/I_\ell T \). Then clearly \( |k_\lambda^\Sigma/k_\lambda^x| \) annihilates \( T/I_\ell T \), where \( k_\lambda \supset k_\ell \) are the residue fields, and so by [MR04, Lem. 1.2.1] there is a finite-singular comparison isomorphism

\[
\phi^p_\ell : H^1_w(K_\ell, T/I_\ell T) \simeq H^1_w(K_\ell, T/I_\ell T) \otimes G_\ell,
\]

where \( G_\ell := k_\lambda^\Sigma/k_\ell^\Sigma \). Moreover, by [MR04, Lem. 1.2.4] the transverse submodule \( H^1_{\mathcal{F}}(K_\lambda, M) \) projects isomorphically onto \( H^1_w(K_\lambda, M) \), thereby giving a splitting

\[
H^1(K_\lambda, M) = H^1_{\mathcal{F}}(K_\lambda, M) \oplus H^1_{\mathcal{F}}(K_\lambda, M).
\]

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

\[
I_n = \sum_{\ell \mid n} I_\ell \subset R, \quad G_n = \bigotimes_{\ell \mid n} G_\ell,
\]

with the convention that \( 1 \in \mathcal{N} I_1 = 0 \), and \( G_1 = \mathbb{Z} \).

Following [How04a], if \( \mathcal{F} \) is a Selmer structure on \( M \) and \( \mathcal{L} \) is a subset of \( \mathcal{L}_0 \) with \( \mathcal{L} \cap \Sigma(\mathcal{F}) = \emptyset \), we shall say that \((M, \mathcal{F}, \mathcal{L})\) is a Selmer triple. Given a Selmer triple \((M, \mathcal{F}, \mathcal{L})\), we define the modified Selmer group \( H^1_{\mathcal{F}^p(c)}(K, M) \) as the one cut out by the local conditions \( H^1_{\mathcal{F}^p(c)}(K_w, M) \) for \( w \nmid abc \), and

\[
H^1_{\mathcal{F}^p(c)}(K, M) = \begin{cases} H^1(K_\lambda, M) & \text{if } \lambda|a, \\
0 & \text{if } \lambda|b, \\
H^1_{\mathcal{F}}(K_\lambda, M) & \text{if } \lambda|c, 
\end{cases}
\]

taking \( \Sigma(\mathcal{F}^p(c)) = \Sigma(\mathcal{F}) \cup \{w|abc\} \).
Definition 3.1.1. A Kolyvagin system for the Selmer triple \((T, F, \mathcal{L})\) is a collection of classes
\[ \kappa = \{ \kappa_n \in H^1_{F(n)}(K, T/I_n T) \otimes G_n \}_{n \in \mathcal{N}} \]
such that \((\phi^e_{\ell} \otimes 1)(\text{loc}_T(\kappa_n)) = \text{loc}_T(\kappa_{n \ell})\) for all \(n \ell \in \mathcal{N}\).

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

3.2. Bounding Selmer groups I. In this section, we assume that \((R, m)\) is a discrete valuation ring with uniformizing parameter \(\pi\) and field of fractions \(\Phi\), and that \((T, F, \mathcal{L})\) is a Selmer triple satisfying hypotheses \((H0)\) and \((H3)-(H4)\) from [How04a, §1.3], and such that

- In place of the (stronger) hypotheses \((H1)-(H2)\) in loc.cit., we have
  \begin{align*}
  (h1) & \quad \bar{T}^{G_K} = 0, \\
  (h2a) & \quad R^\kappa \cap \text{im}\{G_K \to \text{Aut}_R(T)\} \text{ is open in } R^\kappa \\
  (h2b) & \quad V \otimes \epsilon_K \not\simeq V,
  \end{align*}

  where \(V := T \otimes_R \Phi\), with \(\epsilon_K\) the quadratic character associated to \(K\).

- The \(G_K\)-action on \(T\) extends to an action of \(G_Q\), and the action of complex conjugation splits
  \begin{align*}
  (h5) & \quad \bar{T} = \bar{T}^+ \oplus \bar{T}^- \\
  & \quad \text{into one-dimensional eigenspaces.}
  \end{align*}

  The last condition (which replaces hypothesis \((H5)\) in loc.cit.) is forced upon us by the relaxation of hypotheses \((H1)-(H2)\), but will suffice for our applications to rational elliptic curves.

  By propagation (in the sense of [MR04, §1.1]), \(F\) gives rise of a Selmer structure on \(A := T \otimes_R \Phi/R\), with which we define the Selmer group \(H^1_F(K, A)\). Our goal in this section is to prove the following result, extending [How04a, Thm. 1.6.1] to the above setting.

  As in loc.cit., we let \(L_0 = L_0(T) := \{ \ell \in L_0 : I_\ell \subset \beta^* \mathbb{Z}_p \}\), and assume that \(L \supset L_s\) for \(s \gg 0\).

Theorem 3.2.1. Suppose there is a Kolyvagin system \(\kappa \in \text{KS}(T, F, \mathcal{L})\) such that \(\kappa_1 \in H^1_{F}(K, T)\) is non-torsion. Then \(H^1_{F}(K, T)\) has \(R\)-rank one, and there is a finite \(R\)-module \(M\) such that
\[ H^1_{F}(K, A) \simeq (\Phi/R) \oplus M \oplus M \]
with
\[ \text{length}_R(M) \leq \text{length}_R(H^1_{F}(K, T)/R \cdot \kappa_1) + e \]
for some \(e \in \mathbb{Z}_{\geq 0}\) depending only on \(\text{rank}_{\mathbb{Z}_p}(R)\).

Remark 3.2.2. For a fixed \(T\), the bound on the size of the module \(M\) given by Theorem 3.2.1 is of limited use in general; however, for \(T\) varying in a collection twists, it will be a key ingredient in the proof of our Iwasawa-theoretic results in §3.4.

For the proof of Theorem 3.2.1, which will occupy the rest of this section, we shall follow Howard’s strategy. It will be clear from our extension of Howard’s arguments that one can take \(e = 0\) when \(T\) further satisfies the aforementioned hypotheses \((H1)-(H2)\), thereby recovering [How04a, Thm. 1.6.1] in that case.

For any \(k \geq 0\), letting
\[ R^{(k)} := R/m^k R, \quad T^{(k)} := T/m^k T, \quad \mathcal{L}^{(k)} := L \cap L_k(T), \]
we obtain a Selmer triple \((T^{(k)}, F, \mathcal{L}^{(k)})\) satisfying the same hypotheses as \((T, F, \mathcal{L})\), and by [How04a, Rem. 1.2.4] the Kolyvagin system \(\kappa \in \text{KS}(T, F, \mathcal{L})\) gives rise to an element \(\kappa^{(k)} \in \text{KS}(T^{(k)}, F, \mathcal{L}^{(k)})\).

Let \(N^{(k)} := N(L^{(k)})\) be the set of square-free products of primes \(\ell \in L^{(k)}\). By [How04a, Lem. 1.3.3] (whose proof only requires the vanishing of \(T^{G_K}\)), for every \(n \in N^{(k)}\) and \(0 \leq i \leq k\) there are natural isomorphisms
\[ H^1_{F(n)}(K, T^{(k)}/m^i T^{(k)}) \simeq H^1_{F(n)}(K, T^{(k)}/m^i) \simeq H^1_{F(n)}(K, T^{(k)})/m^i \]
induced by the maps \(T^{(k)}/m^i T^{(k)} \xrightarrow{\pi^{k-1}} T^{(k)}/m^i \to T^{(k)}\).
Denote by $H^1(K, T^{(k)})^\pm$ the $\pm$-eigenspaces under the action of complex conjugation, and for any element $c$ is an $R^{(k)}$-module $H$, define

$$\text{ord}(c) := \min\{r \in \mathbb{Z}_{\geq 0} : \pi^r c = 0\}.$$ 

The starting point of our extension of Howard’s arguments will be the following result.

**Lemma 3.2.3.** Given any nonzero classes $c^\pm \in H^1(K, T^{(k)})^\pm$ there exist infinitely many $\ell \in \mathcal{L}^{(k)}$ such that

$$\text{ord}(\text{loc}_\ell(c^\pm)) \geq \text{ord}(c^\pm) - e$$

for some $e \in \mathbb{Z}_{\geq 0}$ bounded independently of $k$ and depending only on $\text{rank}_{R_p}(R)$.

**Proof.** This follows from [Nek07, (7.5.1)] (an application of the Cebotarev density theorem in [loc.cit., (6.5.1)]), where the result of shown for $e = C_2 + C_3$ for the constants $C_2$ and $C_3$ defined in (6.1.2) and (6.2.1) of [Nek07], respectively. By hypothesis (h2a), the constant $C_2$ is bounded independently of $k$, and by hypothesis (h2b) the constant $C_3$ is independent of $k$ and bounded by a constant depending only on $\text{rank}_{R_p}(R)$. The result follows.

Abbreviate $\mathcal{H}^{(k)}(n) = H^1_{\mathcal{F}(n)}(K, T^{(k)})$. Let $e \in \mathbb{Z}_{\geq 0}$ be the constant given by Lemm 3.2.3, and set

$$\mathcal{H}^{(k)}(n) := \frac{H^1_{\mathcal{F}(n)}(K, T^{(k)})[\pi^{e+1}]}{H^0_{\mathcal{F}(n)}(K, T^{(k)})[\pi^e]}.$$ 

Denoting by $\mathcal{H}^{(k)}(n)^\pm$ the $\pm$-eigenspaces under the action of complex conjugation, set also

$$\varrho^{(k)}(n)^\pm := \dim_{R/m}(\mathcal{H}^{(k)}(n)^\pm), \quad \varrho^{(k)}(n) := \dim_{R/m}(\mathcal{H}^{(k)}(n)).$$

so in particular,

$$\varrho^{(k)}(n) = \varrho^{(k)}(n)^+ + \varrho^{(k)}(n)^-.$$ 

Denote by $\mathcal{L}^{(k)} \subset \mathcal{L}$ be the set of primes $\ell$ as in Lemma 3.2.3, and let $N^{(k)} = N(\mathcal{L}^{(k)})$ be the set of square-free products of primes $\ell \in \mathcal{L}^{(k)}$.

**Lemma 3.2.4.** For any $n \in N^{(k)}$ the following hold:

(a) If $\text{loc}_\ell(\mathcal{H}^{(k)}(n)^\pm) \neq 0$, then $\varrho^{(k)}(n\ell)^\pm = \varrho^{(k)}(n)^\pm - 1$.

(b) If $\text{loc}_\ell(\mathcal{H}^{(k)}(n)^\pm) = 0$, then $\varrho^{(k)}(n\ell)^\pm = \varrho^{(k)}(n)^\pm + 1$.

In particular, the parity of $\varrho^{(k)}(n)$ is independent of $n \in N^n$.

**Proof.** This follows by the same argument as in [How04a, Lem. 1.5.3], using the fact that by Lemma 3.2.3 the localization map at $\ell$ induces maps

$$0 \to H^1_{\mathcal{F}(n)}(K, T^{(k)})[\pi^{e+1}] \to \mathcal{H}^{(k)}(n) \xrightarrow{\text{loc}_\ell} H^1_{\ell}(K, T^{(k)}),$$

$$0 \to \mathcal{H}^{(k)}(n) \xrightarrow{H^1_{\mathcal{F}(n)}(K, T^{(k)})[\pi^e]} \xrightarrow{\text{loc}_\ell} H^1_{\ell}(K, T^{(k)}),$$

with the action of complex conjugation splitting the right-most terms into one-dimensional eigenspaces by the isomorphisms in (3.1) and hypothesis (h5).

An important consequence of preceding “parity lemma” is in the next result.

**Proposition 3.2.5.** For every $n \in N^{(k)}$, there is an $R^{(k)}$-module $M^{(k)}(n)$ such that

$$\mathcal{H}^{(k)}(n) \simeq (R^{(k)})^\epsilon \oplus M^{(k)}(n) \oplus M^{(k)}(n)$$

for some $\epsilon \in \{0, 1\}$ independent of both $k$ and $n \in N^{(k)}$.

**Proof.** The existence of a decomposition of the given form follows from [How04a, Thm. 1.4.2], which applies without change in our setting. One the other hand, that $\epsilon$ is independent of $k$ is immediate from (3.2), while the independence on $n$ follows from the observation that

$$\varrho^{(k)}(n) = \epsilon + 2 \dim_{R/m} M^{(k)}(n)[m]$$

and this has parity independent of $n \in N^{(k)}$ by Lemma 3.2.4.
Similarly as in [MR04, §4.3] (and following [How04a, Def. 1.5.4]), define the stub Selmer module by
\[ S^{(k)}(n) := \mathfrak{m}^{\lambda_n(k)}(n)H^{(k)}(n), \]
where \( \lambda_n(k) = \text{length}_{R(k)}(M^{(k)}(n)) \). The next result is an easy consequence of the definitions and global duality.

**Lemma 3.2.6.**

1. For \( n\ell \in \mathcal{N} \), the following implication holds:
   \[ \text{loc}_\ell(S^{(k)}(n)) = 0 \implies \text{loc}_\ell(S^{(k)}(n\ell)) = 0. \]
2. If \( n \in \mathcal{N}(2k-1) \) is such that \( S^{(k)}(n) \neq 0 \), then the image of the natural map
   \[ H^1_{\mathcal{F}(n)}(K, T^{(2k-1)}) \to H^1_{\mathcal{F}(n)}(K, T^{(k)}) \]
   contains a free \( R^{(k)} \)-module of rank one.

**Proof.** Part (1) is [How04a, Prop. 1.5.9], which follows from global duality, while part (2) is [How04a, Lem. 1.6.3], whose proof only uses (3.2) and the definitions (so they both apply without change to our more general context).

From on, we fix a generator of \( G_\ell \) for every \( \ell \in \mathcal{L}_0 \), so that we may view the classes \( \kappa^{(k)}_n \) as elements in \( H^1_{\mathcal{F}(n)}(K, T^{(k)}) \simeq H^1_{\mathcal{F}(n)}(K, T^{(k)}) \otimes G_\ell \).

**Proposition 3.2.7.** If \( n \in \mathcal{N}^{(k)} \), then \( \pi^e\kappa^{(k)}_n \in S^{(k)}(n) \).

**Proof.** We shall prove this by an argument is similar to that in [How04a, Lem. 1.6.4], but rather than arguing by induction on \( k \) and the \( R/\mathfrak{m} \)-dimension of \( H^1_{\mathcal{F}(n)}(K, T^{(k)}) \), we shall argue by induction on \( k \) and the quantity \( \varrho^{(k)}(n) \) in (3.3).

Assume that \( k > 0 \) is the minimal integer giving a counterexample (for some \( n \)). Recall that
\[ \lambda_n^{(k)} := \text{length}_{R^{(k)}}(M^{(k)}(n)). \]
If \( \lambda^{(k)}(n) < e \), then \( \pi^eS^{(k)}(n) = \pi^eH^{(k)}(n) \), which clearly contains \( \pi^e\kappa^{(k)}_n \), so from now on we assume \( \lambda^{(k)}(n) \geq e \). Suppose first that \( S^{(k)}(n) \neq 0 \). This implies that \( e = 1 \) and
\[ i := \lambda^{(k)}(n) < k. \]
By minimality of \( k \), we must have \( \pi^e\kappa^{(i)}_n \in S^{(i)}(n) \). Since by (3.2) multiplication by \( \pi^{k-i} \) induces the first identification
\[ M^{(i)}(n) \simeq M^{(k)}(n)[\mathfrak{m}^i] = M^{(k)}(n), \]
it follows that \( \lambda^{(i)}(n) = \lambda^{(k)}(n) = i \), and so \( S^{(i)}(n) = 0 \). Thus \( \pi^e\kappa^{(i)}_n = 0 \), i.e., \( \pi^{e+k-i}\kappa^{(k)}_n = 0 \). By Lemma 3.2.6(2), it follows that \( \kappa^{(k)}_n \) is divisible by \( \pi^{-e} \) (a non-negative power of \( \pi \), as noted above) in \( H^{(k)}(n) \), and so \( \pi^e\kappa^{(k)}_n \in \pi^eH^{(k)}(n) \), yielding the result in the case \( S^{(k)}(n) \neq 0 \).

Now keep \( k \) as above fixed, and suppose \( n \in \mathcal{N}^{(k)} \) gives a counterexample with \( \varrho^{(k)}(n) \) minimal. By the preceding argument, we must have
\[ S^{(k)}(n) = 0. \]
Moreover, by Proposition 3.2.5 if \( \varrho^{(k)}(n) \in \{0, 1\} \) then \( S^{(k)}(n) = H^{(k)}(n) \) (which contains \( \kappa^{(k)}_n \)), so to have a counterexample we must have \( \varrho^{(k)}(n) > 1 \).

**Case i:** \( \varrho^{(k)}(n) \) are both nonzero. Since we assume \( \varrho^e\kappa^{(k)}_n \notin S^{(k)}(n) \), we have \( \varrho^e\kappa^{(k)}_n \neq 0 \). Thus by Lemma 3.2.3 we can find some \( \ell \in \mathcal{L}^{(k)} \) such that \( \kappa^{(k)}_n \) has a multiple with non-zero image under the localization map
\[ H^{(k)}(n) \xrightarrow{\text{loc}_\ell} H^1_{\mathcal{F}(\ell)}(K_\ell, T^{(k)}) \]
for some sign \( \pm \), say equal to +1; in particular, \( \text{loc}_\ell(\kappa^{(k)}_n) \neq 0 \). Similarly, since \( \varrho^{(k)}(n) - 2 \), so by induction \( \varrho^e\kappa^{(k)}_{n\ell} \in S^{(k)}(n\ell) \), which by Lemma 3.2.6(1) implies \( \text{loc}_\ell(\kappa^{(k)}_{n\ell}) = 0 \); impossible by the Kolyvagin system relations.
Case ii: One of \( \varrho (k)(n) \) is equal to zero. Suppose \( \varrho (k)(n) = 0 \), so that \( \varrho (k)(n) > 1 \). If \( \pi \kappa_{n}^{(k)} \neq 0 \) \((\Leftrightarrow \pi \kappa_{n}^{(k)} \not\in \mathcal{S}(k)(n))\), then \( \kappa_{n}^{(k)} \) has a multiple with nonzero image under the localization map (3.4) for \( \pm = +1 \). By Lemma 3.2.4, it follows that \( \varrho (k)(nl) = \varrho (k)(n) - 1 \) and \( \varrho (k)(nl)^{-} = 1 \), and these are both positive. Since also \( \varrho (k)(nl) = \varrho (k)(n) \), by Case i we deduce that \( \pi \kappa_{n}^{(k)} \in \mathcal{S}(k)(nl) \), and so \( \varrho (k)(nl) = 0 \) by Lemma 3.2.6(1), contradicting again the Kolyvagin system relations.

We can now conclude the proof of Theorem 3.2.1.

Proof of Theorem 3.2.1. The rest of the proof now proceeds as in [How04a, p.1454-5]. Indeed, taking \( k \gg 0 \) such that \( \pi \kappa_{1}^{(k)} \neq 0 \), by Proposition 3.2.7 with \( n = 1 \) we get \( \pi \kappa_{1}^{(k)} \in \mathcal{S}(k)(1) \), so in particular \( \mathcal{S}(k)(1) \neq 0 \). It follows that

\[
H^1_{\mathbb{F}} (K, A) \simeq (\Phi / R) \oplus M \oplus M
\]

for some finite \( R \)-module \( M \cong M^{(k)}(1) \) with

\[
\lambda := \text{length}_R (M) = \lambda^{(k)}(1) < k.
\]

Thus Proposition 3.2.7 again gives \( \pi \kappa_{1}^{(k)} \in \pi \lambda H^1_{\mathbb{F}} (K, T^{(k)}) \), which by the injectivity of the map

\[
H^1_{\mathbb{F}} (K, T) / m^k H^1_{\mathbb{F}} (K, T) \to H^1_{\mathbb{F}} (K, T^{(k)})
\]

implies that \( \pi \kappa_{1} \in \pi \lambda H^1_{\mathbb{F}} (K, T) \); this inclusion, combined with (3.5), yields the result.

3.3. Bounding Selmer groups II. Let \( E / \mathbb{Q} \) be an elliptic curve of conductor \( N \), let \( p \) be a prime of good ordinary reduction for \( E \), and let \( K \) be an imaginary quadratic field of discriminant prime to \( Np \). Assume that

\[
E(K)[p] = 0
\]

and that

\[
E \text{ does not have CM by } K.
\]

Let \( \Gamma = \text{Gal}(K_{\infty} / K) \) be the Galois group of the anticyclotomic \( \mathbb{Z}_{p} \)-extension of \( K \), and let \( \alpha : \Gamma \to R^{\times} \) be a character with values in the ring of integers \( R \) of a finite extension \( \Phi / \mathbb{Q}_{p} \). Consider the \( G_{K} \)-module

\[
T := (T_{p} E) \otimes_{\mathbb{Z}_{p}} R(\alpha), \quad A := T \otimes_{R} \Phi / R,
\]

where \( T_{p} E \) is the \( p \)-adic Tate module of \( E \), and \( R(\alpha) \) is the free \( R \)-module of rank one on which \( G_{K} \) acts via \( \alpha \).

For \( w \) a prime of \( K \) above \( p \), let

\[
\text{Fil}^+_w (T_{p} E) := \ker \{ T_{p} E \to T_{p} \hat{E} \}, \quad \text{Fil}^-_w (T_{p} E) := T_{p} E / \text{Fil}^+_w (T_{p} E),
\]

where \( \hat{E} \) is the reduction of \( E \) at \( v \). Following [CG96], we define the ordinary Selmer structure \( \mathcal{F}_{\text{ord}} \) on \( T \) by

\[
H^1_{\mathcal{F}_{\text{ord}}} (K_{w}, T) := \begin{cases} 
\ker \{ H^1 (K_{w}, T) \to H^1 (K_{w}, \text{Fil}^-_w (T_{p} E) \otimes \Phi) \} & \text{if } w \mid p, \\
H^1 (K_{w}, T) & \text{else},
\end{cases}
\]

and let \( \mathcal{F}_{\text{ord}} \) also denote the induced Selmer structure on \( A \). (Note that since \( T \otimes_{R} \Phi \) is \( 2 \)-dimensional and pure of weight \(-1 \), these are the same as the Selmer structures considered in [How04a, §2.1].)

Let

\[
\mathcal{L} := \{ \ell \in \mathcal{L}_0 : a_{\ell} \equiv \ell + 1 \equiv 0 \pmod{p} \},
\]

where \( a_{\ell} = \ell + 1 - | \hat{E}(\mathbb{F}_{\ell}) | \), so that \( \mathcal{L} = \mathcal{L}_1 (T_{p} E) \) in the notations of §3.2.

Theorem 3.3.1. Suppose that there is a Kolyvagin system \( \kappa \in \text{KS}(T, F_{\text{ord}}, \mathcal{L}_{E}) \) with \( \kappa_{1} \in H^1_{\mathcal{F}_{\text{ord}}} (K, T) \) non-torsion. Then \( H^1_{\mathcal{F}_{\text{ord}}} (K, T) \) has rank one, and there is a finite \( R \)-module \( M \) such that

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

with

\[
\text{length}_R (M) \leq \text{length}_R (H^1_{\mathcal{F}_{\text{ord}}} (K, T) / R \cdot \kappa_{1}) + e
\]

for some constant \( e \in \mathbb{Z}_{\geq 0} \) depending only on \( \text{rank}_{K_{0}} (R) \).
For the proof, note that $T$ satisfies hypotheses (H0), (h1), (h2a)-(h2b), and (H3)-(H4) from §3.2, but because of the twist by the character $\alpha$, hypothesis (h5) may not hold (unless $\alpha$ is trivial), and so Theorem 3.2.1 cannot be applied to $T$. However, the strategy of proof of Theorem 3.2.1 can still be adapted, and in the remainder of this section we shall explain how to modify the arguments of §3.2 to obtain a proof of Theorem 3.3.1.

For the ease of notation, let $({\mathcal F},L)$ denote $({\mathcal F}_{\text{ord}},L_{E})$. As in §3.2, every $\kappa \in \text{KS}(T, {\mathcal F},L)$ gives rise to $\kappa^{(k)} \in \text{KS}(T^{(k)},{\mathcal F},L^{(k)})$. Fix $k > 0$, and an integer $N = N(k)$ such that the composite character

$$\kappa := \text{Res} \circ R^{\times} \to (R/m^{k})^{\times}$$

factors through $\Gamma_{N} := \text{Gal}(K_{N}/K)$, where $K_{N}$ denote the subextension of $K_{\infty}$ of degree $p^{N}$ over $K$.

We shall prove an analogue of Proposition 3.2.7 for $T$ (from which Theorem 3.3.1 will easily follow) by considering the image of classes under the restriction map

$$H^{1}(K,T^{(k)}) \xrightarrow{\text{res}_{N}} H^{1}(K_{N},T^{(k)}) \simeq H^{1}(K_{N},T_{E} \otimes \mathbb{Z}/p^{k}\mathbb{Z}) \otimes (R/m^{k})(\alpha),$$

exploiting the natural action of complex conjugation on the target.

**Lemma 3.3.2.** The map $\text{res}_{N}$ is injective.

**Proof.** By the inflation-restriction exact sequence, the kernel $\text{res}_{N}$ is given by

$$H^{1}(K_{N}/K, (T^{(k)})^{G_{K_{N}}}) = (T^{(k)})^{G_{K_{N}}} / (\sigma - 1)(T^{(k)})^{G_{K_{N}}} ,$$

where $\sigma$ is a generator of $\Gamma_{N}$. Since $G_{K_{N}}$ acts trivially on $R/m^{k}(\alpha)$, $(T^{(k)})^{G_{K_{N}}}$ is a scalar extension of $(T_{E} \otimes \mathbb{Z}/p^{k}\mathbb{Z})^{G_{K_{N}}}$, and this vanishes by (h1′), since it implies $E(K_{\infty})[p^{\infty}] = 0$. $\square$

Notice that, being inert in $K$, the primes $\ell \in \mathcal{L}$ split completely in $K_{N}$, and so

$$(3.7) \quad H^{1}((K_{N})_{\ell},T^{(k)}):= \prod_{\lambda | \ell} H^{1}((K_{N})_{\lambda},T^{(k)}) \simeq H^{1}(K_{\ell},T^{(k)}) \otimes (R/m^{k})[\Gamma_{N}]$$

by Shapiro’s lemma. In particular, letting $\text{loc}_{\ell}$ be the restriction map $H^{1}(K,T^{(k)}) \to H^{1}((K_{N})_{\ell},T^{(k)})$, we have a commutative diagram

$$
\begin{array}{ccc}
H^{1}(K,T^{(k)}) & \xrightarrow{\text{res}_{N}} & H^{1}(K_{N},T^{(k)}) \\
\downarrow \text{loc}_{\ell} & & \downarrow \text{loc}_{\ell} \\
H^{1}(K_{\ell},T^{(k)}) & \longrightarrow & H^{1}((K_{N})_{\ell},T^{(k)})
\end{array}
$$

(3.8)

in which the horizontal maps are injective.

As before, let $\bar{T} = T/m$ be the residual representation associated to $T$. The local Tate pairing

$$(a,b)_{\ell} : H^{1}((K_{N})_{\ell},\bar{T}) \times H^{1}((K_{N})_{\ell},\bar{T}) \to R/m,$$

defined as a sum of the local Tate pairings for $(K_{N})_{\lambda}$ over $\lambda | \ell$, extends to a non-degenerate pairing

$$(a,b)_{N} : H^{1}((K_{N})_{\ell},\bar{T}) \times H^{1}((K_{N})_{\ell},\bar{T}) \to (R/m)[\Gamma_{N}]$$

(3.9)

which is $(R/m)[\Gamma_{N}]$-linear in the first argument and anti-linear in the second, by the rule

$$(a,b)_{N} : \sum_{\sigma \in \Gamma_{N}} (a,b^{\sigma})_{N} \cdot \sigma^{-1},$$

and it follows from the properties of $(a,b)_{\ell}$ that $H^{1}_{\ell}((K_{N})_{\ell},\bar{T})$ is its own orthogonal complement under $(a,b)_{N}$.

Similarly as in §3.2, for every $n \in \mathcal{N}^{(k)}$ we abbreviate $H_{N}^{(k)}(n) = H^{1}_{F(n)}(K_{N},T^{(k)})$, set

$$\mathcal{H}_{N}^{(k)}(n) := \frac{H_{N}^{(k)}(n)[\pi^{e+1}]}{H_{N}^{(k)}(n)[\pi^{e}]},$$

and denote by $\mathcal{H}_{N}^{(k)}(n)_{\pm}$ its $\pm$-eigenspaces under the action of complex conjugation. Set also

$$(3.10) \quad e_{N}^{(k)}(n) := \text{rank}_{(R/m)[\Gamma_{N}]}(\mathcal{H}_{N}^{(k)}(n)), \quad e_{N}^{(k)}(n)_{\pm} := \text{rank}_{(R/m)[\Gamma_{N}]}(\mathcal{H}_{N}^{(k)}(n))_{\pm},$$

where $e$ is as in Lemma 3.2.3, and the ranks are to be understood as the minimal number of generators.
Let also $\mathcal{H}^{(k)}(n)$ and $\mathcal{H}^{(k)}_{\mathbb{Q}}(n)$ be as in §3.2, and with a slight abuse of notation, denote by
\[
\text{res}_N(\mathcal{H}^{(k)}(n)) \subset \mathcal{H}^{(k)}_{\mathbb{Q}}(n)
\]
the image of $\mathcal{H}^{(k)}(n)$ in $\mathcal{H}^{(k)}_{\mathbb{Q}}(n)$ under the map induced by $\text{res}_N$ (note that $\text{res}_N(\mathcal{H}^{(k)}(n))$ may not be an isomorphic copy of $\mathcal{H}^{(k)}(n)$, despite Lemma 3.3.2), and set
\[
\text{res}_N(\mathcal{H}^{(k)}(n))^{\pm} := \mathcal{H}^{(k)}_{\mathbb{Q}}(n)^{\pm} \cap \text{res}_N(\mathcal{H}^{(k)}(n)).
\]
Recall that $\mathcal{H}^{(k)}_{\mathbb{Q}}$ denotes the set of square-free products of primes $\ell$ as in Lemma 3.2.3 (denoted $\ell \in \mathcal{L}^{(k)\mathbb{Q}}$).

**Lemma 3.3.3.** For any $n\ell \in \mathcal{H}^{(k)\mathbb{Q}}$ the following hold:

(a) If $\ell \not| (\text{res}_N(\mathcal{H}^{(k)}(n)))^\pm$, then $\hat{\gamma}^{(k)}_N(n\ell)^\pm = \hat{\gamma}^{(k)}_N(n)^\pm - 1$.

(b) If $\ell \not| (\text{res}_N(\mathcal{H}^{(k)}(n)))^\pm$, then $\hat{\gamma}^{(k)}_N(n\ell)^\pm = \hat{\gamma}^{(k)}_N(n)^\pm + 1$.

**Proof.** By (3.8), the localization map at $\ell$ induces $(R/m)[\Gamma_N]$-linear maps
\[
0 \to H^1_{\mathcal{F}(n)}(K_N, T^{(k)})[\pi^e + 1] \to \mathcal{H}^{(k)}_{\mathbb{Q}}(n) \xrightarrow{\text{loc}_\ell} H^1((K_N)_\ell, \bar{T}),
\]
\[
0 \to \mathcal{H}^{(k)}_{\mathbb{Q}}(n) \to H^1_{\mathcal{F}(n)}(K_N, T^{(k)})[\pi^e + 1] \xrightarrow{\text{loc}_\ell} H^1((K_N)_\ell, \bar{T}),
\]
and by (3.1), hypothesis $\text{(h5)}$, and (3.7), the action of complex conjugation splits $H^1((K_N)_\ell, \bar{T})$ and $H^1((K_N)_\ell, \bar{T})$ into free $(R/m)[\Gamma_N]$-modules of rank one. Since the assumption in part (a) implies that the restriction of $\text{loc}_\ell$ to the $\pm$-eigenspace is surjective, the result follows as in Lemma 3.3.3, using the properties of the local Tate pairing $(\cdot, \cdot)_N$ recalled above, and the proof of part (b) follows as in [How04a, Lem. 1.5.3].

As in §3.2, set
\[
\mathcal{S}^{(k)}(n) = \mathcal{S}^{(k)}(n) = \lambda^{(k)}(n)H^1_{\mathcal{F}(n)}(K, T^{(k)}),
\]
where $\lambda^{(k)}(n) = \text{length}_{R^{(k)}}(M^{(k)}(n))$ for $M^{(k)}(n)$ as in Proposition 3.2.5.

**Proposition 3.3.4.** If $n \in \mathcal{H}^{(k)\mathbb{Q}}$, then $\pi^{(k)}_N \in \mathcal{S}^{(k)}(n)$.

**Proof.** The proof of Proposition 3.2.7 applies almost verbatim, inducting on $k$ and the quantity $\hat{\gamma}^{(k)}_N(n)^\pm$ in (3.10), and using Lemma 3.3.3 (in place of Lemma 3.2.4) to handle the Cases i-ii.

The proof of Theorem 3.3.1 now follows from Proposition 3.3.4 as in the proof of Theorem 3.2.1.

### 3.4. Iwasawa theory

Let $E$, $p$ and $K$ be as in §3.3, and assume in addition that every prime factor of $N$ splits in $K$. Let $\Lambda = \mathbb{Z}_p[[\Gamma]]$ be the anticyclotomic Iwasawa algebra, and consider the $\Lambda$-modules $M_E := (T_p E) \otimes_{\mathbb{Z}_p} \Lambda^\gamma$, $T := T_p E(1) \simeq (T_p E) \otimes_{\mathbb{Z}_p} \Lambda$, where the $G_K$-action on $\Lambda$ is given by the tautological character $G_K \rightarrow \Gamma \rightarrow \Lambda^\times$.

Following [CG96] (see also [How04b, Def. 3.2.2]), we define the ordinary Selmer structure $\mathcal{F}_\Lambda$ on $M_E$ by
\[
H^1_{\mathcal{F}_\Lambda}(K^w, M_E) := \begin{cases} 
\ker\{H^1(K^w, M_E) \to H^1(K^w, \text{Fil}_w(T_p E) \otimes \Lambda)\} & \text{if } w|p, \\
0 & \text{else,}
\end{cases}
\]
and let $\mathcal{F}_\Lambda$ also denote the Selmer structure on $T$ defined by the orthogonal complements of $H^1_{\mathcal{F}_\Lambda}(K^w, M_E)$ under local Tate duality. Denote by
\[
X := \text{Hom}_{cts}(H^1_{\mathcal{F}_\Lambda}(K, M_E), \mathbb{Q}_p/\mathbb{Z}_p)
\]
the Pontryagin dual, and let $\mathcal{L}_E = \mathcal{L}_1(T_p E)$ be as in §3.3.

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

(i) $X \sim \Lambda \oplus M \oplus M$,

(ii) $\text{char}_\Lambda(M)$ divides $\text{char}_\Lambda(H^1_{\mathcal{F}_\Lambda}(K, T)/\Lambda \kappa_1)$ in $\Lambda[1/p]$. 
Proof. This now follows by applying the result of Theorem 3.3.1 for the specializations of $T$ at height one primes of $\Lambda$, similarly as in the proof of [How04a, Thm. 2.2.10]. We just explain how to deduce the divisibility in part (ii), since the other statements are shown exactly as in [How04a, Thm. 2.2.10].

For any height one prime $\mathfrak{P} \subset \Lambda$ with $\mathfrak{P} \not\mid p\Lambda$, set

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

where $S_{\mathfrak{P}}$ is the integral closure of $\Lambda/\mathfrak{P}$. (Notice that this is a representation of the type considered in §3.3.) Suppose $\mathfrak{P} \not\mid p\Lambda$, write $\mathfrak{P} = (g)$, and set $\Omega_m := (g + p^m)$ for $m > 0$. Writing $\kappa^{(\Omega_m)}$ for the image of $\kappa$ under the specialization map

$$\text{KS}(T, F_{\Lambda}, L_E) \to \text{KS}(T_{\Omega_m}, F_{\text{ord}}, L_E),$$

as in [How04a, p.1463] we see that the equalities

$$\text{length}_{\mathfrak{p}}(H^1_{X_{\Omega_m}}(K, T_{\Omega_m})/S_{\Omega_m}\kappa^{(\Omega_m)}) = md \text{ ord}_{\mathfrak{P}}(f_{\Lambda})$$

and

$$2 \text{ length}_{\mathfrak{p}}(M_{\Omega_m}) = md \text{ ord}_{\mathfrak{P}}(\text{char}_A(X_{\text{tors}}))$$

hold up to $O(1)$ as $m$ varies, where $f_{\Lambda} \in \Lambda$ is a characteristic power series of $H^1_{X_{\Lambda}}(K, T)/\Lambda\kappa_1$, and $X_{\text{tors}}$ denotes the $\Lambda$-torsion submodule of $X$. On the other hand, Theorem 3.3.1 yields the inequality

$$\text{length}_{\mathfrak{p}}(M_{\Omega_m}) \leq \text{length}_{\mathfrak{p}}(H^1_{X_{\Omega_m}}(K, T_{\Omega_m})/S_{\Omega_m}\kappa^{(\Omega_m)}) + e_m$$

for some error term $e_m$ depending only on $\text{rank}_{\mathfrak{p}}(S_{\Omega_m}) = \text{rank}_{\mathfrak{p}}(S_{\mathfrak{P}})$, and hence $O(1)$ as $m$ varies. Letting $m \to \infty$ we thus deduce that

$$\text{ord}_{\mathfrak{P}}(\text{char}_A(X_{\text{tors}})) \leq 2 \text{ ord}_{\mathfrak{P}}(f_{\Lambda}),$$

yielding the divisibility in part (ii). \[ \square \]

4. Proof of Theorem C and Corollary D

4.1. Preliminaries. Let $E/Q$ be an elliptic curve of conductor $N$, let $K$ be an imaginary quadratic field satisfying hypotheses (Heeg) and (disc), and fix an integral ideal $\mathfrak{N} \subset O_K$ with $O_K/\mathfrak{N} = \mathbb{Z}/N\mathbb{Z}$. For each positive integer $m$ prime to $N$, let $K[m]$ be the ring class field of $K$ of conductor $m$, and set

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

Let also $O_m = \mathbb{Z} + mO_K$ be the order of $K$ of conductor $m$.

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

$$\mathbb{C}/O_K \to \mathbb{C}/(\mathfrak{N} \cap O_m)^{-1}$$

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 $\kappa^{\text{Hg}} \in \text{KS}(T, F_{\Lambda}, L_E)$ such that $\kappa^{\text{Hg}} \in H^1_{X_{\Lambda}}(K, T)$ is nonzero.

**Proof.** Under the additional hypotheses that $p \nmid h_K$, the class number of $K$, and the representation $G_K \to \text{Aut}_{\mathfrak{p}}(T)$ 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 explaining the construction of $\kappa^{\text{Hg}}$, which will be the same as in [How04a, §2.3], and to which the reader is referred for further details. For each $n \in N$ and $k \geq 0$ set

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

where $d(k) = \min\{d \in \mathbb{Z}_{\geq 0} \mid K_k \subset K[p^d(k)]\}$, 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 $\mathbb{Z}_p[\text{Gal}(K_k[n]/K)]$-submodule generated by $P[n]$ and $P_j[n]$ for $j \leq k$, it follows from the norm relations between Heegner points [PR87, §3.1] that one can form the $\mathcal{G}(n)$-module

$$H[n] := \lim_k H_k[n].$$
By [How04a, Lem. 2.3.3], there is a family
\[\{Q[n] = \lim_{\kappa} Q_{K[n]} \in H[n]\}_{n \in \mathbb{N}}\]
satisfying the relations
\[(4.1) \quad Q_0[n] = \Phi P[n], \text{ where } \Phi = \begin{cases} (p - a_p \sigma_p + \sigma_p^2)(p - a_p \sigma_p^*) + \sigma_p^2) & \text{if } p \text{ splits in } K, \\ (p + 1)^2 - a_p^2 & \text{else,} \end{cases}\]
with \(\sigma_p\) and \(\sigma_p^*\) the Frobenius elements at the primes above \(p\) in the split case, and
\[\text{Norm}_{K_{\infty}[n\ell]/K_{\infty}[n\ell]} Q[n\ell] = a_t Q[n]\]
for all \(n \in \mathbb{N}\). Letting \(D_n \in \mathbb{Z}_p[G(n)]\) be Kolyvagin’s derivative operators, and choosing a set \(S\) of representatives for \(G(n)/G(n)\), the class \(\kappa(n) \in H^1(K, T/I_n T)\) is defined as the natural image of
\[(4.2) \quad \bar{\kappa}_n := \sum_{\alpha \in S} sD_n Q[n] \in H[n]\]
under the composite map
\[\left( H[n]/I_n H[n] \right)^{\varphi(n)} \xrightarrow{\delta(n)} H^1(K[n], T/I_n T)^{\varphi(n)} \xrightarrow{\kappa_n} H^1(K, T/I_n T),\]
where \(\delta(n)\) is induced by the limit of Kummer maps \(\delta(n) : E(K[n]) \otimes \mathbb{Z}_p \to H^1(K[n], T)\), 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 \(\kappa_n\) land in \(H^1_{\mathcal{F}_\Lambda}(K, T)\) and can be modified to a system \(\kappa_H^1 = \{\kappa_H^1\}_{n \in \mathbb{N}}\) 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 \(\varphi(p)\)) apply almost verbatim in the case when \(p\) divides the class number of \(K\). Finally, that \(\kappa_H^1\) is nonzero follows from Cornut–Vatsal [Cor02, Vat03].

**Remark 4.1.2.** For our later use, we compare the \(\Lambda\)-adic class \(\kappa_1^H \in H^1_{\mathcal{F}_\Lambda}(K, T)\) from Theorem 4.1.1 with the \(\Lambda\)-adic class constructed in [CH18, §5.2] (taking for \(f\) the newform associated with \(E\)). We assume that \(p\) splits in \(K\), although the comparison could also be made in the other cases.

Denote by \(\alpha\) the \(p\)-adic unit root of \(x^2 - a_p x + p\). With the notations introduced in the proof of Theorem 4.1.1, define the \(\alpha\)-stabilized Heegner point \(P[p^k]_{\alpha} \in E(K[p^k]) \otimes \mathbb{Z}_p\) by
\[(4.3) \quad P[p^k]_{\alpha} := \begin{cases} P[p^k] - \alpha^{-1} P[p^{k-1}] & \text{if } k \geq 1, \\ u_K^{-1}(1 - \alpha^{-1} \sigma_p)(1 - \alpha^{-1} \sigma_p^*) P[1] & \text{if } k = 0. \end{cases}\]
Using the Heegner point norm relations, a straightforward calculation shows that the points \(\alpha^{-k} P[p^k]_{\alpha}\) are norm-compatible, and letting \(\delta : E(K[p^k]) \otimes \mathbb{Z}_p \to H^1(K[p^k], T)\) be the Kummer map, one sets
\[\kappa_\infty := \lim_{\kappa} \delta(\kappa_k) \in \lim_{\kappa} H^1(K, T) \simeq H^1(K, T),\]
where \(\kappa_k = \alpha^{-d(k)} \text{Norm}_{K[p^d(k)]/K[p^k]}(P[p^{d(k)}]_{\alpha})\). The inclusion \(\kappa_\infty \in H^1_{\mathcal{F}_\Lambda}(K, T)\) follows immediately from the construction. For the comparison with \(\kappa_1^H\), note that by (4.2) the projection of \(\text{pr}_K(\kappa_1^H)\) of \(\kappa_1^H\) to \(H^1(K, T)\) is given by the Kummer image of \(\text{Norm}_{K[1]/K}(Q_0[1])\), while \(\kappa_0\) is the Kummer image of \(\text{Norm}_{K[1]/K}(P[1])\). Thus comparing (4.1) and (4.3) we see that
\[(4.4) \quad \text{pr}_K(\kappa_1^H) = u_K \alpha^2(1 - \beta)^2 \cdot \kappa_0,\]
where \(\beta = p \alpha^{-1}\). Since hypothesis (disc) implies \(u_K = 1\), this shows that \(\kappa_\infty\) and \(\kappa_1^H\) generate the same \(\Lambda\)-submodule of \(H^1_{\mathcal{F}_\Lambda}(K, T)\).

**4.2. Proof of the Iwasawa main conjectures.** Let \(\kappa_\infty \in H^1_{\mathcal{F}_\Lambda}(K, T)\) be the \(\Lambda\)-adic Heegner class introduced in Remark 4.1.2.

**Proposition 4.2.1.** Assume that \(p = \varphi(p)\) splits in \(K\) and that \(E(K)[p] = 0\), and let \(\Lambda'\) denote either \(\Lambda\) or \(\Lambda[1/p]\). Then the following statements are equivalent:
(i) Both $H^1_{\mathcal{F}_\Lambda}(K, T)$ and $H^1_{\mathcal{F}_\Lambda}(K, M_E)$ have $\Lambda$-rank one, and the divisibility
\[ \text{char}_\Lambda(H^1_{\mathcal{F}_\Lambda}(K, M_E)_{\text{tors}}) \supset \text{char}_\Lambda(H^1_{\mathcal{F}_\Lambda}(K, T)/\Lambda\kappa_\infty)^2 \]
holds in $\Lambda'$.
(ii) Both $\mathcal{S}_E$ and $\mathcal{X}_E$ are $\Lambda$-torsion, and the divisibility
\[ \text{char}_\Lambda(\mathcal{X}_E)\Lambda^{\text{ur}} \supset (\mathcal{L}_E)^2 \]
holds in $\Lambda'\otimes_{\mathbb{Z}_p} \mathbb{Z}_p^{ur}$
Moreover, the same result holds for the opposite divisibilities.

Proof. See [BCK19, Thm. 4.4], whose proof still applies after inverting $p$. \qed

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

Theorem 4.2.2. Assume that $K$ satisfies hypotheses (Heeg), (spl), and (disc), and that
- $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ as $G_{\mathbb{Q}}$-modules, with $\phi|_{G_p} \neq 1, \omega$.
- $E$ does not have CM by $K$.

Then $\mathcal{X}_E$ is $\Lambda$-torsion, and
\[ \text{char}_\Lambda(\mathcal{X}_E)\Lambda^{\text{ur}} = (\mathcal{L}_E) \]
as ideals in $\Lambda^{\text{ur}}$.

Proof. By Theorem 4.1.1, we can apply Theorem 3.4.1 with $\kappa = \kappa^{Hg}$, and so the modules $H^1_{\mathcal{F}_\Lambda}(K, T)$ and $H^1_{\mathcal{F}_\Lambda}(K, M_E)_{\text{tors}}^{\vee}$ have both $\Lambda$-rank one, with
\[ \text{char}_\Lambda(H^1_{\mathcal{F}_\Lambda}(K, M_E)_{\text{tors}}^{\vee}) \supset \text{char}_\Lambda(H^1_{\mathcal{F}_\Lambda}(K, T)/\Lambda\kappa_1^{Hg})^2 \]
as ideals in $\Lambda[1/p]$. Since by Remark 4.1.2 the classes $\kappa_1^{Hg}$ and $\kappa_\infty$ the generate the same $\Lambda$-submodule of $H^1_{\mathcal{F}_\Lambda}(K, T)$ (possibly up to powers of $p$), by Proposition 4.2.1, it follows that $\mathcal{X}_E$ is $\Lambda$-torsion (under the above hypotheses on $\phi$, this also follows independently by Proposition 1.4.2), with
\[ \text{char}_\Lambda(\mathcal{X}_E)\Lambda^{\text{ur}} \supset (\mathcal{L}_E) \]
as ideals in $\Lambda^{\text{ur}}[1/p]$. This divisibility, together with the equalities $\lambda(\mathcal{X}_E) = \lambda(\mathcal{L}_E) = 0$ and $\lambda(\mathcal{X}_E) = \lambda(\mathcal{L}_E)$ in Theorem 2.2.3, yields the result. \qed

As a consequence, we can also deduce the first cases of Perrin-Riou’s Heegner point main conjecture [PR87] in the non-CM residually reducible case (i.e., Corollary D in the introduction).

Corollary 4.2.3. Assume that $K$ satisfies hypotheses (Heeg), (spl), and (disc), and that
- $E[p]^{ss} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ as $G_{\mathbb{Q}}$-modules, with $\phi|_{G_p} \neq 1, \omega$.
- $E$ does not have CM by $K$.

Then both $H^1_{\mathcal{F}_\Lambda}(K, T)$ and $H^1_{\mathcal{F}_\Lambda}(K, M_E)_{\text{tors}}^{\vee}$ have $\Lambda$-rank one, and
\[ \text{char}_\Lambda(H^1_{\mathcal{F}_\Lambda}(K, M_E)_{\text{tors}}^{\vee}) = \text{char}_\Lambda(H^1_{\mathcal{F}_\Lambda}(K, T)/\Lambda\kappa_\infty)^2 \]
as ideals in $\Lambda$.

Proof. Everything except one of the divisibilities of the characteristic ideals has been shown in Theorem 3.4.1; the missing divisibility now follows from Theorem 4.2.2 together with Proposition 4.2.1. \qed

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 B and C in the introduction from our main Theorem 4.2.2.
5.1.1. Anticyclotomic control theorem. As in [JSW17, §2.2.3], define the anticyclotomic Selmer group of $W = E[p^\infty]$ by

$$H^1_{F_w}(K, W) = \ker \left\{ H^1(K^\Sigma/K, W) \to \prod_{w \in S} H^1(K_w, W) \times \frac{H^1(K_w, W)}{H^1(K_w, W)_{\text{div}}} \times H^1(K_v, W) \right\},$$

where $H^1(K_v, W)_{\text{div}} \subset H^1(K_v, W)$ is the maximal divisible submodule.

**Lemma 5.1.1.** Assume that $\text{rank}_E H(K) = 1$ and $\# \Sigma(E/K)[p^\infty] < \infty$. Then $\# H^1_{F,w}(K, W) < \infty$.

**Proof.** This follows from [Ski19, Lem. 2.3.2].

**Proposition 5.1.2.** Assume that $E(K)[p] = 0$. Then the natural map $W \to M_E$ induces an injection

$$H^1_{F_w}(K, W) \hookrightarrow H^1_{\text{co}(E_p)}(K, M_E)[\gamma - 1]$$

with finite cokernel.

**Proof.** By the assumption, the cohomology long exact sequence for $0 \to W \to M_E \to W \to 0$ yields an identification $H^1(K^\Sigma/K, W) = H^1(K^\Sigma/K, M_E)[\gamma - 1]$. Similarly taking cohomology for the local Galois groups we thus obtain the commutative diagram

$$\begin{array}{ccc}
H^1(K^\Sigma/K, W) & \to & H^1(K^\Sigma/K, M_E)[\gamma - 1] \\
\downarrow & & \downarrow \\
0 & \to & \prod_w M^{G_w}_{E}(\gamma - 1)M^{G_w}_{E} \xrightarrow{\gamma - 1} \prod_w H^1(K_w, W) \to \prod_w H^1(K_w, M_E)[\gamma - 1],
\end{array}$$

where the vertical arrows are given by restriction maps over all primes $w \in \Sigma$. As shown in the proof of [JSW17, Prop. 3.3.7], each of the above terms $M^{G_w}_{E}(\gamma - 1)M^{G_w}_{E}$ is finite, and hence the snake lemma applied to this diagram yields the result. 

The index appearing in Proposition 5.1.2 can be explicitly computed (if $E(\mathbb{Q}_p)[p] = 0$, it is given by the product of the $p$-part of the Tamagawa numbers of $E/K_w$ over the primes $w|N$); this computation is one of the steps in the following “anticyclotomic control theorem” from [JSW17], which we simply state in the form that will be needed as one of the ingredients in the proof of Theorem C.

**Theorem 5.1.3.** Assume that

- $E(K)[p] = 0$,
- $\text{rank}_E H(K) = 1$,
- $\# \Sigma(E/K)[p^\infty] < \infty$.

Then $x_E$ is a torsion $\Lambda$-module, and letting $F_E \in \Lambda$ be a generator of $\text{char}_\Lambda(x_E)$, we have

$$\# \mathbb{Z}_p/F_E(0) = \# \Sigma(E/K)[p^\infty] \cdot \left( \frac{[\mathbb{Z}_p/(1 - \omega_p + P)] \cdot \log_{\omega_p} P}{[E(K) : \mathbb{Z}, P]_p} \right)^2 \cdot \prod_{w \in S} c_w(E/K)_p,$$

where

- $P \in E(K)$ is any point of infinite order,
- $\log_{\omega_p} : E(K)_p/\text{tors} \to \mathbb{Z}_p$ is the formal group logarithm associated to a Néron differential $\omega_E$,
- $[E(K) : \mathbb{Z}, P]_p$ denotes the $p$-part of the index $[E(K) : \mathbb{Z}, P]$,
- $c_w(E/K)_p$ 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 $E(K)[p] = 0$. 

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 $x_1 = [C/\mathcal{O}_K \to C/\mathfrak{N}^{-1}] \in X_0(N)$ be the Heegner point of conductor 1 on $X_0(N)$, which is defined over the Hilbert class field $H_1/K$, and set

$$P_K = \sum_{\sigma \in \text{Gal}(H_1/K)} \pi(x_1)^\sigma \in E(K).$$

Let $f \in S_2(\Gamma_0(N))$ be the newform associated with $f$, 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 $\omega_E$ 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 5.1.4.** 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 $u_K = \#(\mathcal{O}_K^\times/\{\pm 1\})$, $D_K < 0$ is the discriminant of $K$, $\hat{h}(P_K)$ is the canonical height of $P_K$, and $\|\omega_E\|^2 = \int_{E(\mathbb{Q})} |\omega_E \wedge \omega_E|$. 

**Proof.** This is [GZ86, Thm. V.2.1].

**Theorem 5.1.5.** 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

$$L_E(0) = c_E^{-2} \cdot (1 - a_p^p - 1)^2 \cdot \log_{\omega_E}(P_K)^2,$$

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

**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 $k = 2$, $r = 0$, and $\chi = \mathbb{N}_{K}^{-1}$, we have

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

where $\log_{\omega_f} : J_0(N)(H_v) \to H_v$ is the formal group logarithm associated to $\omega_f$. 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 5.1.6.** 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 $\Phi_A$, with the $G_\mathbb{Q}$-action on $\Phi_A$ 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

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

where $\text{Tam}(A/\mathbb{Q})$ is the product of the Tamagawa numbers of $A/Q_\ell$ over the bad primes $\ell$ of $A$.

**Proof.** By [Kol88], if $L(A, 1) \neq 0$ then $\text{rank}_2 A(\mathbb{Q}) = 0$ and $\#\text{III}(A/\mathbb{Q}) < \infty$; in particular, $\#\text{Sel}_{p\infty}(A/\mathbb{Q}) = \#\text{III}(A/\mathbb{Q})[p^\infty] < \infty$. Letting $\Lambda_{\text{cyc}} = \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p/\mathbb{Q})]$ be the cyclotomic Iwasawa algebra, by [Gre99, Thm. 4.1] we therefore have

$$\text{(5.1)} \quad \#\mathbb{Z}_p / F_A(0) = \frac{\#(\mathbb{Z}_p/(1 - a_p^p A + p^2) \cdot \#\text{III}(A/\mathbb{Q}) \cdot \text{Tam}(A/\mathbb{Q}))}{\#(\mathbb{Z}_p/(A/Q)_{\text{tors}}^2)},$$

where $F_A \in \Lambda_{\text{cyc}}$ is a generator of the characteristic ideal of the dual Selmer group $\text{Sel}_{Q_\infty}(T_p A, T_p^+ A)^\vee$ in the notations of [SU14, §3.6.1]. Under the given assumptions, the cyclotomic main conjecture for $A$, i.e., the equality

$$\text{(5.2)} \quad (F_A) = (L_A) \subset \Lambda_{\text{cyc}}$$
where $L_A$ 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 $L_A$,

\begin{equation}
L_A(0) = (1 - \alpha_p^{-1})^2 \cdot \frac{L(A,1)}{\Omega_A},
\end{equation}

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

5.2. Proof of the $p$-converse. The following is Theorem E in the introduction.

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

\begin{equation}
\text{rank}_2E(\mathbb{Q}) = 1 \quad \#\text{III}(E/\mathbb{Q})[p^\infty] < \infty \quad \implies \quad \text{ord}_{s=1}L(E,s) = 1.
\end{equation}

**Proof.** Suppose $\text{rank}_2E(\mathbb{Q}) = 1$ and $\#\text{III}(E/\mathbb{Q})[p^\infty] < \infty$, and choose an imaginary quadratic field $K$ of discriminant $D_K$ such that

- (a) $D_K < -4$ is odd,
- (b) every prime $\ell$ dividing $N$ splits in $K$,
- (c) $p$ splits in $K$, say $p = \nu \overline{\nu}$,
- (d) $L(E^K,1) \neq 0$,
- (e) $E$ does not have CM by $K$.

The existence of such $K$ (in fact, of an infinitude of them) is ensured by [FH95, Thm. B], 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 $\text{rank}_2E^K(\mathbb{Q}) = 0$ and $\#\text{III}(E^K/\mathbb{Q}) < \infty$, and therefore we have

$$\text{rank}_2E(K) = 1 \quad \text{and} \quad \#\text{III}(E/K)[p^\infty] < \infty.$$ 

By Lemma 5.1.1, it follows that $\#H^1_{\text{reg}}(K,E[p^\infty]) < \infty$, and since our hypotheses on $\phi$ imply that $E(K)[p] = 0$, by Proposition 5.1.2 we conclude that $H^1_{\text{reg}}(K,M_E)[\gamma - 1]$ is also finite. Hence

$$\#(\mathcal{X}_E/(\gamma - 1)\mathcal{X}_E) < \infty,$$

or equivalently, $\mathcal{F}_E(0) \neq 0$, where $\mathcal{F}_E \in \Lambda = \mathbb{Z}_p[[T]]$ is any generator of $\text{char}_\Lambda(\mathcal{X}_E)$. By Theorem 4.2.2, this shows that $L_E(0) \neq 0$, and hence the Heegner point $P_K$ is non-torsion by Theorem 5.1.5. By Theorem 5.1.4, it follows that $\text{ord}_{s=1}L(E/K,s) = 1$, from which we conclude that $\text{ord}_{s=1}L(E/\mathbb{Q},s) = 1$ by our choice of $K$.

As mentioned in the introduction, with a similar argument can prove the following stronger version of Theorem 5.2.1 (building on Corollary 4.2.3 rather than Theorem 4.2.2).

**Corollary 5.2.2.** Assume that $E[p]^\text{sa} = \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$ with $\phi|_{G_p} \neq 1, \omega$. Then

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

In particular, $\text{rank}_2E(\mathbb{Q}) = 1$ and $\#\text{III}(E/\mathbb{Q}) < \infty$.

**Proof.** Choosing an auxiliary $K$ as in the proof of Theorem 5.2.1, we obtain $\text{corank}_{\mathbb{Z}_p}\text{Sel}_{p^\infty}(E/K) = 1$. By Corollary D, this easily implies that the Heegner point $P_K$ is non-torsion (see [Wan14, Thm. 3.17]), from where the conclusion that $\text{ord}_{s=1}L(E,s) = 1$ follows immediately by Theorem 5.1.4.

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

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


If ord\(_s=1 L(E, s) = 1\), then
\[
\text{ord}_p \left( \frac{L'(E, 1)}{\text{Reg}(E/\mathbb{Q}) \cdot \Omega_E} \right) = \text{ord}_p \left( \# \mathcal{III}(E/\mathbb{Q}) \prod_{\ell \mid \infty} c_\ell(E/\mathbb{Q}) \right).
\]

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

**Proof.** We begin by noting that by Theorem 4.2.2, there is a \(p\)-adic unit \(u \in (\mathbb{Z}_p^\times)^\times\) for which
\[
(5.4) \quad \mathcal{F}_E(0) = u \cdot \mathcal{L}_E(0),
\]
where \(\mathcal{F}_E \in \Lambda\) is a generator of \(\text{char}(\mathfrak{A}_E)\). Now suppose \(\text{ord}_s=1 L(E, s) = 1\), and as in the proof of Theorem 5.2.1 choose an imaginary quadratic field \(K\) of discriminant \(D_K\) such that

(a) \(D_K < -4\) is odd,
(b) every prime \(\ell\) dividing \(N\) splits in \(K\),
(c) \(p\) splits in \(K\), say \(p = \overline{v}\),
(d) \(L(E^K, 1) \neq 0\),
(e) \(E\) does not have CM by \(K\).

Then \(\text{ord}_s=1 L(E/K, s) = 1\), which by Theorem 5.1.4 implies that the Heegner point \(P_K \in E(K)\) has infinite order, and therefore \(\text{rank}_E(E(K)) = 1\) and \(\# \mathcal{III}(E/K) < \infty\) by [Kol88]. The hypotheses on \(\phi\) imply that \(E(K)[p] = 0\), and therefore Theorem 5.1.3 applies with \(P = P_K\), which combined with Theorem 5.1.5 and the relation (4.4) reduces (5.4) to the equality
\[
(5.5) \quad \text{ord}_p(\# \mathcal{III}(E/K)) = 2 \text{ord}_p(c_E^{-1} u_K^{-1} \cdot [E(K) : \mathbb{Z}.P_K]) - \sum_{w \in S} \text{ord}_p(c_w(E/K)),
\]

On the other hand, possibly up to a factor of 2 (given by the number of connected components \([E(\mathbb{R}) : E(\mathbb{R})^0]\)), the Gross–Zagier formula of Theorem 5.1.4 can be rewritten as
\[
L'(E, 1) = c_E^{-2} u_K^{-2} \cdot \hat{h}(P_K) \cdot \Omega_E \cdot E^K,
\]
which together with the relations \(L(E/K, s) = L(E, s) \cdot L(E^K, s)\) and
\[
\hat{h}(P_K) = [E(K) : \mathbb{Z}.P_K]^2 \cdot \text{Reg}(E/K) = [E(K) : \mathbb{Z}.P_K]^2 \cdot \text{Reg}(E/\mathbb{Q}),
\]
using that \(\text{rank}_E(E^K(\mathbb{Q})) = 0\) for the last equality, amounts to the formula
\[
(5.6) \quad \frac{L'(E, 1)}{\text{Reg}(E/\mathbb{Q}) \cdot \Omega_E} \cdot \frac{L(E^K, 1)}{\Omega_E} = c_E^{-2} u_K^{-2} \cdot [E(K) : \mathbb{Z}.P_K]^2.
\]
Note that \(u_K = 1\), since \(D_K < -4\). Since \(\mathcal{III}(E/K) \simeq \mathcal{III}(E/\mathbb{Q}) \oplus \mathcal{III}(E^K/\mathbb{Q})\) and
\[
\sum_{w \mid \ell} \text{ord}_p(c_w(E/K)) = \text{ord}_p(c_\ell(E/\mathbb{Q})) + \text{ord}_p(c_\ell(E^K/\mathbb{Q}))
\]
for any prime \(\ell\) (see [SZ14, Cor. 9.2]), combining (5.5) and (5.6) we arrive at
\[
\text{ord}_p \left( \frac{L'(E, 1)}{\text{Reg}(E/\mathbb{Q}) \cdot \Omega_E \cdot \prod_{\ell} c_\ell(E/\mathbb{Q})} \right) = \text{ord}_p(\# \mathcal{III}(E/\mathbb{Q})),
\]
\[
(5.7) \quad \text{ord}_p \left( \frac{L(E^K, 1)}{\Omega_E \cdot \prod_{\ell} c_\ell(E^K/\mathbb{Q})} \right) = \text{ord}_p(\# \mathcal{III}(E^K/\mathbb{Q})).
\]
Finally, by our hypotheses on \(\phi\) the curve \(E^K\) satisfies the hypotheses of Theorem 5.1.6, and hence the right-hand side of (5.7) vanishes, concluding the proof of Theorem 5.3.1.

### References


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

(G. Grossi) University College London, Gower street, WC1E 6BT, London, UK  
*Email address*: giada.grossi.16@ucl.ac.uk

(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