ON THE $p$-PART OF THE BIRCH–SWINNERTON-DYER FORMULA FOR
MULTIPLICATIVE PRIMES

FRANCESC CASTELLA

Abstract. Let $E/\mathbb{Q}$ be a semistable elliptic curve of analytic rank one, and let $p > 3$ be a
prime for which $E[p]$ is irreducible. In this note, following a slight modification of the methods
of [JSW15], we use Iwasawa theory to establish the $p$-part of the Birch and Swinnerton-Dyer
formula for $E$. In particular, we extend the main result of loc.cit. to primes of multiplicative
reduction.

Contents
1. Introduction 1
2. Selmer groups 3
3. A $p$-adic Waldspurger formula 8
4. Main Conjectures 10
5. Proof of Theorem A 12
References 14

1. Introduction

Let $E/\mathbb{Q}$ be a semistable elliptic curve of conductor $N$, and let $L(E, s)$ be the Hasse–Weil
$L$-function of $E$. By the celebrated work of Wiles [Wil95] and Taylor–Wiles [TW95], $L(E, s)$ is
known to admit analytic continuation to the entire complex plane, and to satisfy a functional
equation relating its values at $s$ and $2 - s$. The purpose of this note is to prove the following
result towards the Birch and Swinnerton-Dyer formula for $E$.

Theorem A. Let $E/\mathbb{Q}$ be a semistable elliptic curve of conductor $N$ with $\text{ord}_{s=1} L(E, s) = 1$,
and let $p > 3$ be a prime such that the mod $p$ Galois representation

$$\bar{\rho}_{E,p} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}_{\mathbb{F}_p}(E[p])$$

is irreducible. If $p \mid N$, assume in addition that $E[p]$ is ramified at some prime $q \neq p$. Then

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

where

- $\text{Reg}(E/\mathbb{Q})$ is the discriminant of the Néron–Tate height pairing on $E(\mathbb{Q}) \otimes \mathbb{R}$;
- $\Omega_E$ is the Néron period of $E$;
- $\Sha(E/\mathbb{Q})$ is the Tate–Shafarevich group of $E$; and
- $c_\ell(E/\mathbb{Q})$ is the Tamagawa number of $E$ at the prime $\ell$.

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

2010 Mathematics Subject Classification. 11R23 (primary); 11G05, 11G40 (secondary).

This project has received funding from the European Research Council (ERC) under the European Union’s
Horizon 2020 research and innovation programme (grant agreement No. 682152).
Remark. Having square-free conductor, any elliptic curve $E/Q$ as in Theorem A is necessarily non-CM. By [Ser72 Thm. 2], if follows that $\rho_{E,p}$ is in fact surjective for all but finitely many primes $p$; by [Maz78 Thm. 4], this holds as soon as $p \geq 11$.

When $p$ is a prime of good reduction for $E$, Theorem A (in the stated level of generality) was first established by Jetchev–Skinner–Wan [JSW15]. (We should note that [JSW15 Thm. 1.2.1] also allows $p = 3$ provided $E$ has good supersingular reduction at $p$, the assumption $a_3(E) = 0$ having been removed in a recent work by Sprung; see [Spr16 Cor. 1.3].) For primes $p \nmid N$, some particular cases of Theorem A are contained in the work of Skinner–Zhang (see [SZ14 Thm. 1.1]) under further hypotheses on $N$ and, in the case of split multiplicative reduction, on the $L$-invariant of $E$. Thus the main novelty in Theorem A is for primes $p \mid N$.

Similarly as in [JSW15], our proof of Theorem A uses anticyclotomic Iwasawa theory. In order to clarify the relation between the arguments in loc. cit. and the arguments in this paper, let us recall that the proof of [JSW15 Thm. 1.2.1] (for primes $p \nmid N$) is naturally divided into two steps:

1. **Exact lower bound on the predicted order of $\Sha(E/Q)[p^\infty]$**. For this part of the argument, in [JSW15] one chooses a suitable imaginary quadratic field $K_1 = Q(\sqrt{-d_1})$ with $L(E^{D_1}, 1) \neq 0$; combined with the hypothesis that $E$ has analytic rank one, it follows that $E(K_1)$ has rank one and that $\#\Sha(E/K_1) < \infty$ by the work of Gross–Zagier and Kolyvagin. The lower bound

$$\text{ord}_p(\#\Sha(E/K_1)[p^\infty]) \geq 2 \cdot \text{ord}_p([E(K_1) : \mathbb{Z}P_{K_1}]) - \sum_{w|N^+ [w \text{ split}]} \text{ord}_p(c_w(E/K_1)),$$

where $P_{K_1} \in E(K_1)$ is a Heegner point, $c_w(E/K_1)$ is the Tamagawa number of $E/K_1$ at $w$, and $N^+$ is the product of the prime factors of $N$ that are either split or ramified in $K_1$, is then established by combining:

1.a A Mazur control theorem proved “à la Greenberg” [Gre99] for an anticyclotomic Selmer group $X_{ac}(E[p^\infty])$ attached to $E/K_1$ ([JSW15 Thm. 3.3.1]);

1.b The proof by Xin Wan [Wan14a, Wan14b] of one of the divisibilities predicted by the Iwasawa–Greenberg Main Conjecture for $X_{ac}(E[p^\infty])$, namely the divisibility

$$\text{Ch}_\Lambda(X_{ac}(E[p^\infty]))\Lambda_{R_0} \subseteq (L_p(f))$$

where $f = \sum_{n=1}^{\infty} a_n q^n$ is the weight 2 newform associated with $E$, $\Lambda_{R_0}$ is a scalar extension of the anticyclotomic Iwasawa algebra $\Lambda$ for $K_1$, and $L_p(f) \in \Lambda_R$ is a certain anticyclotomic $p$-adic $L$-function;

1.c The “$p$-adic Waldspurger formula” of Bertolini–Darmon–Prasanna [BDP13] (as extended by Brooks [HB15] to indefinite Shimura curves):

$$L_p(f, 1) = (1 - a_p p^{-1} + p^{-1})^2 \cdot (\log_{\omega_{E}} P_{K_1})^2$$

relating the value of $L_p(f)$ at the trivial character to the formal group logarithm of the Heegner point $P_{K_1}$.

When combined with the known $p$-part of the Birch and Swinnerton-Dyer formula for the quadratic twist $E^{D_1}/Q$ (being of rank analytic zero, this follows from [SU14 and Wan14c]), inequality (1.1) easily yields the exact lower bound for $\#\Sha(E/Q)[p^\infty]$ predicted by the BSD conjecture.

2. **Exact upper bound on the predicted order of $\Sha(E/Q)[p^\infty]$**. For this second part of the argument, in [JSW15] one chooses another imaginary quadratic field $K_2 = Q(\sqrt{-d_2})$ (in general different from $K_1$) such that $L(E^{D_2}, 1) \neq 0$. Crucially, $K_2$ is chosen so that the associated $N^+$ (the product of the prime factors of $N$ that are split or ramified
in $K_2$) is as small as possible in a certain sense; this ensures optimality of the upper bound provided by Kolyvagin’s methods:

$$\text{ord}_p(\#\text{II}(E/K_2)[p^\infty]) \leq 2 \cdot \text{ord}([E(K_2) : \mathbb{Z} \cdot P_{K_2}]),$$

where $P_{K_2} \in E(K_2)$ is a Heegner point coming from a parametrization of $E$ by a Shimura curve attached to an indefinite quaternion algebra (which is non-split unless $N$ is prime). Combined with the general Gross–Zagier formula [YZZ13] and the $p$-part of the Birch and Swinnerton-Dyer formula for $E^{2g}/\mathbb{Q}$, inequality (1.2) then yields the predicted optimal upper bound for $\#\text{II}(E/\mathbb{Q})[p^\infty]$.

Our proof of Theorem A dispenses with part (2) of the above argument; in particular, it only requires the use of classical modular parametrizations of $E$. Indeed, if $K$ is an imaginary quadratic field satisfying the following hypotheses relative to the square-free integer $N$:

- every prime factor of $N$ is either split or ramified in $K$;
- there is at least one prime $q \mid N$ nonsplit in $K$;
- $p$ splits in $K$,

in [Cas17a] (for good ordinary $p$) and [CW16] (for good supersingular $p$) we have completed under mild hypotheses the proof of the Iwasawa–Greenberg main conjecture for the associated $X_{ac}(E[p^\infty])$:

$$\text{Ch}_{\Lambda}(X_{ac}(E[p^\infty])) \Lambda_{R_0} = (L_p(f)).$$

With this result at hand, a simplified form (since $N^* = 1$ here) of the arguments from [JSW15] in part (1) above lead to an equality in [111] taking $K_1 = K$, and so to the predicted order of $\text{III}(E/\mathbb{Q})[p^\infty]$ when $p \nmid N$.

To treat the primes $p \mid N$ of multiplicative reduction for $E$ (which, as already noted, is the only new content of Theorem A), we use Hida theory. Indeed, if $a_p$ is the $U_p$-eigenvalue of $f$ for such $p$, we know that $a_p \in \{\pm 1\}$, so in particular $f$ is ordinary at $p$. Let $f \in \mathcal{I}[[q]]$ be the Hida family associated with $f$, where $\mathcal{I}$ is a certain finite flat extension of the one-variable Iwasawa algebra. In Section 11 we deduce from [Cas17a] and [Wan14a] a proof of a two-variable analog of the Iwasawa–Greenberg main conjecture [123] over the Hida family:

$$\text{Ch}_{\Lambda_f}(X_{ac}(A_f)) \Lambda_{\mathcal{I},R_0} = (L_p(f)),$$

where $L_p(f) \in \Lambda_{\mathcal{I},R_0}$ is the two-variable anticyclotomic $p$-adic $L$-function introduced in [Cas14]. By construction, $L_p(f)$ specializes to $L_p(f)$ in weight 2, and by a control theorem for the Hida variable, the characteristic ideal of $X_{ac}(A_f)$ similarly specializes to $\text{Ch}_{\Lambda}(X_{ac}(E[p^\infty]))$, yielding a proof of the Iwasawa–Greenberg main conjecture [133] in the multiplicative reduction case. Combined with the anticyclotomic control theorem of (1.a) and the natural generalization (contained in [Cas17a]) of the $p$-adic Waldspurger formula in (1.c) to this case:

$$L_p(f, 1) = (1 - a_p p^{-1})^2 \cdot (\log_{\omega_E} P_K)^2,$$

we arrive at the predicted formula for $\#\text{III}(E/\mathbb{Q})[p^\infty]$ just as in the good reduction case.

Acknowledgements. As will be clear to the reader, this note borrows many ideas and arguments from [JSW15]. It is a pleasure to thank Chris Skinner for several useful conversations.

2. Selmer groups

2.1. Definitions. Let $E/\mathbb{Q}$ be a semistable elliptic curve of conductor $N$, and let $p \geq 5$ be a prime such that the mod $p$ Galois representations

$$\tilde{\rho}_{E,p} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut}_{\mathbb{F}_p}(E[p])$$

is irreducible. Let $T = T_p(E)$ be the $p$-adic Tate module of $E$, and set $V = T \otimes \mathbb{Z}_p \mathbb{Q}_p$. 
Let $K$ be an imaginary quadratic field in which $p = \mathfrak{p} \mathfrak{P}$ splits, and for every place $w$ of $K$ define the anticyclotomic local condition $H^1_{\text{ac}}(K_w, V) \subseteq H^1(K_w, V)$ by

$$H^1_{\text{ac}}(K_w, V) := \left\{ \begin{array}{ll} H^1(K_{\mathfrak{p}}, V) & \text{if } w = \mathfrak{p}; \\
0 & \text{if } w = \mathfrak{p}; \\
H^1_{\text{ur}}(K_w, V) & \text{if } w \nmid p, \end{array} \right.$$ 

where $H^1_{\text{ur}}(K_w, V) := \ker\{H^1(K_w, V) \to H^1(I_w, V)\}$ is the unramified part of cohomology.

**Definition 2.1.** The anticyclotomic Selmer group for $E$ is

$$H^1_{\text{ac}}(K, E[p^\infty]) := \ker\left\{ H^1(K, E[p^\infty]) \to \prod_{w \mid p} H^1_{\text{ac}}(K_w, E[p^\infty]) \right\},$$

where $H^1_{\text{ac}}(K_w, E[p^\infty]) \subseteq H^1(K_w, E[p^\infty])$ is the image of $H^1_{\text{ac}}(K_w, V)$ under the natural map $H^1(K_w, V) \to H^1(K_w, E[p^\infty])$.

Let $\Gamma = \text{Gal}(K_\infty/K)$ be the Galois group of the anticyclotomic $\mathbf{Z}_p$-extension of $K$, and let $\Lambda = \mathbf{Z}_p[\Gamma]$ be the anticyclotomic Iwasawa algebra. Consider the $\Lambda$-module

$$M := T \otimes_{\mathbf{Z}_p} \Lambda^\ast,$$

where $\Lambda^\ast = \text{Hom}_{\text{cont}}(\Lambda, \mathbf{Q}_p/\mathbf{Z}_p)$ is the Pontryagin dual of $\Lambda_{\text{ac}}$. Letting $\rho_{E,p}$ denote the natural action of $G_K := \text{Gal}(\overline{\mathbf{Q}}/K)$ on $T$, the $G_K$-action on $M$ is given by $\rho_{E,p} \otimes \Psi^{-1}$, where $\Psi$ is the composite character $G_K \to \Gamma \to \Lambda^\ast$.

**Definition 2.2.** The anticyclotomic Selmer group for $E$ over $K_\infty^\mathrm{ac}/K$ is defined by

$$\text{Sel}_p(K_\infty, E[p^\infty]) := \ker\left\{ H^1(K, M) \to H^1(K_p, M) \oplus \prod_{w \mid p} H^1(K_w, M) \right\}.$$ 

More generally, for any given finite set $\Sigma$ of places $w \nmid p$ of $K$, define the “$\Sigma$-imprimitive” Selmer group $\text{Sel}_p^\Sigma(K_\infty, E[p^\infty])$ by dropping the summands $H^1(K_w, M)$ for the places $w \in \Sigma$ in the above definition. Set

$$X^\Sigma_{\text{ac}}(E[p^\infty]) := \text{Hom}_{\mathbf{Z}_p}(\text{Sel}_p^\Sigma(K_\infty, E[p^\infty]), \mathbf{Q}_p/\mathbf{Z}_p),$$

which is easily shown to be a finitely generated $\Lambda$-module.

2.2. Control theorems. Let $E$, $p$, and $K$ be as in the preceding section, and let $N^+$ denote the product of the prime factors of $N$ which are split in $K$.

**Anticyclotomic Control Theorem.** Denote by $\hat{E}$ the formal group of $E$, and let

$$\log_{\omega_E} : E(\mathbf{Q}_p) \to \mathbf{Z}_p$$

the formal group logarithm attached to a fixed invariant differential $\omega_E$ on $\hat{E}$. Letting $\gamma \in \Gamma$ be a fixed topological generator, we identify the one-variable power series ring $\mathbf{Z}_p[[T]]$ with the Iwasawa algebra $\Lambda = \mathbf{Z}_p[[\Gamma]]$ by sending $1 + T \mapsto \gamma$.

**Theorem 2.3.** Let $\Sigma$ be any set of places of $K$ not dividing $p$, and assume that $\text{rank}_\mathbf{Z}(E(K)) = 1$ and that $\#\Pi(E/K)[p^\infty] < \infty$. Then $X^\Sigma_{\text{ac}}(E[p^\infty])$ is $\Lambda$-torsion, and letting $f^\Sigma_{\text{ac}}(T) \in \Lambda$ be a generator of $\text{Ch}_\Lambda(X^\Sigma_{\text{ac}}(E[p^\infty]))$, we have

$$\#\mathbf{Z}_p/f^\Sigma_{\text{ac}}(0) = \#\Pi(E/K)[p^\infty] \cdot \frac{\#\mathbf{Z}_p/((1 - ap^{-1} + \varepsilon_p) \log_{\omega_E}(P))}{[E(K) \otimes \mathbf{Z}_p : \mathbf{Z}_p[P]]^2} \times \prod_{\mathbf{w}|N^+ \in \Sigma} c_w^{(p)}(E/K) \cdot \prod_{w \in \Sigma} \#H^1(K_w, E[p^\infty]),$$
where \(\varepsilon_p = p^{-1}\) if \(p \nmid N\) and \(\varepsilon_p = 0\) otherwise, \(P \in E(K)\) is any point of infinite order, and \(c_w^{(p)}(E/K)\) is the \(p\)-part of the Tamagawa number of \(E/K\) at \(w\).

Proof. As we are going to show, this follows easily from the “Anticyclotomic Control Theorem” established in [JSW15, §3.3]. The hypotheses imply that \(\text{corank}_{Z_p} \text{Sel}(K, E[p^\infty]) = 1\) and that the natural map

\[
E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow E(K_w) \otimes \mathbb{Q}_p/\mathbb{Z}_p
\]

is surjective for all \(w \mid p\). By [JSW15, Prop. 3.2.1] (see also the discussion in [loc.cit., p. 22]) it follows that \(H_{\ac}^1(K, E[p^\infty])\) is finite with

\[
\#H_{\ac}^1(K, E[p^\infty]) = \#\text{III}(E/K)[p^\infty] \cdot \frac{[E(K_p)/\text{tors} \otimes Z_p : Z_p, P]^2}{[E(K) \otimes Z_p : Z_p, P]^2},
\]

where \(E(K_p)/\text{tors}\) is the quotient \(E(K_p)\) by its maximal torsion submodule, and \(P \in E(K)\) is any point of infinite order. If \(p \nmid N\), then

\[
[E(K_p)/\text{tors} \otimes Z_p : Z_p, P] = \frac{\#Z_p/((1-a_p+p/p) \log_{\omega_E} P)}{\#H^0(K_p, E[p^\infty])}
\]

as shown in [JSW15, p. 23], and substituting (2.2) into (2.1) we arrive at

\[
\#H_{\ac}^1(K, E[p^\infty]) = \#\text{III}(E/K)[p^\infty] \cdot \left(\frac{\#Z_p/((1-a_p+p/p) \log_{\omega_E} P)}{[E(K) \otimes Z_p : Z_p, P] \cdot \#H^0(K_p, E[p^\infty])}\right)^2,
\]

from where the result follows immediately by [JSW15, Thm. 3.3.1].

Suppose now that \(p \mid N\). Let \(\hat{E}_{\text{ns}}(F_p)\) be the group on nonsingular points on the reduction of \(E\) modulo \(p\), \(E_0(K_p)\) be the inverse image of \(\hat{E}_{\text{ns}}(F_p)\) under the reduction map, and \(E_1(K_p)\) be defined by the exactness of the sequence

\[
0 \longrightarrow E_1(K_p) \longrightarrow E_0(K_p) \longrightarrow \hat{E}_{\text{ns}}(F_p) \longrightarrow 0.
\]

The formal group logarithm defines an injective homomorphism \(\log_{\omega_E} : E(K_p)/\text{tors} \otimes Z_p \rightarrow Z_p\) mapping \(E_1(K_p)\) isomorphically onto \(pZ_p\), and hence we see that

\[
[E(K_p)/\text{tors} \otimes Z_p : Z_p, P] = \frac{\#Z_p/((1-a_p+p/p) \log_{\omega_E} P) \cdot \#(E(K_p))/E_1(K_p) \otimes Z_p)}{\#Z_p/((1-a_p+p/p) \log_{\omega_E} P) \cdot \#(E_0(K_p))/E_1(K_p) \otimes Z_p)}.
\]

where the first equality follows from the same immediate calculation as in [JSW15, p. 23], and in the second equality \([E(K_p) : E_0(K_p)]_p\) denotes the \(p\)-part of the index \([E(K_p) : E_0(K_p)]\). By (2.3), we have \(E_1(K_p)/E_0(K_p) \otimes Z_p \simeq \hat{E}_{\text{ns}}(F_p) \otimes Z_p\), which is trivial by e.g. [Sil94, Prop. 5.1] (and \(p > 2\)). Since clearly \(E(K_p)/\text{tors} \otimes Z_p = H^0(K_p, E[p^\infty])\), we thus conclude that

\[
[E(K_p)/\text{tors} \otimes Z_p : Z_p, P] = [E(K_p) : E_0(K_p)]_p \cdot \frac{\#Z_p/((1-a_p+p/p) \log_{\omega_E} P)}{\#H^0(K_p, E[p^\infty])},
\]

and substituting (2.2) into (2.1) we arrive at

\[
H_{\ac}^1(K, E[p^\infty]) = \#\text{III}(E/K)[p^\infty] \cdot \left(\frac{[E(K_p) : E_0(K_p)]_p \cdot \#Z_p/((1-a_p+p/p) \log_{\omega_E} P)}{[E(K) \otimes Z_p : Z_p, P] \cdot \#H^0(K_p, E[p^\infty])}\right)^2.
\]
Plugging this formula for $H^1_{ac}(K, E[p]\infty)$ into [JSWI15] Thm. 3.3.1 yields the equality

$$\#Z_p/f_{ac}(0) = \#\text{III}(E/K)[p\infty] \cdot \left( \frac{\#Z_p/(\frac{1}{p} \log_{\infty} P)}{[E(K) \otimes Z_p : Z_p.P]} \right)^2 \cdot [E(K_p) : E_0(K_p)]^2_p \times \prod_{w \in S \setminus \Sigma} \prod_{w \mid p \text{ split}} \#H^1_{ur}(K_w, E[p\infty]) \cdot \prod_{w \in \Sigma} \#H^1(K_w, E[p\infty]),$$

(2.5)

where $S$ is any finite set of places of $K$ containing $\Sigma$ and the primes above $N$. Now, if $w \mid p$, then

$$[E(K_p) : E_0(K_p)]_p = c_{ur}^{(p)}(E/K)$$

by definition, while if $w \nmid p$, then

$$\#H^1_{ur}(K_w, E[p\infty]) = c_{ur}^{(p)}(E/K)$$

by [SZ14] Lem. 9.1. Since $c_{ur}^{(p)}(E/K) = 1$ unless $w \mid N$, substituting (2.6) and (2.7) into (2.5), the proof of Theorem 2.3 follows.

**Control Theorem for Greenberg Selmer groups.** Let $\Lambda_W = Z_p[[W]]$ be a one-variable power series ring. Let $M$ be an integer prime to $p$, let $\chi$ be a Dirichlet character modulo $pM$, and let

$$f = \sum_{n=1}^{\infty} a_n q^n \in \mathbb{Z}[q]$$

be an ordinary $p$-adic cusp eigenform of tame level $M$ and character $\chi$ (as defined in [SU11] §3.3.9) defined over a local reduced finite integral extension $\mathcal{O}/\Lambda_W$.

Let $X^n_{\phi}$ the set of continuous $Z_p$-algebra homomorphisms $\phi : \mathcal{O} \rightarrow \mathcal{O}_p$ whose composition with the structural map $\Lambda_W \rightarrow \mathcal{O}$ is given by $\phi(1 + W) = (1 + p)^{k_{\phi} - 2}$ for some integer $k_{\phi} \in \mathbb{Z}_{\geq 2}$ called the weight of $\phi$. Then for all $\phi \in X^n_{\phi}$ we have

$$f_{\phi} = \sum_{n=1}^{\infty} \phi(a_n) q^n \in S_{k_{\phi}}(\Gamma_0(pM), \chi \omega^{2-k_{\phi}}),$$

where $\omega$ is the Teichmüller character. In this paper will only consider the case where $\chi$ is the trivial character, in which case for all $\phi \in X^n_{\phi}$ of weight $k_{\phi} \equiv 2 \pmod{p-1}$, either

1. $f_{\phi}$ is a newform on $\Gamma_0(pM)$;
2. $f_{\phi}$ is the $p$-stabilization of a $p$-ordinary newform on $\Gamma_0(M)$.

As is well-known, for weights $k_{\phi} > 2$ only case (2) is possible; for $k_{\phi} = 2$ both cases occur.

Let $k_1 = \mathcal{O}/m_1$ be the residue field of $\mathcal{O}$, and assume that the residual Galois representation

$$\tilde{\rho}_f : G_{\mathcal{O}} := \text{Gal}(\overline{\mathbb{Q}}/\mathcal{O}) \rightarrow GL_2(k_{1})$$

attached to $f$ is irreducible. Then there exists a free $\mathcal{O}$-module $T_f$ of rank two equipped with a continuous $\mathcal{O}$-linear action of $G_{\mathcal{O}}$ such that, for all $\phi \in X^n_{\phi}$, there is a canonical $G_{\mathcal{O}}$-isomorphism

$$T_f \otimes \phi(\mathcal{O}) \simeq T_{f_{\phi}},$$

where $T_{f_{\phi}}$ is a $G_{\mathcal{O}}$-stable lattice in the Galois representation $V_{f_{\phi}}$ associated with $f_{\phi}$. (Here, $T_f$ corresponds to the Galois representation denoted $M(F)^*$ in [KLZ14] Def. 7.2.5; in particular, det$(V_{f_{\phi}})$ = $e^{k_{\phi} - 1}$, where $e : G_{\mathcal{O}} \rightarrow Z_p^\times$ is the $p$-adic cyclotomic character.)

Let $\Lambda_{\mathcal{O}} := \mathcal{O}[[\Gamma]]$ be the anticyclotomic Iwasawa algebra over $\mathcal{O}$, and consider the $\Lambda_{\mathcal{O}}$-module

$$M_f := T_f \otimes \Lambda^\oplus_\mathcal{O},$$

where $\Lambda^\oplus_\mathcal{O} = \text{Hom}_{cont}(\mathcal{O}, Q_p/\mathbb{Z}_p)$ is the Pontryagin dual of $\Lambda_{\mathcal{O}}$. This is equipped with a natural $G_{\mathcal{O}}$-action defined similarly as for the $\Lambda$-module $M = T \otimes \mathbb{Z}_p \Lambda^\oplus$ introduced in (2.1).
Definition 2.4. The Greenberg Selmer group of $E$ over $K_\infty/K$ is
\[ \mathfrak{Sel}_{Gr}(K_\infty, E[p^\infty]) := \ker \left\{ H^1(K, M) \to H^1(I_p, M) \oplus \prod_{w \nmid p} H^1(I_w, M) \right\}. \]

The Greenberg Selmer group $\mathfrak{Sel}_{Gr}(K_\infty, A_f)$ for $f$ over $K_\infty/K$, where $A_f := T_f \otimes \mathbb{I}^*$, is defined by replacing $M$ by $M_f$ in the above definition.

Similarly as for the anticyclotomic Selmer groups in (2.11) for any given finite set $\Sigma$ of places $w \nmid p$ of $K$, we define $\Sigma$-imprimitive Selmer groups $\mathfrak{Sel}_{Gr}^{\Sigma}(K_\infty, E[p^\infty])$ and $\mathfrak{Sel}_{Gr}^{\Sigma}(K_\infty, A_f)$ by dropping the summands $H^1(I_w, M)$ and $H^1(I_w, M_f)$, respectively, for the places $w \in \Sigma$ in the above definition. Let $X_{Gr}^\Sigma(E[p^\infty]) := \text{Hom}_{cont}(\mathfrak{Sel}_{Gr}^{\Sigma}(K_\infty, E[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p)$ be the Pontrjagin dual of $\mathfrak{Sel}_{Gr}^{\Sigma}(K_\infty, E[p^\infty])$, and define $X_{Gr}^\Sigma(A_f)$ similarly.

We will have use for the following comparison between the Selmer groups $\mathfrak{Sel}_{Gr}(K_\infty, E[p^\infty])$ and $\mathfrak{Sel}_{ac}(K_\infty, E[p^\infty])$. Note that directly from the definition we have an exact sequence
\[ 0 \to \mathfrak{Sel}_{ac}(K_\infty, E[p^\infty]) \to \mathfrak{Sel}_{Gr}(K_\infty, E[p^\infty]) \to \mathcal{H}_{ur}^{\Sigma} \oplus \prod_{w \nmid p} \mathcal{H}_{ur}^{w}, \]
where $\mathcal{H}_{ur}^{w} := \ker \left\{ H^1(K_w, M) \to H^1(I_w, M) \right\}$ is the set of unramified cocycles.

For a torsion $\Lambda$-module $X$, let $\lambda(X)$ (resp. $\mu(X)$) denote the $\lambda$-invariant (resp. $\mu$-invariant) of a generator of $\text{Ch}_\Lambda(X)$.

Proposition 2.5. Assume that $X_{Gr}^\Sigma(E[p^\infty])$ is $\Lambda$-torsion. Then $X_{ac}^\Sigma(E[p^\infty])$ is $\Lambda$-torsion, and we have the relations
\[ \lambda(X_{Gr}^\Sigma(E[p^\infty])) = \lambda(X_{ac}^\Sigma(E[p^\infty])), \]
and
\[ \mu(X_{Gr}^\Sigma(E[p^\infty])) = \mu(X_{ac}^\Sigma(E[p^\infty])) + \sum_{w \nmid p} \text{ord}_p(c_w(E/K)). \]

Proof. Since $X_{ac}^\Sigma(E[p^\infty])$ is a quotient of $X_{Gr}^\Sigma(E[p^\infty])$, the first claim of the proposition is clear. Also, note that $X_{Gr}^\Sigma(E[p^\infty])$ is $\Lambda$-torsion for some $\Sigma$ if and only if it is $\Lambda$-torsion for any finite set of primes $\Sigma$. Therefore to establish the claimed relations between Iwasawa invariants, it suffices to consider primitive Selmer groups, i.e. $\Sigma = \emptyset$.

For primes $v \nmid p$ which are split in $K$, it is easy to see that the restriction map $H^1(K_v, M) \to H^1(I_v, M)$ is injective (see [PW11, Rem. 3.1]), and so $\mathcal{H}_{ur}^{w}$ vanishes. Since $M_{I_p} = \{0\}$, the term $\mathcal{H}_{ur}^{w}$ also vanishes, and the exact sequence (2.8) thus reduces to
\[ 0 \to \mathfrak{Sel}_{ac}(K_\infty, E[p^\infty]) \to \mathfrak{Sel}_{Gr}(K_\infty, E[p^\infty]) \to \prod_{w \nmid p} \mathcal{H}_{ur}^{w}. \]

Now, a straightforward modification of the argument in [PW11, Lem. 3.4] shows that $\mathcal{H}_{ur}^{w} \simeq \left( \mathbb{Z}_p/p^{\text{v}(w)E(K)} \mathbb{Z}_p \right) \otimes \Lambda^*$, where $t_{E(w)} := \text{ord}_p(c_w(E/K))$ is the $p$-exponent of the Tamagawa number of $E$ at $w$, and $\Lambda^*$ is the Pontrjagin dual of $\Lambda$. In particular, $\mathcal{H}_{ur}^{w}$ is $\Lambda$-torsion, with $\lambda(\mathcal{H}_{ur}^{w}) = 0$ and $\mu(\mathcal{H}_{ur}^{w}) = \text{ord}_p(c_w(E/K))$. Since the rightmost arrow in (2.9) is surjective by [PW11, Prop. A.2], taking characteristic ideals in (2.9) the result follows. \qed

For the rest of this section, assume that $E$ has ordinary reduction at $p$, so that the associated newform $f \in S_2(\Gamma_0(N))$ is $p$-ordinary. Let $f \in \mathbb{I}[q]$ be the Hida family associated with $f$, let $\phi \subseteq \mathbb{I}$ be the kernel of the arithmetic map $\phi \in \Lambda_1^\*$ such that $f_\phi$ is either $f$ itself (if $p \nmid N$) or
the ordinary $p$-stabilization of $f$ (if $p \nmid N$), and set $\tilde{\varphi} := \varphi \Lambda_1 \subseteq \Lambda$. Since we assume that $\tilde{\rho}_{E,p}$ is irreducible, so is $\tilde{\rho}_f$.

**Theorem 2.6.** Let $S_p$ be the places of $K$ above $p$, and assume that $\Sigma \cup S_p$ contains all places of $K$ at which $T$ is ramified. Then there is a canonical isomorphism

$$X^\Sigma_{\text{Gr}}(E[p^\infty]) \simeq X^\Sigma_{\text{Gr}}(A_T)/\tilde{\varphi}X^\Sigma_{\text{Gr}}(A_T).$$

**Proof.** This follows from a slight variation of the arguments proving [SU14 Prop. 3.7] (see also [Och06 Prop. 5.1]). Since $M \simeq M_T[\tilde{\varphi}]$, by Pontrjagin duality it suffices to show that the canonical map

$$(2.10) \quad \text{Sel}^\Sigma_{\text{Gr}}(K, M_T[\varphi]) \longrightarrow \text{Sel}^\Sigma_{\text{Gr}}(K, M_T)[\tilde{\varphi}]$$

is an isomorphism. Note that our assumption on $S$ implies that

$$(2.11) \quad \text{Sel}^\Sigma_{\text{Gr}}(K, M_T) = \ker \left\{ H^1(G_{K,S}, M_T) \longrightarrow \frac{H^1(K_p, M_T)}{H^1_{\text{Gr}}(K_p, M_T)} \right\},$$

where $M_T = M_T[\varphi]$ or $M_T$, $G_{K,S}$ is the Galois group of the maximal extension of $K$ unramified outside $S$, and

$$H^1_{\text{Gr}}(K_p, M_T) := \ker \left\{ H^1(K_p, M_T) \longrightarrow H^1(I_p, M_T) \right\}.$$

As shown in the proof of [SU14 Prop. 3.7] (taking $A = \Lambda$ and $a = \tilde{\varphi}$ in loc.cit.), we have $H^1(G_{K,S}, M_T[\tilde{\varphi}]) = H^1(G_{K,S}, M_T)[\tilde{\varphi}]$. On the other hand, using that $G_{K,S}/I_p$ has cohomological dimension one, we immediately see that

$$H^1(I_p, M_T)/H^1_{\text{Gr}}(K_p, M_T) \simeq H^1(I_p, M_T)^{G_{K,S}}.$$

From the long exact sequence in $I_p$-cohomology associated with $0 \rightarrow \Lambda_1 \rightarrow \Lambda_2 \rightarrow \tilde{\varphi} \Lambda_1 \rightarrow 0$ tensored with $T_f$, we obtain

$$(M_T^\varphi/(T_f \otimes \tilde{\varphi} \Lambda_1^\varphi)^{I_p})^{G_{K,S}} \simeq \ker \left\{ H^1(I_p, M_T[\tilde{\varphi}])^{G_{K,S}} \longrightarrow H^1(I_p, M_T)^{G_{K,S}} \right\}.$$

Since $H^0(I_p, M_T) = \{0\}$, we thus have a commutative diagram

$$\begin{array}{ccc}
H^1(G_{K,S}, M_T[\tilde{\varphi}]) & \longrightarrow & H^1(K_p, M_T[\tilde{\varphi}])/H^1_{\text{Gr}}(K_p, M_T[\tilde{\varphi}]) \\
\downarrow \simeq & & \downarrow \\
H^1(G_{K,S}, M_T)[\tilde{\varphi}] & \longrightarrow & H^1(K_p, M_T)/H^1_{\text{Gr}}(K_p, M_T)
\end{array}$$

in which the right vertical map is injective. In light of (2.11), the result follows. \qed

## 3. A $p$-adic Waldspurger Formula

Let $E$, $p$, and $K$ be an introduced in [2.1]. In this section, we define in addition that $K$ satisfies the following Heegner hypothesis relative to the square-free integer $N$:

(Heeg) every prime factor of $N$ is either split or ramified in $K$.

**Anticyclotomic $p$-adic $L$-function.** Let $f = \sum_{n=1}^\infty a_n q^n \in S_2(\Gamma_0(N))$ be the newform associated with $E$. Denote by $R_0$ the completion of the ring of integers of the maximal unramified extension of $\mathbb{Q}_p$, and set $\Lambda_{R_0} := \Lambda \otimes \mathbb{Z}_p R_0$, where as before $\Lambda = \mathbb{Z}_p[\Gamma]$ is the anticyclotomic Iwasawa algebra.

**Theorem 3.1.** There exists a $p$-adic $L$-function $L_p(f) \in \Lambda_{R_0}$ such that if $\tilde{\phi} : \Gamma \rightarrow \mathbb{C}_p^\times$ is the $p$-adic avatar of an unramified anticyclotomic Hecke character $\phi$ with infinity type $(-n,n)$ with $n > 0$, then

$$L_p(f, \tilde{\phi}) = \Gamma(n)\Gamma(n+1) \cdot (1 - a_p p^{-1} \phi(p) + \varepsilon_p \phi^2(p))^2 \cdot \Omega_p^{4n} \cdot \frac{L(f/K, \phi, 1)}{p^{2n+1} \Omega_K^{4n}}.$$
ON THE $p$-PART OF THE BIRCH–SWINNERTON-DYER FORMULA FOR MULTIPLICATIVE PRIMES

where $\varepsilon_p = p^{-1}$ if $p \nmid N$ and $\varepsilon_p = 0$ otherwise, and $\Omega_p \in R_0^\times$ and $\Omega_K \in \mathbb{C}^\times$ are CM periods.

**Proof.** Let $\psi$ be an anticyclotomic Hecke character of $K$ of infinity type $(1, -1)$ and conductor prime to $p$, let $\mathcal{L}_{p,\psi}(f) \in \Lambda_{R_0}$ be as in [CH17, Def. 3.7], and set

$$L_p(f) := \text{Tw}_{\psi^{-1}}(\mathcal{L}_{p,\psi}(f)),$$

where $\text{Tw}_{\psi^{-1}} : \Lambda_{R_0} \to \Lambda_{R_0}$ is the $R_0$-linear isomorphism given by $\gamma \mapsto \psi^{-1}(\gamma)\gamma$ for $\gamma \in \Gamma$. If $p \nmid N$, the interpolation property for $L_p(f)$ is a reformulation of [CH17, Thm. 3.8]. Since the construction in [CH17, §3.3] readily extends to the case $p | N$, with the $p$-adic multiplier $\varepsilon_p(f, \phi)$ in loc. cit. reducing to $1 - a_p p^{-1} \phi(p)$ for unramified $\phi$ (cf. [Cas17a, Thm. 2.10]), the result follows.

If $\Sigma$ is any finite set of place of $K$ not lying above $p$, we define the “$\Sigma$-imprimitive” $p$-adic $L$-function $L_{p}^{\Sigma}(f)$ by

$$L_{p}^{\Sigma}(f) := L_{p}(f) \times \prod_{w \in \Sigma} \overline{P_{w}(\psi^{-1}(\gamma_{w}))} \in \Lambda_{R_{0}},$$

where $P_{w}(X) := \det(1 - X \cdot \text{Frob}_{w}|V_{L})$, $\psi : G_{K} \to \mathbb{Z}_{\mathbb{C}}^\times$ is the $p$-adic cyclotomic character, $\text{Frob}_{w} \in G_{K}$ is a geometric Frobenius element at $w$, and $\gamma_{w}$ is the image of $\text{Frob}_{w}$ in $\Gamma$.

**$p$-adic Waldspurger formula.** We will have use for the following formula for the value at the trivial character $1$ of the $p$-adic $L$-function of Theorem 3.1.

Recall that $E/\mathbb{Q}$ is assumed to be semistable. From now on, we shall also assume that $E$ is an optimal quotient of the new part of $J_{0}(N) = \text{Jac}(X_{0}(N))$ in the sense of [Maz78, §2], and fix a corresponding modular parametrization

$$\pi : X_{0}(N) \longrightarrow E$$

sending the cusp $\infty$ to the origin of $E$. If $\omega_{E}$ a Néron differential on $E$, and $\omega_{f} = \sum a_{n}q^{n}\frac{dq}{q}$ is the one-form on $J_{0}(N)$ associated with $f$, then

$$\pi^{*}(\omega_{E}) = c \cdot \omega_{f},$$

for some $c \in \mathbb{Z}_{(p)}^\times$ (see [Maz78, Cor. 4.1]).

**Theorem 3.2.** The following equality holds up to a $p$-adic unit:

$$L_{p}(f, 1) = (1 - a_{p}p^{-1} + \varepsilon_{p})^{2} \cdot (\log_{\omega_{E}} P_{K})^{2},$$

where $\varepsilon_{p} = p^{-1}$ if $p \nmid N$ and $\varepsilon_{p} = 0$ otherwise, and $P_{K} \in E(K)$ is a Heegner point.

**Proof.** This follows from [BDP13, Thm. 5.13] and [CH17, Thm. 4.9] in the case $p \nmid N$ and [Cas17a, Thm. 2.11] in the case $p | N$. Indeed, in our case, the generalized Heegner cycles $\Delta$ constructed in either of these references are of the form

$$\Delta = [(A, A[\mathfrak{N}]) - (\infty)] \in J_{0}(N)(H),$$

where $H$ is the Hilbert class field of $K$, and $(A, A[\mathfrak{N}])$ is a CM elliptic curve equipped with a cyclic $N$-isogeny. Letting $F$ denote the $p$-adic completion of $H$, the aforementioned references then yield the equality

$$L_{p}(f, 1) = (1 - a_{p}p^{-1} + \varepsilon_{p})^{2} \cdot \left(\sum_{\sigma \in \text{Gal}(H/K)} \text{AJ}_{F}(\Delta^{\sigma})(\omega_{f})\right)^{2}.$$

By [BK90, Ex. 3.10.1], the $p$-adic Abel–Jacobi map appearing in (3.3) is related to the formal group logarithm on $J_{0}(N)$ by the formula

$$\text{AJ}_{F}(\Delta)(\omega_{f}) = \log_{\omega_{f}}(\Delta),$$
and by $[3.2]$ we have the equalities up to a $p$-adic unit:
\[
\log_{\omega f}(\Delta) = \log_{\pi^\ast(\omega_E)}(\pi(\Delta)) = \log_{\omega_E}(\pi(\Delta))
\]
Thus, taking $P_K := \sum_{\sigma \in \text{Gal}(H/K)} \pi(\Delta_{\sigma}) \in E(K)$, the result follows. $\square$

4. MAIN CONJECTURES

Let $f \in I[[q]]$ be an ordinary $I$-adic cusp eigenform of tame level $M$ as in Section 2 (so $p \nmid M$), with associated residual representation $\bar{\rho}_f$. Letting $D_p \subseteq G_{Q}$ be a fixed decomposition group at $p$, we say that $\bar{\rho}_f$ is $p$-distinguished if the semisimplication of $\bar{\rho}_f|_{D_p}$ is the direct sum of two distinct characters.

Let $K$ be an imaginary quadratic field in which $p = \mathfrak{p} \mathfrak{p}$ splits, and which satisfies hypothesis (Heeg) from Section 3 relative to $M$.

For the next statement, note that for any eigenform $f$ defined over a finite extension $L/Q_p$, with associated Galois representation $V_f$, we may define the Selmer group $X_{\Sigma \text{Gr}}(A_f)$ as in $\S 2.2$, replacing $T = T_pE$ by a fixed $G_{Q}$-stable $O_L$-lattice in $V_f$, and setting $A_f := V_f/T_f$.

Theorem 4.1. Let $f \in S_2(\Gamma_0(M))$ be a $p$-ordinary newform of level $M$, with $p \nmid M$, and let $\bar{\rho}_f$ be the associated residual representation. Assume that:

- $M$ is square-free;
- $\bar{\rho}_f$ is ramified at every prime $q \mid M$ which is nonsplit in $K$, and there is at least one such prime;
- $\bar{\rho}_f|_{G_K}$ is irreducible.

If $\Sigma$ is any finite set of prime not lying above $p$, then $X_{\Sigma \text{Gr}}(A_f)$ is $\Lambda$-torsion, and
\[
\text{Ch}_\Lambda(X_{\Sigma \text{Gr}}(A_f))_{\Lambda R_0} = (L_{\Sigma}^\Sigma(f)),
\]
where $L_{\Sigma}^\Sigma(f)$ is as in $[3.1]$.

Proof. As in the proof of [JSW15, Thm. 6.1.6], the result for an arbitrary finite set $\Sigma$ follows immediately from the case $\Sigma = \emptyset$, which is the content of [Cas17b, Thm. 3.4]. (In [Cas17b] it is assumed that $f$ has rational Fourier coefficients but the extension of the aforementioned result to the setting considered here is immediate.) $\square$

Recall that $\Lambda$ denotes the anticyclotomic Iwasawa algebra over $I$, and set $\Lambda_{1,R_0} := \Lambda \hat{\otimes} \mathbb{Z}_p R_0$. For any $\phi \in \mathcal{X}_{1}^a$, set $\tilde{\phi}_0 := \ker(\phi)\Lambda_{1,R_0}$.

Theorem 4.2. Let $\Sigma$ be a finite set of places of $K$ not above $p$. Letting $M$ be the tame level of $f$, assume that:

- $M$ is square-free;
- $\bar{\rho}_f$ is ramified at every prime $q \mid M$ which is nonsplit in $K$, and there is at least one such prime;
- $\bar{\rho}_f|_{G_K}$ is irreducible;
- $\bar{\rho}_f$ is $p$-distinguished.

Then $X_{\Sigma \text{Gr}}(A_f)$ is $\Lambda_1$-torsion, and
\[
\text{Ch}_{\Lambda_1}(X_{\Sigma \text{Gr}}(A_f))_{\Lambda_1,R_0} = (L_{\Sigma}^\Sigma(f)),
\]
where $L_{\Sigma}^\Sigma(f) \in \Lambda_{1,R_0}$ is such that
\[
L_{\Sigma}^\Sigma(f) \mod \tilde{\phi}_0 = L_{\Sigma}^\Sigma(f_0)
\]
for all $\phi \in \mathcal{X}_{1}^a$. 

(4.1)
Proof. Let $\mathcal{L}_p, (\xi(f)) \in \Lambda_{1,R_0}$ be the two-variable anticyclotomic $p$-adic $L$-function constructed in [Cas14 §2.6], and set

$$L_p(f) := Tw^{-1}(\mathcal{L}_p, (\xi(f))),$$

where $\xi$ is the $\mathbb{L}$-adic character constructed in loc.cit. from a Hecke character $\lambda$ of infinity type $(1,0)$ and conductor prime to $p$, and $Tw^{-1}: \Lambda_{1,R_0} \to \Lambda_{1,R_0}$ is the $R_0$-linear isomorphism given by $\gamma \mapsto \xi^{-1}(\gamma)\gamma$ for $\gamma \in \Gamma$. Viewing $\lambda$ as a character on $\mathbb{A}_K^{\times}$, let $\lambda^\tau$ denote the composition of $\lambda$ with the action of complex conjugation on $\mathbb{A}_K^{\times}$. If the character $\psi$ appearing in the proof of Theorem 3.1 is taken to be $\lambda^{1-\tau} := \lambda/\lambda^\tau$, then the proof of [Cas14 Thm. 2.11] shows that $L_p(f)$ reduces to $L_p(f_\phi)$ modulo $\hat{\varphi}$ for all $\phi \in \Lambda_0^{\tau}$. Similarly as in [Cas14], if for any $\Sigma$ as above we set

$$L_p^\Sigma(f) := L_p(f) \times \prod_{\omega \in \Sigma} \varphi(P, T, w) \in \Lambda_{1,R_0},$$

where $\varphi(P, T, w) := \text{det}(1 - X \cdot \text{Frob}_w|\mathcal{P}_f \otimes \mathbb{F})^T$, with $\mathcal{P}_f$ the fraction field of $\mathcal{I}$, the specialization property (4.1) thus follows.

Let $\phi \in \Lambda_0^{\tau}$ be such that $f_\phi$ is the $p$-stabilization of a $p$-ordinary newform $f \in S_2(\Gamma_0(M))$. By Theorem 4.2 the associated $X^\Sigma_{\text{Gr}}(A_f)$ is $\Lambda$-torsion, and we have

(4.2) \hspace{1cm} Ch_\Lambda(X^\Sigma_{\text{Gr}}(A_f)) A_{1,R_0} = (L_p^\Sigma(f)).

In particular, by Theorem 2.6 (with $A_f$ in place of $E[p^{\infty}]$) it follows that $X^\Sigma_{\text{Gr}}(A_f)$ is $\Lambda$-torsion. On the other hand, from [Wan14a Thm. 1.1] we have the divisibility

(4.3) \hspace{1cm} Ch_\Lambda(X^\Sigma_{\text{Gr}}(A_f)) A_{1,R_0} \subseteq (L_p^\Sigma(f)^{-})

in $\Lambda_{1,R_0}$, where $L_p^\Sigma(f)^{-}$ is the projection onto $\Lambda_{1,R_0}$ of the $p$-adic $L$-function constructed in [Wan14a §7.4]. Since a straightforward extension of the calculations in [JSW15 §5.3] shows that

(4.4) \hspace{1cm} (L_p^\Sigma(f)^{-}) = (L_p^\Sigma(f))

as ideals in $\Lambda_{1,R_0}$, the result follows from an application of [SU14 Lem. 3.2] using (1.2), (1.3), and (1.4). (Note that the possible powers of $p$ in [JSW15 Cor. 5.3.1] only arise when there are primes $q \mid M$ inert in $K$, but these are excluded by our hypothesis (Heeg) relative to $M$.)

In order to deduce from Theorem 3.2 the anticyclotomic main conjecture for arithmetic specializations of $f$ (especially in the cases where the conductor of $f_\phi$ is divisible by $p$, which are not covered by Theorem 3.1), we will require the following technical result.

Lemma 4.3. Let $X^\Sigma_{\text{Gr}}(A_f)_{\text{null}}$ be the largest pseudo-null $\Lambda_1$-submodule of $X^\Sigma_{\text{Gr}}(A_f)$, let $\varphi \subseteq \mathcal{I}$ be a height one prime, and let $\hat{\varphi} := \varphi\mathcal{I}_1$. With hypotheses as in Theorem 4.2 the quotient

$$X^\Sigma_{\text{Gr}}(A_f)_{\text{null}}/\hat{\varphi}X^\Sigma_{\text{Gr}}(A_f)_{\text{null}}$$

is a pseudo-null $\Lambda_1/\hat{\varphi}$-module.

Proof. Using (2.11) as in the proof of Theorem 2.6 and considering the obvious commutative diagram obtained by applying the map given by multiplication by $\hat{\varphi}$, the proof of [Och06 Lem. 7.2] carries through with only small changes. (Note that the argument in loc.cit. requires knowing that $X^\Sigma_{\text{ac}}(M_\mathfrak{f}[\hat{\varphi}])$ is $\Lambda_1/\hat{\varphi}$-torsion, but this follows immediately from Theorem 4.2 and the isomorphism of Theorem 2.6.)

For the next result, let $E/Q$ be an elliptic curve of square-free conductor $N$, and assume that $K$ satisfies hypothesis (Heeg) relative to $N$, and that $p = \mathfrak{p}\mathfrak{f}$ splits in $K$. 


Theorem 4.4. Assume that $\tilde{\rho}_{E,p} : G_{\mathbb{Q}} \to \text{Aut}_{E}(E[p]) \simeq \text{GL}_2(\mathbb{F}_p)$ is irreducible and ramified at every prime $q \nmid N$ which is nonsplit in $K$, and assume that there is at least one such prime. Then $\text{Ch}_{\Lambda}(X_{ac}(E[p^\infty]))$ is $\Lambda$-torsion and

$$\text{Ch}_{\Lambda}(X_{ac}(E[p^\infty]))|_{\Lambda_{R_0}} = (L_p(f)).$$

Proof. If $E$ has good ordinary (resp. supersingular) supersingular reduction at $p$, the result follows from [Cas17, Thm. 3.4] (resp. [CW16, Thm. 5.1]). (Note that by [Ski14, Lem. 2.8.1] the hypotheses in Theorem 4.4 imply that $\tilde{\rho}_{E,p}|G_K$ is irreducible.) Since the conductor of $N$ is square-free, it remains to consider the case in which $E$ has multiplicative reduction at $p$. The associated newform $f = \sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(N))$ then satisfies $a_p = \pm 1$ (see e.g. [Sk16, Lem. 2.1.2]); in particular, $f$ is $p$-ordinary. Let $f \in \mathbb{Z}[q]$ be the ordinary $q$-adic cusp eigenform of tame level $N_0 := N/p$ attached to $f$, so that $f_\phi = f$ for some $\phi \in \mathcal{X}_p$. Let $\tilde{\varphi} := \ker(\phi) \subseteq \Lambda$ be the associated height one prime, and set

$$\tilde{\varphi} := \varphi_{\Lambda_{1,R_0}}, \quad \Lambda_{p,R_0} := \Lambda_{1,R_0}/\tilde{\varphi}, \quad \tilde{\varphi}_0 := \tilde{\varphi} \cap \Lambda_1, \quad \Lambda_p := \Lambda_{1,\tilde{\varphi}_0}.$$

Let $\Sigma$ be a finite set of places of $K$ not dividing $p$ containing the primes above $N_0D$, where $D$ is the discriminant of $K$. As shown in the proof of [JSW15, Thm. 6.1.6], it suffices to show that

$$(4.5) \quad \text{Ch}_{\Lambda}(X_\Sigma^{\Sigma}(E[p^\infty]))|_{\Lambda_{R_0}} = (L_p^\Sigma(f)).$$

Since $f$ specializes $f$, which has weight 2 and trivial nebentypus, the residual representation $\tilde{\rho}_r \simeq \tilde{\rho}_{E,p}$ is automatically $p$-distingshished (see [KLZ17, Rem. 7.2.7]). Thus our assumptions imply that the hypotheses in Theorem 4.4 are satisfied, which combined with Theorem 2.6 show that $X_{\text{Gr}}(E[p^\infty])$ is $\Lambda$-torsion. Moreover, letting $I$ be any height one prime of $\Lambda_{p,R_0}$ and setting $I_0 := I \cap \Lambda_p$, by Theorem 2.6 we have

$$(4.6) \quad \text{length}_{(\Lambda_{p})_{I_0}}(X_\Sigma^{\Sigma}(E[p^\infty]))|_{I_0} = \text{length}_{(\Lambda_{p})_{I_0}}((X_{\text{Gr}}^{\Sigma}(A_f)/\tilde{\varphi}_0X_{\text{Gr}}^{\Sigma}(A_f))|_{I_0}).$$

On the other hand, if $\tilde{\varphi} \subseteq \Lambda_{1,R_0}$ maps to $I$ under the specialization map $\Lambda_{1,R_0} \to \Lambda_{p,R_0}$ and we set $I_0 := \tilde{\varphi} \cap \Lambda_1$, by Theorem 4.2 we have

$$(4.7) \quad \text{length}_{(\Lambda_{p})_{I_0}}(X_\Sigma^{\Sigma}(A_f)|_{I_0}) = \text{ord}_{I_0}(L_p^\Sigma(f) \bmod \tilde{\varphi}) = \text{ord}_{I_0}(L_p^\Sigma(f)).$$

Since Lemma 4.3 implies the equality

$$\text{length}_{(\Lambda_{p})_{I_0}}((X_{\text{Gr}}^{\Sigma}(A_f)/\tilde{\varphi}_0X_{\text{Gr}}^{\Sigma}(A_f))|_{I_0}) = \text{length}_{(\Lambda_{p})_{I_0}}(X_{\text{Gr}}^{\Sigma}(A_f)|_{I_0}),$$

combining (4.6) and (4.7) we conclude that

$$\text{length}_{(\Lambda_{p})_{I_0}}(X_\Sigma^{\Sigma}(E[p^\infty]))|_{I_0} = \text{ord}_{I_0}(L_p^\Sigma(f))$$

for every height one prime $I$ of $\Lambda_{p,R_0}$, and so

$$(4.8) \quad \text{Ch}_{\Lambda}(X_\Sigma^{\Sigma}(E[p^\infty]))|_{\Lambda_{R_0}} = (L_p^\Sigma(f)).$$

Finally, since our hypothesis on $\tilde{\rho}_{E,p}$ implies that $c_w(E/K)$ is a $p$-adic unit for every prime $w$ nonsplit in $K$ (see e.g. [PW11, Def. 3.3]), we have $\text{Ch}_{\Lambda}(X_{\text{Gr}}^{\Sigma}(E[p^\infty])) = \text{Ch}_{\Lambda}(X_{\text{ac}}^{\Sigma}(E[p^\infty]))$ by Proposition 2.5. Equality (4.8) thus reduces to (4.5), and the proof of Theorem 4.4 follows.

5. Proof of Theorem A

Let $E/Q$ be a semistable elliptic curve of conductor $N$ as in the statement of Theorem A; in particular, we note that there exists a prime $q \neq p$ such that $E[p]$ is ramified at $q$. Indeed, if $p \mid N$ this follows by hypothesis, while if $p \nmid N$ the existence of such $q$ follows from Ribet’s level lowering theorem [Rib90, Thm. 1.1], as explained in the first paragraph of [JSW15 §7.4].

Proof of Theorem A. Choose an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ of discriminant $D < 0$ such that

$$\text{Ch}_{\Lambda}(X_{ac}(E[p^\infty]))|_{\Lambda_{R_0}} = (L_p(f)).$$

□
• $q$ is ramified in $K$;
• every prime factor $\ell \neq q$ of $N$ splits in $K$;
• $p$ splits in $K$;
• $L(E^D,1) \neq 0$.

(Of course, when $p \mid N$ the third condition is redundant.) By Theorem 4.4 and Proposition 3.2 we have the equalities

$$(5.1) \quad \# \mathbb{Z}_p/f_{ac}(0) = \# \mathbb{Z}_p/L_p(f,1) = \# \left( \mathbb{Z}_p/(1 - a_p p^{-1} + \epsilon_p) \log_{E} P_K \right)^2,$$

where $\epsilon_p = p^{-1}$ if $p \nmid N$ and $\epsilon_p = 0$ otherwise, and $P_K \in E(K)$ is a Heegner point. Since we assume that $\text{ord}_{s=1} L(E,s) = 1$, our last hypothesis on $K$ implies that $\text{ord}_{s=1} L(E/K,s) = 1$, and so $P_K$ has infinite order, $\text{rank}_{Z}(E(K)) = 1$ and $\# \text{III}(E/K) < \infty$ by the work of Gross–Zagier and Kolyvagin. This verifies the hypotheses in Theorem 2.3, which (taking $\Sigma = \emptyset$ and $P = P_K$) yields a formula for $\# \mathbb{Z}_p/f_{ac}(0)$ that combined with (5.1) immediately leads to

$$(5.2) \quad \text{ord}_p(\# \text{III}(E/K)[p^\infty]) = 2 \cdot \text{ord}_p([E(K) : \mathbb{Z}.P_K]) - \sum_{w \mid N^+} \text{ord}_p(c_w(E/K)),
$$

where $N^+$ is the product of the prime factors of $N$ which are split in $K$. Since $E[p]$ is ramified at $q$, we have $\text{ord}_p(c_w(E/K)) = 0$ for every prime $w \mid q$ (see e.g. [Zha14 Lem. 6.3] and the discussion right after it), and since $N^+ = N/q$ by our choice of $K$, we see that (5.2) can be rewritten as

$$(5.3) \quad \text{ord}_p(\# \text{III}(E/K)[p^\infty]) = 2 \cdot \text{ord}_p([E(K) : \mathbb{Z}.P_K]) - \sum_{w \mid N} \text{ord}_p(c_w(E/K)).$$

On the other hand, as explained in [JSW15 p. 47] the Gross–Zagier formula [GZ86, YZZ13] (as refined in [CST14]) can be paraphrased as the equality

$$\frac{L'(E,1)}{\Omega_E \cdot \text{Reg}(E/Q)} \cdot \frac{L(E^D,1)}{\Omega_{E^D}} = [E(K) : \mathbb{Z}.P_K]^2$$

up to a $p$-adic unit which combined with (5.3) and the immediate relation

$$\sum_{w \mid N} c_w(E/K) = \sum_{\ell \mid N} c_\ell(E/Q) + \sum_{\ell \mid N} c_\ell(E^D/Q)$$

(see [SZ14 Cor. 7.2]) leads to the equality

$$\text{ord}_p(\# \text{III}(E/K)[p^\infty]) = \text{ord}_p \left( \frac{L'(E,1)}{\Omega_E \cdot \text{Reg}(E/Q) \prod_{\ell \mid N} c_\ell(E/Q)} \cdot \frac{L(E^D,1)}{\Omega_{E^D} \prod_{\ell \mid N} c_\ell(E^D/Q)} \right).$$

Finally, since $L(E^D,1) \neq 0$, by the known $p$-part of the Birch and Swinnerton-Dyer formula for $E^D$ (as recalled in [JSW15 Thm. 7.2.1]) we arrive at

$$\text{ord}_p(\# \text{III}(E/Q)[p^\infty]) = \text{ord}_p \left( \frac{L'(E,1)}{\Omega_E \cdot \text{Reg}(E/Q) \prod_{\ell \mid N} c_\ell(E/Q)} \right),$$

concluding the proof of the theorem. \hfill $\square$

---

1This uses a period relation coming from [SZ14 Lem. 9.6], which assumes that $(D,pN) = 1$, but the same argument applies replacing $D$ by $D/(D,pN)$ in the last paragraph of the proof of their result.
References

[BDP13] Massimo Bertolini, Henri Darmon, and Kartik Prasanna, Generalized Heegner cycles and p-adic Rankin L-series, Duke Math. J. 162 (2013), no. 6, 1033–1148.

[BK90] Spencer Bloch and Kazuya Kato, L-functions and Tamagawa numbers of motives, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[Cas14] Francesc Castella, On the p-adic variation of Heegner points, preprint, arXiv:1410.6591 (2014).

[Cas17a] _____, On the exceptional specializations of big Heegner points, J. Inst. Math. Jussieu, to appear (2017).

[Cas17b] _____, p-adic heights of Heegner points and Beilinson–Flach classes, J. Lond. Math. Soc., to appear (2017).

[CH17] Francesc Castella and Ming-Lun Hsieh, Heegner cycles and p-adic L-functions, Math. Ann., to appear (2017).

[CST14] Li Cai, Jie Shu, and Ye Tian, Explicit Gross-Zagier and Waldspurger formulae, Algebra Number Theory 8 (2014), no. 10, 2523–2572.

[CW16] Francesc Castella and Xin Wan, Λ-adic Gross-Zagier formula for elliptic curves at supersingular primes, preprint, arXiv:1607.02019 (2016).

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

[GZ86] Benedict H. Gross and Don B. Zagier, Heegner points and derivatives of L-series, Invent. Math. 84 (1986), no. 2, 225–320.

[HB15] Ernest Hunter Brooks, Shimura curves and special values of p-adic L-functions, Int. Math. Res. Not. IMRN (2015), no. 12, 4177–4241.

[JSW15] Dimitar Jetchev, Christopher Skinner, and Xin Wan, The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one, preprint, arXiv:1512.06894 (2015).

[KLZ14] Guido Kings, David Loeffler, and Sarah Zerbes, Rankin–Selberg Euler systems and p-adic interpolation, preprint, arXiv:1405.3079 (2014).

[KLZ17] _____, Rankin–Eisenstein classes and explicit reciprocity laws, Camb. J. Math. 5 (2017), no. 2, 1–122.

[Maz78] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math. 44 (1978), no. 2, 129–162.

[Och06] Tadashi Ochiai, On the two-variable Iwasawa main conjecture, Compos. Math. 142 (2006), no. 5, 1157–1200.

[PW11] Robert Pollack and Tom Weston, On anticyclotomic μ-invariants of modular forms, Compos. Math. 147 (2011), no. 5, 1353–1381.

[Rib90] K. A. Ribet, On modular representations of Gal(\overline{Q}/Q) arising from modular forms, Invent. Math. 100 (1990), no. 2, 431–476.

[Ser72] Jean-Pierre Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques, Invent. Math. 15 (1972), no. 4, 259–331.

[Sil94] Joseph H. Silverman, Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[Ski14] Christopher Skinner, A converse to a theorem of Gross, Zagier, and Kolyvagin, preprint, arXiv:1405.7294 (2014).

[Ski16] _____, Multiplicative reduction and the cyclotomic main conjecture for GL2, Pacific J. Math. 283 (2016), no. 1, 171–200.

[Spr16] Florian Sprung, The Iwasawa Main Conjecture for elliptic curves at odd supersingular primes, preprint, arXiv:1610.00171 (2016).

[SU14] Christopher Skinner and Eric Urban, The Iwasawa Main Conjectures for GL2, Invent. Math. 195 (2014), no. 1, 1–277.

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

[TW95] Richard Taylor and Andrew Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. of Math. (2) 141 (1995), no. 3, 553–572.

[Wan14a] Xin Wan, Iwasawa main conjecture for Rankin–Selberg p-adic L-functions, preprint, arXiv:1408.4044 (2014).

[Wan14b] _____, Iwasawa main conjecture for Rankin–Selberg p-adic L-functions: non-ordinary case, preprint, arXiv:1412.1767 (2014).

[Wan14c] _____, Iwasawa main conjecture for supersingular elliptic curves, preprint, arXiv:1411.6352 (2014).
[Wil95]  Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[YZZ13]  Xinyi Yuan, Shou-Wu Zhang, and Wei Zhang, *The Gross-Zagier formula on Shimura curves*, Annals of Mathematics Studies, vol. 184, Princeton University Press, Princeton, NJ, 2013.

[Zha14]  Wei Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2** (2014), no. 2, 191–253.

Mathematics Department, Princeton University, Fine Hall, Princeton, NJ 08544-1000, USA

E-mail address: fcabello@math.princeton.edu