On the $p$-part of the Birch–Swinnerton-Dyer formula for multiplicative primes

FRANCESC CASTELLA

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 [JSW17], 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.

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

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

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

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

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

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 [JSW17]. (One should note that [JSW17, 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 [Spr16, Cor. 1.3]; cf. [CQS17, Thm. C].) Earlier results in the \(p\)-ordinary case were obtained by W. Zhang [Zha14, Thm. 10.2] and by Berti–Bertolini–Venerucci [BBV16, Thm. A]. For primes \(p \mid N\), some particular cases of Theorem A were first proved by 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 [JSW17], 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 [JSW17, Thm. 1.2.1] (for primes \(p \not\mid N\)) is naturally divided into two steps:

1. **Exact lower bound on the predicted \(\#\Sha(E/K)[p^{\infty}]\).** For this part of the argument, in [JSW17] 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

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

(1.1)

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 \(E/K_1\) ([JSW17, 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

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

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 $L_p(f) \in \Lambda_{R_0}$ is an anticyclotomic $p$-adic $L$-function;


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

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

2. Exact upper bound on the predicted $\#\Sha(E/\mathbb{Q})[p^\infty]$. For the second part of the argument, in [JSW17] one chooses an imaginary quadratic field $K_2 = \mathbb{Q}(\sqrt{D_2})$ (in general different from $K_1$) with $L(E^{D_2}, 1) \neq 0$. Crucially, $K_2$ is chosen so that the associated $N^+$ (the product of the prime factors of $N$ that are either 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:

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

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 nonsplit unless $N$ is prime). Combined with the general Gross–Zagier formula [YZZ13] and the $p$-part of the Birch and Swinnerton-Dyer formula for $E^{D_2}/\mathbb{Q}$, inequality (1.2) then yields the predicted optimal upper bound for $\#\Sha(E/\mathbb{Q})[p^\infty]$.

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 $q | N$ nonsplit in $K$;
- $p$ splits in $K$,

in [Cas17c] (for good ordinary $p$) and [CW17] (for good supersingular $p$) we have completed under mild hypotheses the proof of the Iwasawa–Greenberg main conjecture for the associated $X_{ac}(E[p^\infty])$:

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

With this result in hand, a simplified form (since $N^- = 1$ here) of the arguments from [JSW17] in part (1) above lead to an equality in (1.1) taking $K_1 = K$, and so to the predicted order of $\Sha(E/Q)[p^\infty]$ when $p \nmid N$.

To treat the primes $p | N$ 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 $f \in \mathbb{I}[[q]]$ be the Hida family associated with $f$, where $\mathbb{I}$ is a certain finite flat extension of the one-variable Iwasawa algebra. In Section 4, we deduce from [Cas17c] and [Wan14a] a proof of a two-variable analog of the Iwasawa–Greenberg main conjecture (1.3) over the Hida family:

$$
Ch_{\Lambda}(X_{ac}(A_f))\Lambda_{E,R_0} = (L_p(f)),
$$

where $L_p(f) \in \Lambda_{E,R_0}$ is the two-variable anticyclotomic $p$-adic $L$-function introduced in [Cas17b]. 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 $Ch_{\Lambda}(X_{ac}(E[p^\infty]))$, yielding a proof of the Iwasawa–Greenberg main conjecture (1.3) in the multiplicative reduction case. Combined with the anticyclotomic control theorem of (1.a) and the generalization (contained in [Cas17a]) of the $p$-adic Waldspurger formula in (1.c) to multiplicative primes:

$$
L_p(f, \mathbb{I}) = (1 - a_pp^{-1})^2 \cdot (\log_{\omega_E} P_K)^2,
$$

we arrive at the predicted formula for $\#\Sha(E/Q)[p^\infty]$ just as in the good reduction case.
Acknowledgements

As will be clear to the reader, this note borrows many ideas and arguments from [JSW17]. 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

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

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 $p = \mathfrak{p}\mathfrak{q}$ 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

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

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

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

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

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 $H^1(K_w, V) \to H^1(K_w, V/T) \cong H^1(K_w, E[p^\infty])$.

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

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

where $\Lambda^\ast = \text{Hom}_\text{cont}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p)$ is the Pontrjagin dual of $\Lambda^{ac}$. Letting $\rho_{E,p}$ denote the natural action of $G_K := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $T$, the $G_K$-action on $M$ is given by $\rho_{E,p} \otimes \Psi^{-1}$, where $\Psi$ is the composite character $G_K \to \Gamma \hookrightarrow \Lambda^\ast$. 
Definition 2.2. The anticyclotomic Selmer group for $E$ over $K_{\infty}^{ac}/K$ is defined by

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

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

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

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

$$\log_{\omega_E} : E(\mathbb{Q}_p) \twoheadrightarrow \mathbb{Z}_p$$

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 $\mathbb{Z}_p[[T]]$ with the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\Gamma]]$ by sending $1 + T \mapsto \gamma$.

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

$$\#\mathbb{Z}_p/f_{\text{ac}}^\Sigma(0) = \#\text{III}(E/K)[p^\infty] \cdot \left(\frac{\#\mathbb{Z}_p/((1 - a_p p^{-1} + \varepsilon_p) \log_{\omega_E} P)}{[E(K) \otimes \mathbb{Z}_p : \mathbb{Z}_p, P]}\right)^2 \times \prod_{w | N^+} c_{w}(E/K)_p \cdot \prod_{w \in \Sigma} \#H^1(K_w, E[p^\infty]),$$

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 $c_{w}(E/K)_p$ 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 [JSW17, §3.3]. The hypotheses imply that \( \text{corank}_{\mathbb{Z}_p} \text{Sel}(K, E[p^\infty]) = 1 \) 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 \( w | p \). By [JSW17, Prop. 3.2.1] it follows that \( H^1_{\text{ac}}(K, E[p^\infty]) \) is finite with

\[
\# H^1_{\text{ac}}(K, E[p^\infty]) = \# \text{III}(E/K)[p^\infty] \cdot \frac{[E(K_p)/\text{tors} \otimes \mathbb{Z}_p : \mathbb{Z}_p\cdot P]_2}{[E(K) \otimes \mathbb{Z}_p : \mathbb{Z}_p\cdot P]_2},
\]

where \( E(K_p)/\text{tors} := E(K_p)/E(K_p)_{\text{tors}} \) 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

\[
[E(K_p)/\text{tors} \otimes \mathbb{Z}_p : \mathbb{Z}_p\cdot P]_2 = \frac{\# \mathbb{Z}_p / ((1-a_p/p) \log_{\omega_E} P)}{\# H^0(K_p, E[p^\infty])}
\]

as shown in [JSW17, §3.5], and substituting (2.2) into (2.1) we arrive at

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

from where the result follows immediately by [JSW17, Thm. 3.3.1].

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

\[
0 \longrightarrow E_1(K_p) \longrightarrow E_0(K_p) \longrightarrow \tilde{E}_{\text{ns}}(\mathbb{F}_p) \longrightarrow 0.
\]

The formal group logarithm defines an injective homomorphism

\[
\log_{\omega_E} : E(K_p)/\text{tor} \otimes \mathbb{Z}_p \longrightarrow \mathbb{Z}_p
\]
mapping $E_1(K_p)$ isomorphically onto $p\mathbb{Z}_p$, and hence we see that

$$
[E(K_p)/\text{tors} \otimes \mathbb{Z}_p : \mathbb{Z}_p.P] = \frac{\#\mathbb{Z}_p/(\log_\omega E)}{\#\mathbb{Z}_p/(\log_\omega (E(K_p)/\text{tors} \otimes \mathbb{Z}_p))} \\
= \frac{\#\mathbb{Z}_p/(\log_\omega E) \cdot \#(E(K_p)/E_1(K_p) \otimes \mathbb{Z}_p)}{\#\mathbb{Z}_p/p\mathbb{Z} \cdot \#(E(K_p)/\text{tors} \otimes \mathbb{Z}_p)} \\
= [E(K_p) : E_0(K_p)]_{p} \cdot \frac{\#\mathbb{Z}_p/(\log_\omega E) \cdot \#(E_0(K_p)/E_1(K_p) \otimes \mathbb{Z}_p)}{\#\mathbb{Z}_p/p\mathbb{Z}_p \cdot \#(E(K_p)/\text{tors} \otimes \mathbb{Z}_p)},
$$

where 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

$$
E_0(K_p)/E_1(K_p) \otimes \mathbb{Z}_p \simeq \mathcal{E}_{ns}(F_p) \otimes \mathbb{Z}_p,
$$

which is trivial by e.g. [Sil94, Prop. 5.1] (and $p > 2$). Since clearly $E(K_p)/\text{tors} \otimes \mathbb{Z}_p = H^0(K_p, E[p^{\infty}])$, we thus conclude that

$$
(2.4) \quad [E(K_p)/\text{tors} \otimes \mathbb{Z}_p : \mathbb{Z}_p.P] = [E(K_p) : E_0(K_p)]_{p} \cdot \frac{\#\mathbb{Z}/(\frac{1}{p} \log_\omega E)}{\#H^0(K_p, E[p^{\infty}])},
$$

and substituting (2.4) into (2.1) we arrive at

$$
#H_{ac}^1(K, E[p^{\infty}]) \\
= #\mathcal{I}(E/K)[p^{\infty}] \cdot \left(\left[\frac{\#E_0(K_p)_{p}}{\#(E_0(K_p)_{p} \otimes \mathbb{Z}_p.P)}\right] \cdot \frac{\#\mathbb{Z}/(\frac{1}{p} \log_\omega E)}{\#H^0(K_p, E[p^{\infty}])}\right)^2.
$$

Plugging this formula for $#H_{ac}^1(K, E[p^{\infty}])$ into [JSW17, Thm. 3.3.1] yields the equality

$$
(2.5) \quad \#\mathbb{Z}_p/f_{ac}^1(0) \\
= #\mathcal{I}(E/K)[p^{\infty}] \cdot \left(\left[\frac{\#E_0(K_p)_{p}}{\#(E_0(K_p)_{p} \otimes \mathbb{Z}_p.P)}\right] \cdot \frac{\#\mathbb{Z}/(\frac{1}{p} \log_\omega E)}{\#H^0(K_p, E[p^{\infty}])}\right)^2 \cdot [E(K_p) : E_0(K_p)]_{p}^2 \\
\times \prod_{w \in S \setminus \Sigma} \#H^1_{ur}(K_w, E[p^{\infty}]) \cdot \prod_{w \in \Sigma} \#H^1(K_w, E[p^{\infty}]),
$$

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

$$
(2.6) \quad [E(K_p) : E_0(K_p)]_{p} = c_w(E/K)_{p}
$$
by definition, while if \( w \nmid p \), then

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

by \([SZ14, Lem. 9.1]\). Since \( c_w(E/K)_p = 1 \) 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 \( \Lambda_W = \mathbb{Z}_p[[W]] \) be the one-variable power series ring in the indeterminate \( W \). Let \( M \) be an integer prime to \( p \), let \( \chi \) be a Dirichlet character modulo \( pM \), and let \( f = \sum_{\infty} a_n q^n \in \mathbb{I}[[q]] \) be an ordinary \( \mathbb{I} \)-adic cusp eigenform of tame level \( M \) and character \( \chi \) (as defined in \([SU14, \S3.3.9]\)) defined over a local reduced finite integral extension \( \mathbb{I}/\Lambda_W \).

Let \( \mathcal{X}^a_i \) the set of continuous \( \mathbb{Z}_p \)-algebra homomorphisms \( \phi: \mathbb{I} \rightarrow \overline{\mathbb{Q}}_p \) whose composition with the structural map \( \Lambda_W \rightarrow \mathbb{I} \) 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 \( \phi \in \mathcal{X}^a_i \) 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. We shall only need consider the case where \( \chi \) is the trivial character, in which case for all \( \phi \in \mathcal{X}^a_i \) of weight \( k_\phi \equiv 2 \) (mod \( p-1 \)), either

1. \( f_\phi \) is a newform on \( \Gamma_0(pM) \); or
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, but for \( k_\phi = 2 \) both cases occur.

Let \( k_\mathbb{I} \) be the residue field of \( \mathbb{I} \), and assume that the residual Galois representation

\[
\bar{\rho}_f: G_\mathbb{Q} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(k_\mathbb{I})
\]

attached to \( f \) is irreducible. Then there exists a free \( \mathbb{I} \)-module \( T_\mathbb{I} \) of rank two equipped with a continuous \( \mathbb{I} \)-linear action of \( G_\mathbb{Q} \) such that, for all \( \phi \in \mathcal{X}^a_i \), there is a canonical \( G_\mathbb{Q} \)-isomorphism

\[
T_\mathbb{I} \otimes_\mathbb{I} \phi(\mathbb{I}) \simeq T_\phi,
\]
where $T_{f_s}$ is a $G_{\mathbb{Q}}$-stable lattice in the Galois representation $V_{f_s}$ associated with $f_s$. (Here, $T_f$ corresponds to the Galois representation $M(f)^*$ in [KLZ17, Def. 7.2.5]; in particular, for $k_\varphi \equiv 2 \pmod{p-1}$ we have $\det(V_{f_s}) = \epsilon^{k_\varphi-1}$, where $\epsilon : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ is the $p$-adic cyclotomic character.)

Let $\Lambda_I := \mathbb{Z}[[\Gamma]]$ be the anticyclotomic Iwasawa algebra over $I$, and consider the $\Lambda_I$-module $M_f := T_f \otimes I \Lambda_I^*$. This is equipped with a natural $G_K$-action defined similarly as for the $\Lambda$-module $M = T \otimes \mathbb{Z}_p$ introduced in §2.1.

**Definition 2.4.** The Greenberg Selmer group of $E$ over $K_\infty/K$ is

$$\text{Sel}_{Gr}(E[p^\infty]) := \ker \left\{ H^1(K, M) \longrightarrow H^1(I_p, M) \oplus \prod_{w \nmid p} H^1(I_w, M) \right\}.$$  

The Greenberg Selmer group $\text{Sel}_{Gr}(K_\infty, A_f)$ for $f$ over $K_\infty/K$, where $A_f := T_f \otimes \mathbb{Z}_p$, is defined similarly as for the $\Lambda_I$-module $M_f$. This equipped with a natural $G_K$-action defined similarly as for the $\Lambda$-module $M = T \otimes \mathbb{Z}_p$.

Similarly as for the Selmer groups introduced in §2.1, for any given finite set $\Sigma$ of places $w \nmid p$ of $K$, the $\Sigma$-imprimitive Selmer groups $\text{Sel}_{Gr}^\Sigma(K_\infty, E[p^\infty])$ and $\text{Sel}_{Gr}^\Sigma(K_\infty, A_f)$ are defined by dropping the summands $H^1(I_w, M)$ and $H^1(I_w, M_f)$ for the places $w \in \Sigma$ in the above definition. Let

$$X_{Gr}^\Sigma(E[p^\infty]) := \text{Hom}_{\text{cont}}(\text{Sel}_{Gr}(K_\infty, E[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p)$$

be the Pontrjagin dual of $\text{Sel}_{Gr}^\Sigma(K_\infty, E[p^\infty])$, and define $X_{Gr}^\Sigma(A_f)$ similarly.

We will have use for the following comparison between the Selmer groups $\text{Sel}_{Gr}(K_\infty, E[p^\infty])$ and $\text{Sel}_p(K_\infty, E[p^\infty])$. Note that directly from the definition we have an exact sequence

$$(2.8) \quad 0 \longrightarrow \text{Sel}_p(K_\infty, E[p^\infty]) \longrightarrow \text{Sel}_{Gr}(K_\infty, E[p^\infty]) \longrightarrow \mathcal{H}^u_p \oplus \prod_{w \mid p} \mathcal{H}^u_{w},$$

where

$$\mathcal{H}^u_{w} := \ker \left\{ H^1(K_v, M) \longrightarrow H^1(I_v, M) \right\}$$

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 \( X^\Sigma_{\text{Gr}}(E[p^\infty]) \) is \( \Lambda \)-torsion. Then \( X_{\text{ac}}^\Sigma(E[p^\infty]) \)

is \( \Lambda \)-torsion, and we have the relations

\[
\lambda(X^\Sigma_{\text{Gr}}(E[p^\infty])) = \lambda(X_{\text{ac}}^\Sigma(E[p^\infty]))
\]

and

\[
\mu(X^\Sigma_{\text{Gr}}(E[p^\infty])) = \mu(X_{\text{ac}}^\Sigma(E[p^\infty])) + \sum_{w \text{ nonsplit } w \not\in \Sigma} \text{ord}_p(c_w(E/K)).
\]

Proof. Since \( X_{\text{ac}}^\Sigma(E[p^\infty]) \) is a quotient of \( X^\Sigma_{\text{Gr}}(E[p^\infty]) \), the first claim of the proposition is clear. Consider the exact sequence (2.8) (or rather its variant for \( \Sigma \)-imprimitive Selmer groups). 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 \( \mathcal{H}^\text{ur}_v \) vanishes. Since \( M'^p = \{0\} \), the term \( \mathcal{H}^\text{ur}_p \) also vanishes, and the aforementioned exact sequence thus reduces to

\[
0 \to \text{Sel}^\Sigma_p(K_\infty, E[p^\infty]) \to \mathfrak{S}^\Sigma_{\text{Gr}}(K_\infty, E[p^\infty]) \to \prod_{w \text{ nonsplit } w \not\in \Sigma} \mathcal{H}^\text{ur}_w.
\]

Now, a straightforward modification of the argument in [PW11, Lem. 3.4] shows that

\[
\mathcal{H}^\text{ur}_w \simeq (\mathbb{Z}/p^tE(w)\mathbb{Z}_p) \otimes \Lambda^*.
\]

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, \( \mathcal{H}^\text{ur}_w \) is \( \Lambda \)-torsion, with \( \lambda(\mathcal{H}^\text{ur}_w) = 0 \) and \( \mu(\mathcal{H}^\text{ur}_w) = \text{ord}_p(c_w(E/K)) \). Since the rightmost arrow in (2.9) is surjective by [PW11, Prop. A.2], the result follows.

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 \( f \in \mathbb{H}[[q]] \) be the Hida family associated with \( f \), let \( \varphi \subseteq \mathbb{H} \) be the kernel of the arithmetic map \( \phi \in \mathcal{X}_T^\omega \) such that \( f_{\bar{\varphi}} \) is either \( f \) itself (if \( p \nmid N \)) or the ordinary \( p \)-stabilization of \( f \) (if \( p \nmid N \)), and set \( \bar{\varphi} := \varphi \Lambda \subseteq \Lambda \). Since we assume that \( \bar{\rho}_{E,p} \) is irreducible, so is \( \bar{\varphi} \).

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

\[
X^\Sigma_{\text{Gr}}(E[p^\infty]) \simeq X^\Sigma_{\text{Gr}}(A_f)/\bar{\varphi}X^\Sigma_{\text{Gr}}(A_f).
\]
Proof. This follows from a slight variation of the arguments proving [SU14, Prop. 3.7] (see also [Och06, Prop. 5.1]). Since $M \simeq M_f[\tilde{\wp}]$, by Pontrjagin duality it suffices to show that the canonical map

$$(2.10) \quad \text{Sel}^\Sigma_{\text{Gr}}(K_{\infty}, M_f[\tilde{\wp}]) \longrightarrow \text{Sel}^\Sigma_{\text{Gr}}(K_{\infty}, M_f)[\tilde{\wp}]$$

is an isomorphism. Note that our assumption on $S := \Sigma \cup S_p$ implies that

$$(2.11) \quad \text{Sel}^\Sigma_p(K_{\infty}, M_\ell) = \ker \left\{ H^1(G_{K,S}, M_\ell) \to H^1(K_p, M_\ell) \right\},$$

where $M_\ell = M_f[\tilde{\wp}]$ or $M_f$; $G_{K,S}$ is the Galois group of the maximal extension of $K$ unramified outside $S$.

As shown in the proof of [SU14, Prop. 3.7] (taking $A = \Lambda_1$ and $a = \tilde{\wp}$ in loc.cit.), we have $H^1(G_{K,S}, M_f[\tilde{\wp}]) = H^1(G_{K,S}, M_f)[\tilde{\wp}]$. On the other hand, using that $G_{K_p}/I_p$ has cohomological dimension one, we immediately see that

$$H^1(K_p, M_\ell)/H^1(G_{K_p}, M_\ell) \simeq H^1(I_p, M_\ell)^{G_{K_p}}.$$

From the long exact sequence in $I_p$-cohomology associated with $0 \to \Lambda_1^\ast[\tilde{\wp}] \to \Lambda_1^\ast \to \tilde{\wp}\Lambda_1^\ast \to 0$ tensored with $T_f$, we obtain

$$(M_f^I/(T_f \otimes \Lambda_1^\ast)^I)^{G_{K_p}} \simeq \ker \left\{ H^1(I_p, M_f[\tilde{\wp}])^{G_{K_p}} \to H^1(I_p, M_f)^{G_{K_p}} \right\}.$$

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

$$\begin{array}{ccc}
H^1(G_{K,S}, M_f[\tilde{\wp}]) & \xrightarrow{\text{loc}_p} & H^1(K_p, M_f[\tilde{\wp}]) / H^1(G_{K_p}, M_f[\tilde{\wp}]) \\
\simeq & & \downarrow \\
H^1(G_{K,S}, M_f)[\tilde{\wp}] & \xrightarrow{\text{loc}_p} & H^1(K_p, M_f) / H^1(G_{K_p}, M_f)
\end{array}$$

in which the right vertical map is injective. By (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 assume 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

$$\Lambda_{R_0} := \Lambda \hat{\otimes} \mathbb{Z}_p R_0,$$

where as before $\Lambda = \mathbb{Z}_p[[\Gamma]]$ is the anticyclotomic Iwasawa algebra.

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

$$L_p(f, \hat{\phi}) = \Gamma(n) \Gamma(n+1) \cdot (1 - a_p p^{-1} \phi(p)) \cdot \Omega_p^{4n} \cdot \frac{L(f/K, \phi, 1)}{\pi^{2n+1} \cdot \Omega_K^{4n}},$$

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 infinity type $(1, -1)$ and conductor prime to $p$, let $L_{p, \psi}(f) \in \Lambda_{R_0}$ 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 stated interpolation property for $L_p(f)$ is a reformulation of [CH17, Thm. 3.8]. Since the construction of $L_{p, \psi}(f)$ given in [CH17, §3.3] readily extends to the case $p \mid N$, with the $p$-adic multiplier $\varepsilon_p(f, \phi)$ in loc.cit. reducing to $1 - a_p p^{-1} \phi(p)$ for unramified $\phi$ (see also [Cas17a, Thm. 2.10]), the result follows. \qed

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

$$L_p^\Sigma(f) := L_p(f) \times \prod_{w \in \Sigma} P_w(\epsilon \Psi^{-1}(\gamma_w)) \in \Lambda_{R_0},$$

where $P_w(X) := \det(1 - X \cdot \text{Frob}_w|V^I_w)$, $\epsilon : G_K \to \mathbb{Z}_p^\times$ 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 $\Gamma$. 


A p-adic Waldspurger formula. Recall that the elliptic curve $E$ 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 $\omega_f = \sum a_n q^n dq$ is the one-form on $J_0(N)$ associated with $f$, then
\[
(3.2) \quad \pi^*(\omega_E) = c \cdot \omega_f,
\]
where $c \in \mathbb{Z}$ is the Manin constant. Since $N$ is square-free, we have $p \nmid c$ by [Maz78, Cor. 4.1].

We will have use for the following formula for the value at the trivial character $\phi = 1$ (which lies outside the range of interpolation) of the $p$-adic $L$-function of Theorem 3.1.

**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
\[
\Delta = [(A(A[N]) - (\infty))] \in J_0(N)(H),
\]
where $H$ is the Hilbert class field of $K$, and $(A, A[N])$ 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
\[
(3.3) \quad L_p(f, 1) = (1 - a_p p^{-1} + \varepsilon_p)^2 \cdot \left( \sum_{\sigma \in \text{Gal}(H/K)} \text{AJ}_F(\Delta^\sigma)(\omega_f) \right)^2.
\]
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:

$$\log_{\omega_f}(\Delta) = \log_{\pi^*(\omega_E)}(\pi(\Delta)) = \log_{\omega_E}(\pi(\Delta))$$

Thus, taking $P_K := \sum_{\sigma \in \text{Gal}(H/K)} \pi(\Delta^\sigma) \in E(K)$, the result follows.

4. Main conjectures

Let $M$ be a square-free integer prime to $p$, and let $f \in \mathbb{I}[q]$ be an ordinary $\mathbb{I}$-adic cusp eigenform of tame level $M$ as in Section 2, with associated residual representation $\bar{\rho}_f$. Letting $D_p \subseteq G_\mathbb{Q}$ 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 $L/\mathbb{Q}_p$ with associated Galois representation $V_f$, we may define the Selmer group $X^\Sigma_{Gr}(A_f)$ as in §2.2, replacing $T = T_pE$ by a fixed $G_\mathbb{Q}$-stable $\mathcal{O}_L$-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 $q | M$ 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 primes not lying above $p$, then $X^\Sigma_{Gr}(A_f)$ is $\Lambda$-torsion, and

$$\text{Ch}_\Lambda(X^\Sigma_{Gr}(A_f))-\Lambda_0 = (L^{\Sigma}_p(f)),$$

where $L_p^\Sigma(f)$ is as in (3.1).

**Proof.** As in the proof of [JSW17, Thm. 6.1.6], the result for an arbitrary finite set $\Sigma$ follows immediately from the case $\Sigma = \emptyset$, which is the content of [Cas17c, Thm. 3.4]. (In [Cas17c] it is assumed that $f$ has rational Fourier coefficients but the extension of the aforementioned result to the setting considered here is immediate.)

Recall that $\Lambda_\mathbb{I}$ denotes the anticyclotomic Iwasawa algebra over $\mathbb{I}$, and set $\Lambda_{\mathbb{I},R_0} := \Lambda_\mathbb{I} \otimes_{\mathbb{Z}_p} R_0$. For any $\phi \in \Lambda'_{\mathbb{I}}$, set $\phi := \ker(\phi)\Lambda_{\mathbb{I},R_0}$. 
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 \( X_{Gr}^\Sigma(A_f) \) is \( \Lambda_\Sigma \)-torsion, and

\[
Ch_{\Lambda}(X_{Gr}^\Sigma(A_f))_{\Lambda_{\mathbb{L},R_0}} = (L_p^\Sigma(f)),
\]

where \( L_p^\Sigma(f) \in \Lambda_{\mathbb{L},R_0} \) is such that

\[
L_p^\Sigma(f) \mod \bar{\psi}_\phi = L_p^\Sigma(f_\phi)
\]

for all \( \phi \in \mathcal{X}_\mathbb{L}^\omega \).

Proof. Let \( L_p,\xi(f) \in \Lambda_{\mathbb{L},R_0} \) be the two-variable anticyclotomic \( p \)-adic \( L \)-function constructed in [Cas17b, §2.6], and set

\[
L_p(f) := \text{Tw}_{\xi^{-1}}(L_p,\xi(f)),
\]

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 \( \text{Tw}_{\xi^{-1}} : \Lambda_{\mathbb{L},R_0} \to \Lambda_{\mathbb{L},R_0} \) is the \( R_0 \)-linear isomorphism given by \( \gamma \mapsto \xi^{-1}(\gamma)\gamma \) for \( \gamma \in \Gamma \). Viewing \( \lambda \) as a character on \( \mathbb{A} \times \mathbb{A} \), let \( \lambda^\tau \) denote the composition of \( \lambda \) with the action of complex conjugation on \( \mathbb{A} \times \mathbb{A} \). If the character \( \psi \) appearing in the proof of Theorem 3.1 is taken to be \( \psi = \lambda/\lambda^\tau \), the proof of [Cas17b, Thm. 2.11] shows that \( L_p(f) \) reduces to \( L_p(f_\phi) \) modulo \( \bar{\psi}_\phi \) for all \( \phi \in \mathcal{X}_\mathbb{L}^\omega \). Similarly as in (3.1), if for any \( \Sigma \) as above we set

\[
L_p^\Sigma(f) := L_p(f) \times \prod_{w \in \Sigma} P_{\lambda,w}(\epsilon \Psi^{-1}(\gamma_w)) \in \Lambda_{\mathbb{L},R_0},
\]

where \( P_{\lambda,w}(X) := \det(1 - X \cdot \text{Frob}_w | (T_{I_T} \otimes I_{F_\mathbb{L}})^I_w) \), with \( F_\mathbb{L} \) the fraction field of \( \mathbb{L} \), the specialization property (4.1) thus follows.

Let \( \phi \in \mathcal{X}_\mathbb{L}^\omega \) 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 \( X_{Gr}^\Sigma(A_f) \) is \( \Lambda \)-torsion, and we have

\[
Ch_{\Lambda}(X_{Gr}^\Sigma(A_f))_{\Lambda_{\mathbb{L},R_0}} = (L_p^\Sigma(f)).
\]
In particular, by Theorem 2.6 (with \( A_f \) in place of \( E[p^{\infty}] \)) it follows that \( X_{\text{Gr}}^\Sigma(A_f) \) is \( \Lambda_\ell \)-torsion. On the other hand, from [Wan14a, Thm. 1.1] we have the divisibility

\[(4.3) \quad Ch_{\Lambda_\ell}(X_{\text{Gr}}^\Sigma(A_f))_{\Lambda_{I,R_0}} \subseteq (L^\Sigma_p(f)^-)\]

in \( \Lambda_{I,R_0} \), where \( L^\Sigma_p(f)^- \) is the projection onto \( \Lambda_{I,R_0} \) of the \( p \)-adic \( L \)-function constructed in [Wan14a, §7.4]. Since a straightforward extension of the calculations in [JSW17, §5.3] shows that

\[(4.4) \quad (L^\Sigma_p(f)^-) = (L^\Sigma_p(f))\]

as ideals in \( \Lambda_{I,R_0} \), the result follows from an application of [SU14, Lem. 3.2] using (4.2), (4.3), and (4.4). (Note that the possible powers of \( p \) in [JSW17, 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 4.2 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 4.1), we will require the following technical result.

**Lemma 4.3.** Let \( X_{\text{Gr}}^\Sigma(A_f)_{\text{null}} \) be the largest pseudo-null \( \Lambda_\ell \)-submodule of \( X_{\text{Gr}}^\Sigma(A_f) \), let \( \wp \subset \mathfrak{p} \) be a height one prime, and let \( \wp := \wp \Lambda_\ell \). With hypotheses as in Theorem 4.2, the quotient

\[X_{\text{Gr}}^\Sigma(A_f)_{\text{null}}/\wp X_{\text{Gr}}^\Sigma(A_f)_{\text{null}}\]

is a pseudo-null \( \Lambda_\ell/\wp \)-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 \( \wp \), the proof of [Och06, Lem. 7.2] carries through with only small changes. (Note that the argument in loc. cit. requires knowing that \( X_{\text{ac}}^\Sigma(M_f[\wp]) \) is \( \Lambda_1/\wp \)-torsion, but this follows immediately from Theorem 4.2 and the isomorphism of Theorem 2.6.)

For the next result, let \( E/Q \) be a semistable elliptic curve of conductor \( N \), and assume that \( K \) satisfies hypothesis (Heeg) relative to \( N \), and that \( p = p\wp \) splits in \( K \).

**Theorem 4.4.** Assume that \( \bar{\rho}_{E,p} : G_K \to \text{Aut}_{\mathbf{F}_p}(E[p]) \simeq \text{GL}_2(\mathbf{F}_p) \) is irreducible and ramified at every prime \( q \mid N \) 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. [CW17, Thm. 6.1]). (Note that by [Ski14, Lem. 2.8.1] the hypotheses in Theorem 4.4 imply that \( \bar{\rho}_{E,p}|_{G_K} \) 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. [Ski16, Lem. 2.1.2]); in particular, \( f \) is \( p \)-ordinary. Let \( f \in \mathbb{I}[[q]] \) be the ordinary \( \mathbb{I} \)-adic cusp eigenform of tame level

\[
N_0 := N/p
\]

attached to \( f \), so that \( f_\phi = f \) for some \( \phi \in \mathbb{X}_1^p \). Let \( \varphi := \ker(\phi) \subseteq \mathbb{I} \) be the associated height one prime, and set

\[
\varphi := \varphi_{\mathbb{I},R_0}, \quad \Lambda_{\mathbb{I},R_0} := \Lambda_{\mathbb{I},R_0}/\varphi, \quad \varphi_0 := \varphi \cap \Lambda_{\mathbb{I}}, \quad \Lambda_{\mathbb{I}} := \Lambda_{\mathbb{I}}/\varphi_0.
\]

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 [JSW17, Thm. 6.1.6], it suffices to show that

\[
(4.5) \quad \text{Ch}_\Lambda(X^\Sigma_{ac}(E[p^\infty])) \Lambda_{R_0} = (L^\Sigma_p(f)).
\]

Since \( f \) specializes \( f \), which has weight 2 and trivial nebentypus, the residual representation \( \bar{\rho}_f \simeq \bar{\rho}_{E,p} \) is automatically \( p \)-distinguished (see [KLZ17, Rem. 7.2.7]). Thus our assumptions imply that the hypotheses in Theorem 4.2 are satisfied, which combined with Theorem 2.6 show that \( X^\Sigma_{Gr}(E[p^\infty]) \) is \( \Lambda \)-torsion. Moreover, letting \( I \) be any height one prime of \( \Lambda_{\mathbb{I},R_0} \) and setting \( I_0 := I \cap \Lambda_{\mathbb{I}} \), by Theorem 2.6 we have

\[
(4.6) \quad \text{length}_{(\Lambda_{\mathbb{I}})_{I_0}}(X^\Sigma_{Gr}(E[p^\infty])_{I_0}) = \text{length}_{(\Lambda_{\mathbb{I}})_{I_0}}((X^\Sigma_{Gr}(A_f)/\varphi_0 X^\Sigma_{Gr}(A_f))_{I_0}).
\]

On the other hand, if \( I \subseteq \Lambda_{\mathbb{I},R_0} \) is a height one prime mapping to \( I \) under the specialization map \( \Lambda_{\mathbb{I},R_0} \to \Lambda_{\mathbb{I},R_0} \) and we set \( I_0 := I \cap \Lambda_{\mathbb{I}} \), by Theorem 4.2 we have

\[
(4.7) \quad \text{length}_{(\Lambda_{\mathbb{I}})_{I_0}}(X^\Sigma_{Gr}(A_f)_{I_0}) = \text{ord}_I([L^\Sigma_p(f) \mod \varphi]) = \text{ord}_I([L^\Sigma_p(f)]).
\]
On the $p$-part of the Birch–Swinnerton-Dyer formula

Since Lemma 4.3 implies the equality

$$\text{length}_{(\Lambda,\psi)}((X_{G_1}^\Sigma(A_f)/\tilde{\cal{Q}}_0 X_{G_1}^\Sigma(A_f))_{\overline{\psi}}) = \text{length}_{(\Lambda,\psi)}(X_{G_1}^\Sigma(A_f)_{\overline{\psi}}),$$

combining (4.6) and (4.7) we conclude that

$$\text{length}_{(\Lambda,\psi)}(X_{G_1}^\Sigma(E[p^\infty])_{\overline{\psi}}) = \text{ord}_1(L_p^\Sigma(f))$$

for every height one prime $l$ of $\Lambda_{\psi,R_0}$, and so

(4.8)

$$\text{Ch}_\Lambda(X_{G_1}^\Sigma(E[p^\infty]))_{\Lambda R_0} = (L_p^\Sigma(f)).$$

Finally, since our hypothesis on $\bar{\rho}_{E,p}$ implies that $c_w(E/K)$ is a $p$-adic unit for every prime $w$ which is nonsplit in $K$ (see e.g. [PW11, Def. 3.3]), we have $\text{Ch}_\Lambda(X_{G_1}^\Sigma(E[p^\infty])) = \text{Ch}_\Lambda(X_{ac}^\Sigma(E[p^\infty]))$ by Proposition 2.5. Thus (4.8) reduces to (4.5), and the proof of Theorem 4.4 follows.

5. Proof of Theorem A

Let $E/\mathbb{Q}$ 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 $p | N$ 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 [JSW17, §7.4].

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

- $q$ 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 $p | N$ the third condition is redundant.) By Theorem 4.4 and Proposition 3.2 we have the equalities

(5.1)  \[ \#\mathbb{Z}_p/fac(0) = \#\mathbb{Z}_p/L_p(f,1) = \left( \#\mathbb{Z}_p/(1-a_p p^{-1} + \varepsilon_p) \log_{\omega_E} P_K \right)^2, \]

where $\varepsilon_p = p^{-1}$ if $p \nmid N$ and $\varepsilon_p = 0$ otherwise, and $P_K \in E(K)$ is a Heegner point. Since we assume that $\text{ord}_{s=1} L(E,s) = 1$, the nonvanishing of $L(E^D,1)$ implies that $\text{ord}_{s=1} L(E/K,s) = 1$, and so $P_K$ has infinite order, $\text{rank}_\mathbb{Z}(E(K)) = 1$ and $\#\Pi(E/K) < \infty$ 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 $\#Z_p/f_{ac}(0)$ that combined with (5.1) immediately leads to

$$\text{ord}_p(\#\text{III}(E/K)[p^\infty])$$

(5.2)

$$= 2 \cdot \text{ord}_p([E(K) : Z.P_K]) - \sum_{w|N^+} \text{ord}_p(c_w(E/K)),$$

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 $w | q$ (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

$$\text{ord}_p(\#\text{III}(E/K)[p^\infty])$$

(5.3)

$$= 2 \cdot \text{ord}_p([E(K) : Z.P_K]) - \sum_{w|N} \text{ord}_p(c_w(E/K)).$$

On the other hand, as in [JSW17, Eqn. (7.4.c)], the Gross–Zagier formula in our case [GZ86], [YZZ13] (as refined in [CST14]) can be rewritten as the equality

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

up to a $p$-adic unit,\(^1\) which combined with (5.3) and the immediate relation

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

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

$$\text{ord}_p(\#\text{III}(E/K)[p^\infty])$$

$$= \text{ord}_p\left(\frac{L'(E, 1)}{\Omega_E \cdot \text{Reg}(E/\mathbb{Q}) \prod_{\ell|N} c_\ell(E/\mathbb{Q})} \cdot \frac{L(E^D, 1)}{\Omega_{E^D} \prod_{\ell|N} c_\ell(E^D/\mathbb{Q})}\right).$$

Finally, since $L(E^D, 1) \neq 0$, by the known $p$-part of the Birch–Swinnerton-Dyer formula in analytic rank zero (as recalled in [JSW17, Thm. 7.2.1]) and the isomorphism $\text{III}(E/K)[p^\infty] \simeq \text{III}(E/\mathbb{Q})[p^\infty] \oplus \text{III}(E^D/\mathbb{Q})[p^\infty]$ we arrive at

\(^1\)This 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.
On the $p$-part of the Birch–Swinnerton-Dyer formula

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

concluding the proof of the theorem. \hfill \Box

References


On the $p$-part of the Birch–Swinnerton-Dyer formula


FRANCESC CASTELLA
DEPARTMENT OF MATHEMATICS
PRINCETON UNIVERSITY
FINE HALL, WASHINGTON ROAD
PRINCETON, NJ 08544
USA
E-mail address: fcabello@math.princeton.edu

RECEIVED APRIL 21, 2017