Cambridge Journal of Mathematics
Volume 6, Number 1, 1–23, 2018

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

Francesc Castella

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

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

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

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

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).

- $\mathrm{Reg}(E/\mathbf{Q})$ *is the discriminant of the Néron–Tate height pairing on* $E(\mathbf{Q})\otimes\mathbf{R}$*;*
- Ω_E *is the real Néron period of* E*;*
- $Ш(E/\mathbf{Q})$ *is the Tate–Shafarevich group of* E*; and*
- $c_\ell(E/\mathbf{Q})$ *is the Tamagawa number of* E *at the prime* ℓ*.*

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.* [CÇSS17, 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 $p\nmid N$) is naturally divided into two steps:

1. *Exact lower bound on the predicted* $\#Ш(E/\mathbf{Q})[p^\infty]$. For this part of the argument, in [JSW17] one chooses a suitable imaginary quadratic field $K_1=\mathbf{Q}(\sqrt{D_1})$ 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 $\#Ш(E/K_1)<\infty$ by the work of Gross–Zagier and Kolyvagin. The lower bound

$$\begin{aligned}\mathrm{ord}_p(\#Ш(E/K_1)[p^\infty]) &\geqslant 2\cdot\mathrm{ord}_p([E(K_1):\mathbf{Z}.P_{K_1}])\\ &\quad-\sum_{\substack{w\mid N^+\\ w\ \text{split}}}\mathrm{ord}_p(c_w(E/K_1)),\end{aligned}\tag{1.1}$$

   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 $X_{\mathrm{ac}}(E[p^\infty])$ 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 $X_{\mathrm{ac}}(E[p^\infty])$, namely the divisibility

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

where $f = \sum_{n=1}^\infty a_n q^n$ is the weight 2 newform associated with E, Λ_{R_0} is a scalar extension of the anticyclotomic Iwasawa algebra Λ for K_1, and $L_p(f) \in \Lambda_{R_0}$ is an 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):

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

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 $E^{D_1}/\mathbf{Q}$ (being of analytic rank zero, this follows from [SU14] and [Wan14c]), inequality (1.1) easily yields the exact lower bound for $\#\text{Ш}(E/\mathbf{Q})[p^\infty]$ predicted by the BSD conjecture.

2. *Exact upper bound on the predicted* $\#\text{Ш}(E/\mathbf{Q})[p^\infty]$. For the second part of the argument, in [JSW17] one chooses an imaginary quadratic field $K_2 = \mathbf{Q}(\sqrt{D_2})$ (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:

$$\mathrm{ord}_p(\#\text{Ш}(E/K_2)[p^\infty]) \leqslant 2 \cdot \mathrm{ord}([E(K_2) : \mathbf{Z}.P_{K_2}]), \tag{1.2}$$

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 $E^{D_2}/\mathbf{Q}$, inequality (1.2) then yields the predicted optimal upper bound for $\#\text{Ш}(E/\mathbf{Q})[p^\infty]$.

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 [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 $X_{\mathrm{ac}}(E[p^\infty])$:

$$Ch_\Lambda(X_{\mathrm{ac}}(E[p^\infty]))\Lambda_{R_0} = (L_p(f)). \tag{1.3}$$

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 $\text{Ш}(E/\mathbf{Q})[p^\infty]$ 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 $\mathbf{f} \in \mathbb{I}[[q]]$ 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:

$$Ch_{\Lambda_{\mathbb{I}}}(X_{\mathrm{ac}}(A_{\mathbf{f}}))\Lambda_{\mathbb{I},R_0} = (L_p(\mathbf{f})),$$

where $L_p(\mathbf{f}) \in \Lambda_{\mathbb{I},R_0}$ is the two-variable anticyclotomic p-adic L-function introduced in [Cas17b]. By construction, $L_p(\mathbf{f})$ specializes to $L_p(f)$ in weight 2, and by a control theorem for the Hida variable, the characteristic ideal of $X_{\mathrm{ac}}(A_{\mathbf{f}})$ similarly specializes to $Ch_\Lambda(X_{\mathrm{ac}}(E[p^\infty]))$, 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:

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

we arrive at the predicted formula for $\#\text{Ш}(E/\mathbf{Q})[p^\infty]$ 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 $E/\mathbf{Q}$ be a semistable elliptic curve of conductor N, and let $p \geqslant 5$ be a prime such that the mod p Galois representations

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

is irreducible. Let $T = T_p(E)$ be the p-adic Tate module of E, and set $V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.

Let K be an imaginary quadratic field in which $p = \mathfrak{p}\overline{\mathfrak{p}}$ splits, and for every place w of K define the *anticyclotomic local condition* $H^1_{\mathrm{ac}}(K_w, V) \subseteq H^1(K_w, V)$ by

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

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

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

$$H^1_{\mathrm{ac}}(K, E[p^\infty]) := \ker\biggl\{H^1(K, E[p^\infty]) \longrightarrow \prod_w \frac{H^1(K_w, E[p^\infty])}{H^1_{\mathrm{ac}}(K_w, E[p^\infty])}\biggr\},$$

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

Let $\Gamma = \mathrm{Gal}(K_\infty/K)$ 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 Λ-module

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

where $\Lambda^* = \mathrm{Hom}_{\mathrm{cont}}(\Lambda, \mathbf{Q}_p/\mathbf{Z}_p)$ is the Pontrjagin dual of Λ^{ac}. Letting $\rho_{E,p}$ denote the natural action of $G_K := \mathrm{Gal}(\overline{\mathbf{Q}}/K)$ on T, the G_K-action on M is given by $\rho_{E,p} \otimes \Psi^{-1}$, where Ψ is the composite character $G_K \twoheadrightarrow \Gamma \hookrightarrow \Lambda^\times$.

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

$$\mathrm{Sel}_{\mathfrak{p}}(K_\infty, E[p^\infty]) := \ker\biggl\{H^1(K,M) \longrightarrow H^1(K_{\mathfrak{p}}, M) \oplus \prod_{w\nmid p} H^1(K_w, M)\biggr\}.$$

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

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

which is easily shown to be a finitely generated Λ-module.

2.2. Control theorems

Let E, p, and K be an 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

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

the formal group logarithm attached to a fixed invariant differential ω_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 Σ be any set of places of K not dividing p, and assume that* $\mathrm{rank}_{\mathbf{Z}}(E(K)) = 1$ *and that* $\#\text{Ш}(E/K)[p^\infty] < \infty$. *Then $X_{\mathrm{ac}}^{\Sigma}(E[p^\infty])$ is Λ-torsion, and letting $f_{\mathrm{ac}}^{\Sigma}(T) \in \Lambda$ be a generator of $Ch_\Lambda(X_{\mathrm{ac}}^{\Sigma}(E[p^\infty]))$, we have*

$$\#\mathbf{Z}_p/f_{\mathrm{ac}}^{\Sigma}(0) = \#\text{Ш}(E/K)[p^\infty] \cdot \left(\frac{\#\mathbf{Z}_p/((1 - a_p p^{-1} + \varepsilon_p)\log_{\omega_E} P)}{[E(K) \otimes \mathbf{Z}_p : \mathbf{Z}_p.P]}\right)^2$$
$$\times \prod_{\substack{w \mid N^+ \\ w \notin \Sigma}} c_w(E/K)_p \cdot \prod_{w \in \Sigma} \#H^1(K_w, E[p^\infty]),$$

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 $\mathrm{corank}_{\mathbf{Z}_p}\mathrm{Sel}(K, E[p^\infty]) = 1$ and that the natural map

$$E(K) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow E(K_w) \otimes \mathbf{Q}_p/\mathbf{Z}_p$$

is surjective for all $w \mid p$. By [JSW17, Prop. 3.2.1] it follows that $H^1_{\mathrm{ac}}(K, E[p^\infty])$ is finite with

$$\#H^1_{\mathrm{ac}}(K, E[p^\infty]) = \#\text{Ш}(E/K)[p^\infty] \cdot \frac{[E(K_\mathfrak{p})_{/\mathrm{tors}} \otimes \mathbf{Z}_p : \mathbf{Z}_p.P]^2}{[E(K) \otimes \mathbf{Z}_p : \mathbf{Z}_p.P]^2}, \tag{2.1}$$

where $E(K_\mathfrak{p})_{/\mathrm{tors}} := E(K_\mathfrak{p})/E(K_\mathfrak{p})_{\mathrm{tors}}$ is the quotient $E(K_\mathfrak{p})$ by its maximal torsion submodule, and $P \in E(K)$ is any point of infinite order. If $p \nmid N$, then

$$[E(K_\mathfrak{p})_{/\mathrm{tors}} \otimes \mathbf{Z}_p : \mathbf{Z}_p.P] = \frac{\#\mathbf{Z}_p/((\frac{1-a_p+p}{p}) \log_{\omega_E} P)}{\#H^0(K_\mathfrak{p}, E[p^\infty])} \tag{2.2}$$

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

$$\begin{aligned} &\#H^1_{\mathrm{ac}}(K, E[p^\infty]) \\ &= \#\text{Ш}(E/K)[p^\infty] \cdot \left(\frac{\#\mathbf{Z}_p/((\frac{1-a_p+p}{p}) \log_{\omega_E} P)}{[E(K) \otimes \mathbf{Z}_p : \mathbf{Z}_p.P] \cdot \#H^0(K_\mathfrak{p}, E[p^\infty])}\right)^2, \end{aligned}$$

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

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

$$0 \longrightarrow E_1(K_\mathfrak{p}) \longrightarrow E_0(K_\mathfrak{p}) \longrightarrow \tilde{E}_{\mathrm{ns}}(\mathbf{F}_p) \longrightarrow 0. \tag{2.3}$$

The formal group logarithm defines an injective homomorphism

$$\log_{\omega_E} : E(K_\mathfrak{p})_{/\mathrm{tor}} \otimes \mathbf{Z}_p \longrightarrow \mathbf{Z}_p$$

mapping $E_1(K_{\mathfrak{p}})$ isomorphically onto $p\mathbf{Z}_p$, and hence we see that

$$\begin{aligned}
[E(K_{\mathfrak{p}})_{/\mathrm{tors}} \otimes \mathbf{Z}_p : \mathbf{Z}_p.P] &= \frac{\#\mathbf{Z}_p/(\log_{\omega_E} P)}{\#\mathbf{Z}_p/(\log_{\omega_E}(E(K_{\mathfrak{p}})_{/\mathrm{tors}} \otimes \mathbf{Z}_p))} \\
&= \frac{\#\mathbf{Z}_p/(\log_{\omega_E} P) \cdot \#(E(K_{\mathfrak{p}})/E_1(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p)}{\#\mathbf{Z}_p/p\mathbf{Z} \cdot \#(E(K_{\mathfrak{p}})_{\mathrm{tors}} \otimes \mathbf{Z}_p)} \\
&= [E(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})]_p \cdot \frac{\#\mathbf{Z}_p/(\log_{\omega_E} P) \cdot \#(E_0(K_{\mathfrak{p}})/E_1(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p)}{\#\mathbf{Z}_p/p\mathbf{Z}_p \cdot \#(E(K_{\mathfrak{p}})_{\mathrm{tors}} \otimes \mathbf{Z}_p)},
\end{aligned}$$

where in the second equality $[E(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})]_p$ denotes the p-part of the index $[E(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})]$. By (2.3), we have

$$E_0(K_{\mathfrak{p}})/E_1(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p \simeq \tilde{E}_{\mathrm{ns}}(\mathbf{F}_p) \otimes \mathbf{Z}_p,$$

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

$$[E(K_{\mathfrak{p}})_{/\mathrm{tors}} \otimes \mathbf{Z}_p : \mathbf{Z}_p.P] = [E(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})]_p \cdot \frac{\#\mathbf{Z}/(\frac{1}{p}\log_{\omega_E} P)}{\#H^0(K_{\mathfrak{p}}, E[p^\infty])}, \tag{2.4}$$

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

$$\begin{aligned}
&\#H^1_{\mathrm{ac}}(K, E[p^\infty]) \\
&= \#\text{Ш}(E/K)[p^\infty] \cdot \left(\frac{[E(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})]_p \cdot \#\mathbf{Z}_p/(\frac{1}{p}\log_{\omega_E} P)}{[E(K) \otimes \mathbf{Z}_p : \mathbf{Z}_p.P] \cdot \#H^0(K_{\mathfrak{p}}, E[p^\infty])}\right)^2.
\end{aligned}$$

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

$$\begin{aligned}
&\#\mathbf{Z}_p/f^{\Sigma}_{\mathrm{ac}}(0) \\
&= \#\text{Ш}(E/K)[p^\infty] \cdot \left(\frac{\#\mathbf{Z}_p/(\frac{1}{p}\log_{\omega_E} P)}{[E(K) \otimes \mathbf{Z}_p : \mathbf{Z}_p.P]}\right)^2 \cdot [E(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})]_p^2 \\
&\quad \times \prod_{\substack{w \in S \smallsetminus \Sigma \\ w \nmid p \text{ split}}} \#H^1_{\mathrm{ur}}(K_w, E[p^\infty]) \cdot \prod_{w \in \Sigma} \#H^1(K_w, E[p^\infty]),
\end{aligned} \tag{2.5}$$

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

$$[E(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})]_p = c_w(E/K)_p \tag{2.6}$$

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

$$\#H^1_{\mathrm{ur}}(K_w, E[p^\infty]) = c_w(E/K)_p \tag{2.7}$$

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. $\square$

Control Theorem for Greenberg Selmer groups. Let $\Lambda_W = \mathbf{Z}_p[[W]]$ be the one-variable power series ring in the indeterminate W. Let M be an integer prime to p, let χ be a Dirichlet character modulo pM, and let

$$\mathbf{f} = \sum_{n=1}^{\infty} \mathbf{a}_n q^n \in \mathbb{I}[[q]]$$

be an ordinary $\mathbb{I}$-adic cusp eigenform of tame level M and character χ (as defined in [SU14, §3.3.9]) defined over a local reduced finite integral extension $\mathbb{I}/\Lambda_W$.

Let $\mathcal{X}^a_{\mathbb{I}}$ the set of continuous $\mathbf{Z}_p$-algebra homomorphisms $\phi : \mathbb{I} \to \overline{\mathbf{Q}}_p$ whose composition with the structural map $\Lambda_W \to \mathbb{I}$ is given by $\phi(1+W) = (1+p)^{k_\phi - 2}$ for some integer $k_\phi \in \mathbf{Z}_{\geqslant 2}$ called the *weight* of ϕ. Then for all $\phi \in \mathcal{X}^a_{\mathbb{I}}$ we have

$$\mathbf{f}_\phi = \sum_{n=1}^{\infty} \phi(\mathbf{a}_n) q^n \in S_{k_\phi}(\Gamma_0(pM), \chi\omega^{2-k_\phi}),$$

where ω is the Teichmüller character. We shall only need consider the case where χ is the trivial character, in which case for all $\phi \in \mathcal{X}^a_{\mathbb{I}}$ of weight $k_\phi \equiv 2 \pmod{p-1}$, either

(1) $\mathbf{f}_\phi$ is a newform on $\Gamma_0(pM)$; or
(2) $\mathbf{f}_\phi$ 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

$$\bar\rho_{\mathbf{f}} : G_{\mathbf{Q}} := \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(k_{\mathbb{I}})$$

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

$$T_{\mathbf{f}} \otimes_{\mathbb{I}} \phi(\mathbb{I}) \simeq T_{\mathbf{f}_\phi},$$

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

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

$$M_{\mathbf{f}} := T_{\mathbf{f}} \otimes_{\mathbb{I}} \Lambda_{\mathbb{I}}^*,$$

where $\Lambda_{\mathbb{I}}^* = \mathrm{Hom}_{\mathrm{cont}}(\Lambda_{\mathbb{I}}, \mathbf{Q}_p/\mathbf{Z}_p)$ is the Pontrjagin dual of $\Lambda_{\mathbb{I}}$. This is equipped with a natural G_K-action defined similarly as for the Λ-module $M = T \otimes_{\mathbf{Z}_p} \Lambda^*$ introduced in §2.1.

Definition 2.4. The *Greenberg Selmer group* of E over K_∞/K is

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

The *Greenberg Selmer group* $\mathfrak{Sel}_{\mathrm{Gr}}(K_\infty, A_{\mathbf{f}})$ for $\mathbf{f}$ over K_∞/K, where $A_{\mathbf{f}} := T_{\mathbf{f}} \otimes_{\mathbb{I}} \mathbb{I}^*$, is defined by replacing M by $M_{\mathbf{f}}$ in the above definition.

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

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

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

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

$$0 \longrightarrow \mathrm{Sel}_{\mathfrak{p}}(K_\infty, E[p^\infty]) \longrightarrow \mathfrak{Sel}_{\mathrm{Gr}}(K_\infty, E[p^\infty]) \longrightarrow \mathcal{H}_{\mathfrak{p}}^{\mathrm{ur}} \oplus \prod_{w \nmid p} \mathcal{H}_w^{\mathrm{ur}}, \tag{2.8}$$

where

$$\mathcal{H}_v^{\mathrm{ur}} := \ker\{H^1(K_v, M) \longrightarrow H^1(I_v, M)\}$$

is the set of unramified cocycles.

For a torsion Λ-module X, let $\lambda(X)$ (resp. $\mu(X)$) denote the λ-invariant (resp. μ-invariant) of a generator of $Ch_\Lambda(X)$.

Proposition 2.5. *Assume that $X^{\Sigma}_{\rm Gr}(E[p^\infty])$ is Λ-torsion. Then $X^{\Sigma}_{\rm ac}(E[p^\infty])$ is Λ-torsion, and we have the relations*

$$\lambda(X^{\Sigma}_{\rm Gr}(E[p^\infty])) = \lambda(X^{\Sigma}_{\rm ac}(E[p^\infty]))$$

and

$$\mu(X^{\Sigma}_{\rm Gr}(E[p^\infty])) = \mu(X^{\Sigma}_{\rm ac}(E[p^\infty])) + \sum_{\substack{w \text{ nonsplit} \\ w\notin\Sigma}} {\rm ord}_p(c_w(E/K)).$$

Proof. Since $X^{\Sigma}_{\rm ac}(E[p^\infty])$ is a quotient of $X^{\Sigma}_{\rm Gr}(E[p^\infty])$, the first claim of the proposition is clear. Consider the exact sequence (2.8) (or rather its variant for Σ-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 $\mathcal{H}^{\rm ur}_v$ vanishes. Since $M^{I_{\mathfrak{p}}} = \{0\}$, the term $\mathcal{H}^{\rm ur}_{\mathfrak{p}}$ also vanishes, and the aforementioned exact sequence thus reduces to

$$0 \longrightarrow {\rm Sel}^{\Sigma}_{\mathfrak{p}}(K_\infty, E[p^\infty]) \longrightarrow \mathfrak{Sel}^{\Sigma}_{\rm Gr}(K_\infty, E[p^\infty]) \longrightarrow \prod_{\substack{w \text{ nonsplit} \\ w\notin\Sigma}} \mathcal{H}^{\rm ur}_w. \tag{2.9}$$

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

$$\mathcal{H}^{\rm ur}_w \simeq (\mathbf{Z}_p/p^{t_E(w)}\mathbf{Z}_p) \otimes \Lambda^*,$$

where $t_E(w) := {\rm ord}_p(c_w(E/K))$ is the p-exponent of the Tamagawa number of E at w, and Λ^* is the Pontrjagin dual of Λ. In particular, $\mathcal{H}^{\rm ur}_w$ is Λ-torsion, with $\lambda(\mathcal{H}^{\rm ur}_w) = 0$ and $\mu(\mathcal{H}^{\rm ur}_w) = {\rm ord}_p(c_w(E/K))$. Since the rightmost arrow in (2.9) is surjective by [PW11, Prop. A.2], the result follows. $\square$

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 $\mathbf{f} \in \mathbb{I}[[q]]$ be the Hida family associated with f, let $\wp \subseteq \mathbb{I}$ be the kernel of the arithmetic map $\phi \in \mathcal{X}^a_{\mathbb{I}}$ such that $\mathbf{f}_\phi$ is either f itself (if $p \mid N$) or the ordinary p-stabilization of f (if $p \nmid N$), and set $\widetilde{\wp} := \wp\Lambda_{\mathbb{I}} \subseteq \Lambda_{\mathbb{I}}$. Since we assume that $\bar\rho_{E,p}$ is irreducible, so is $\bar\rho_{\mathbf{f}}$.

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*

$$X^{\Sigma}_{\rm Gr}(E[p^\infty]) \simeq X^{\Sigma}_{\rm Gr}(A_{\mathbf{f}})/\widetilde{\wp}X^{\Sigma}_{\rm Gr}(A_{\mathbf{f}}).$$

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

$$\mathrm{Sel}^{\Sigma}_{\mathrm{Gr}}(K_\infty, M_{\mathbf{f}}[\widetilde{\wp}]) \longrightarrow \mathrm{Sel}^{\Sigma}_{\mathrm{Gr}}(K_\infty, M_{\mathbf{f}})[\widetilde{\wp}] \tag{2.10}$$

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

$$\mathrm{Sel}^{\Sigma}_{\mathfrak{p}}(K_\infty, M_?) = \ker\left\{H^1(G_{K,S}, M_?) \xrightarrow{\mathrm{loc}_{\mathfrak{p}}} \frac{H^1(K_{\mathfrak{p}}, M_?)}{H^1_{\mathrm{Gr}}(K_{\mathfrak{p}}, M_?)}\right\}, \tag{2.11}$$

where $M_? = M_{\mathbf{f}}[\widetilde{\wp}]$ or $M_{\mathbf{f}}$, $G_{K,S}$ is the Galois group of the maximal extension of K unramified outside S, and

$$H^1_{\mathrm{Gr}}(K_{\mathfrak{p}}, M_?) := \ker\big\{H^1(K_{\mathfrak{p}}, M_?) \longrightarrow H^1(I_{\mathfrak{p}}, M_?)\big\}.$$

As shown in the proof of [SU14, Prop. 3.7] (taking $A = \Lambda_{\mathbb{I}}$ and $\mathfrak{a} = \widetilde{\wp}$ in *loc.cit.*), we have $H^1(G_{K,S}, M_{\mathbf{f}}[\widetilde{\wp}]) = H^1(G_{K,S}, M_{\mathbf{f}})[\widetilde{\wp}]$. On the other hand, using that $G_{K_{\mathfrak{p}}}/I_{\mathfrak{p}}$ has cohomological dimension one, we immediately see that

$$H^1(K_{\mathfrak{p}}, M_?)/H^1_{\mathrm{Gr}}(K_{\mathfrak{p}}, M_?) \simeq H^1(I_{\mathfrak{p}}, M_?)^{G_{K_{\mathfrak{p}}}},$$

From the long exact sequence in $I_{\mathfrak{p}}$-cohomology associated with $0 \to \Lambda_{\mathbb{I}}^*[\widetilde{\wp}] \to \Lambda_{\mathbb{I}}^* \to \widetilde{\wp}\Lambda_{\mathbb{I}}^* \to 0$ tensored with $T_{\mathbf{f}}$, we obtain

$$(M_{\mathbf{f}}^{I_{\mathfrak{p}}}/(T_{\mathbf{f}} \otimes_{\mathbb{I}} \widetilde{\wp}\Lambda_{\mathbb{I}}^*)^{I_{\mathfrak{p}}})^{G_{K_{\mathfrak{p}}}} \simeq \ker\big\{H^1(I_{\mathfrak{p}}, M_{\mathbf{f}}[\widetilde{\wp}])^{G_{K_{\mathfrak{p}}}} \longrightarrow H^1(I_{\mathfrak{p}}, M_{\mathbf{f}})^{G_{K_{\mathfrak{p}}}}\big\}.$$

Since $H^0(I_{\mathfrak{p}}, M_{\mathbf{f}}) = \{0\}$, we thus have a commutative diagram

$$\begin{tikzcd}
H^1(G_{K,S}, M_{\mathbf{f}}[\widetilde{\wp}]) \arrow[r, "\mathrm{loc}_{\mathfrak{p}}"] \arrow[d, "\simeq"] & H^1(K_{\mathfrak{p}}, M_{\mathbf{f}}[\widetilde{\wp}])/H^1_{\mathrm{Gr}}(K_{\mathfrak{p}}, M_{\mathbf{f}}[\widetilde{\wp}]) \arrow[d] \\
H^1(G_{K,S}, M_{\mathbf{f}})[\widetilde{\wp}] \arrow[r, "\mathrm{loc}_{\mathfrak{p}}"] & H^1(K_{\mathfrak{p}}, M_{\mathbf{f}})/H^1_{\mathrm{Gr}}(K_{\mathfrak{p}}, M_{\mathbf{f}})
\end{tikzcd}$$

in which the right vertical map is injective. By (2.11), the result follows. □

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 $\mathbf{Q}_p$, and set

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

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

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

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

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

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

$$L_p(f) := \mathrm{Tw}_{\psi^{-1}}(\mathscr{L}_{\mathfrak{p},\psi}(f)),$$

where $\mathrm{Tw}_{\psi^{-1}} : \Lambda_{R_0} \to \Lambda_{R_0}$ 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 $\mathscr{L}_{\mathfrak{p},\psi}(f)$ given in [CH17, §3.3] readily extends to the case $p \mid N$, with the p-adic multiplier $e_{\mathfrak{p}}(f, \phi)$ in *loc.cit.* reducing to $1 - a_p p^{-1}\phi(\mathfrak{p})$ for unramified ϕ (see also [Cas17a, Thm. 2.10]), the result follows. □

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

$$L_p^{\Sigma}(f) := L_p(f) \times \prod_{w \in \Sigma} P_w(\epsilon\Psi^{-1}(\gamma_w)) \in \Lambda_{R_0}, \tag{3.1}$$

where $P_w(X) := \det(1 - X \cdot \mathrm{Frob}_w | V^{I_w})$, $\epsilon : G_K \to \mathbf{Z}_p^\times$ is the p-adic cyclotomic character, $\mathrm{Frob}_w \in G_K$ is a geometric Frobenius element at w, and γ_w is the image of Frob_w in Γ.

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 $J_0(N) = \mathrm{Jac}(X_0(N))$ in the sense of [Maz78, §2], and fix a corresponding modular parametrization

$$\pi : X_0(N) \longrightarrow E$$

sending the cusp ∞ to the origin of E. If ω_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

$$\pi^*(\omega_E) = c \cdot \omega_f, \tag{3.2}$$

where $c \in \mathbf{Z}$ 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 $\phi = \mathbb{1}$ (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:*

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

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 $p \mid N$. Indeed, in our case, the generalized Heegner cycles Δ 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

$$L_p(f, \mathbb{1}) = (1 - a_p p^{-1} + \varepsilon_p)^2 \cdot \left(\sum_{\sigma \in \mathrm{Gal}(H/K)} \mathrm{AJ}_F(\Delta^\sigma)(\omega_f) \right)^2. \tag{3.3}$$

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

$$\mathrm{AJ}_F(\Delta)(\omega_f) = \log_{\omega_f}(\Delta),$$

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

4. Main conjectures

Let M be a square-free integer prime to p, and let $\mathbf{f} \in \mathbb{I}[[q]]$ be an ordinary $\mathbb{I}$-adic cusp eigenform of tame level M as in Section 2, with associated residual representation $\bar{\rho}_{\mathbf{f}}$. Letting $D_p \subseteq G_{\mathbf{Q}}$ be a fixed decomposition group at p, we say that $\bar{\rho}_{\mathbf{f}}$ is *p-distinguished* if the semisimplication of $\bar{\rho}_{\mathbf{f}}|_{D_p}$ is the direct sum of two distinct characters.

Let K be an imaginary quadratic field in which $p = \mathfrak{p}\bar{\mathfrak{p}}$ 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 $L/\mathbf{Q}_p$ with associated Galois representation V_f, we may define the Selmer group $X_{\mathrm{Gr}}^{\Sigma}(A_f)$ as in §2.2, replacing $T = T_pE$ by a fixed $G_{\mathbf{Q}}$-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 $q \mid M$ which is nonsplit in K, and there is at least one such prime;*
- *$\bar{\rho}_f|_{G_K}$ is irreducible.*

If Σ is any finite set of primes not lying above p, then $X_{\mathrm{Gr}}^{\Sigma}(A_f)$ is Λ-torsion, and

$$Ch_\Lambda(X_{\mathrm{Gr}}^{\Sigma}(A_f))\Lambda_{R_0} = (L_p^{\Sigma}(f)),$$

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 Σ 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.) $\square$

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

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

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

Then $X^{\Sigma}_{\mathrm{Gr}}(A_{\mathbf{f}})$ is $\Lambda_{\mathbb{I}}$-torsion, and

$$Ch_{\Lambda_{\mathbb{I}}}(X^{\Sigma}_{\mathrm{Gr}}(A_{\mathbf{f}}))\Lambda_{\mathbb{I},R_0} = (L^{\Sigma}_p(\mathbf{f})),$$

where $L^{\Sigma}_p(\mathbf{f}) \in \Lambda_{\mathbb{I},R_0}$ is such that

$$L^{\Sigma}_p(\mathbf{f}) \bmod \widetilde{\wp}_{\phi} = L^{\Sigma}_p(\mathbf{f}_{\phi}) \tag{4.1}$$

for all $\phi \in \mathcal{X}^a_{\mathbb{I}}$.

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

$$L_p(\mathbf{f}) := \mathrm{Tw}_{\boldsymbol{\xi}^{-1}}(\mathscr{L}_{\mathfrak{p},\boldsymbol{\xi}}(\mathbf{f})),$$

where $\boldsymbol{\xi}$ is the $\mathbb{I}$-adic character constructed in *loc.cit.* from a Hecke character λ of infinity type $(1,0)$ and conductor prime to p, and $\mathrm{Tw}_{\boldsymbol{\xi}^{-1}} : \Lambda_{\mathbb{I},R_0} \to \Lambda_{\mathbb{I},R_0}$ is the R_0-linear isomorphism given by $\gamma \mapsto \boldsymbol{\xi}^{-1}(\gamma)\gamma$ for $\gamma \in \Gamma$. Viewing λ as a character on $\mathbb{A}^{\times}_K$, let λ^{τ} denote the composition of λ with the action of complex conjugation on $\mathbb{A}^{\times}_K$. If the character ψ 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 $L_p(\mathbf{f})$ reduces to $L_p(\mathbf{f}_{\phi})$ modulo $\widetilde{\wp}_{\phi}$ for all $\phi \in \mathcal{X}^a_{\mathbb{I}}$. Similarly as in (3.1), if for any Σ as above we set

$$L^{\Sigma}_p(\mathbf{f}) := L_p(\mathbf{f}) \times \prod_{w \in \Sigma} P_{\mathbf{f},w}(\epsilon\Psi^{-1}(\gamma_w)) \in \Lambda_{\mathbb{I},R_0},$$

where $P_{\mathbf{f},w}(X) := \det(1 - X \cdot \mathrm{Frob}_w | (T_{\mathbf{f}} \otimes_{\mathbb{I}} F_{\mathbb{I}})^{I_w})$, with $F_{\mathbb{I}}$ the fraction field of $\mathbb{I}$, the specialization property (4.1) thus follows.

Let $\phi \in \mathcal{X}^a_{\mathbb{I}}$ be such that $\mathbf{f}_{\phi}$ is the p-stabilization of a p-ordinary newform $f \in S_2(\Gamma_0(M))$. By Theorem 4.2, the associated $X^{\Sigma}_{\mathrm{Gr}}(A_f)$ is Λ-torsion, and we have

$$Ch_{\Lambda}(X^{\Sigma}_{\mathrm{Gr}}(A_f))\Lambda_{R_0} = (L^{\Sigma}_p(f)). \tag{4.2}$$

In particular, by Theorem 2.6 (with A_f in place of $E[p^\infty]$) it follows that $X_{\rm Gr}^{\Sigma}(A_{\mathbf{f}})$ is $\Lambda_{\mathbb{I}}$-torsion. On the other hand, from [Wan14a, Thm. 1.1] we have the divisibility

$$Ch_{\Lambda_{\mathbb{I}}}(X_{\rm Gr}^{\Sigma}(A_{\mathbf{f}}))\Lambda_{\mathbb{I},R_0} \subseteq (\mathcal{L}_p^{\Sigma}(\mathbf{f})^-) \tag{4.3}$$

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

$$(\mathcal{L}_p^{\Sigma}(\mathbf{f})^-) = (L_p^{\Sigma}(\mathbf{f})) \tag{4.4}$$

as ideals in $\Lambda_{\mathbb{I},R_0}$, 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.) $\square$

In order to deduce from Theorem 4.2 the anticyclotomic main conjecture for arithmetic specializations of $\mathbf{f}$ (especially in the cases where the conductor of $\mathbf{f}_\phi$ is divisible by p, which are not covered by Theorem 4.1), we will require the following technical result.

Lemma 4.3. *Let $X_{\rm Gr}^{\Sigma}(A_{\mathbf{f}})_{\rm null}$ be the largest pseudo-null $\Lambda_{\mathbb{I}}$-submodule of $X_{\rm Gr}^{\Sigma}(A_{\mathbf{f}})$, let $\wp \subseteq \mathbb{I}$ be a height one prime, and let $\widetilde{\wp} := \wp\Lambda_{\mathbb{I}}$. With hypotheses as in Theorem 4.2, the quotient*

$$X_{\rm Gr}^{\Sigma}(A_{\mathbf{f}})_{\rm null}/\widetilde{\wp}X_{\rm Gr}^{\Sigma}(A_{\mathbf{f}})_{\rm null}$$

is a pseudo-null $\Lambda_{\mathbb{I}}/\widetilde{\wp}$-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 $\widetilde{\wp}$, the proof of [Och06, Lem. 7.2] carries through with only small changes. (Note that the argument in *loc.cit.* requires knowing that $X_{\rm ac}^{\Sigma}(M_{\mathbf{f}}[\widetilde{\wp}])$ is $\Lambda_{\mathbb{I}}/\widetilde{\wp}$-torsion, but this follows immediately from Theorem 4.2 and the isomorphism of Theorem 2.6.) $\square$

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

Theorem 4.4. *Assume that $\bar{\rho}_{E,p} : G_{\mathbf{Q}} \to {\rm Aut}_{\mathbf{F}_p}(E[p]) \simeq {\rm GL}_2(\mathbf{F}_p)$ 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 $Ch_\Lambda(X_{\mathrm{ac}}(E[p^\infty]))$ is Λ-torsion and*

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

Proof. If E has good ordinary (resp. supersingular) supersingular reduction at p, the result follows from [Cas17c, 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 $\mathbf{f} \in \mathbb{I}[[q]]$ be the ordinary $\mathbb{I}$-adic cusp eigenform of tame level

$$N_0 := N/p$$

attached to f, so that $\mathbf{f}_\phi = f$ for some $\phi \in \mathcal{X}_{\mathbb{I}}^a$. Let $\wp := \ker(\phi) \subseteq \mathbb{I}$ be the associated height one prime, and set

$$\widetilde{\wp} := \wp\Lambda_{\mathbb{I},R_0}, \quad \Lambda_{\wp,R_0} := \Lambda_{\mathbb{I},R_0}/\widetilde{\wp}, \quad \widetilde{\wp}_0 := \widetilde{\wp} \cap \Lambda_{\mathbb{I}}, \quad \Lambda_\wp := \Lambda_{\mathbb{I}}/\wp_0.$$

Let Σ 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

$$Ch_\Lambda(X_{\mathrm{ac}}^\Sigma(E[p^\infty]))\Lambda_{R_0} = (L_p^\Sigma(f)). \tag{4.5}$$

Since $\mathbf{f}$ specializes f, which has weight 2 and trivial nebentypus, the residual representation $\bar{\rho}_{\mathbf{f}} \simeq \bar{\rho}_{E,p}$ 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 $X_{\mathrm{Gr}}^\Sigma(E[p^\infty])$ is Λ-torsion. Moreover, letting $\mathfrak{l}$ be any height one prime of $\Lambda_{\wp,R_0}$ and setting $\mathfrak{l}_0 := \mathfrak{l} \cap \Lambda_\wp$, by Theorem 2.6 we have

$$\mathrm{length}_{(\Lambda_\wp)_{\mathfrak{l}_0}}(X_{\mathrm{Gr}}^\Sigma(E[p^\infty])_{\mathfrak{l}_0}) = \mathrm{length}_{(\Lambda_\wp)_{\mathfrak{l}_0}}((X_{\mathrm{Gr}}^\Sigma(A_{\mathbf{f}})/\widetilde{\wp}_0 X_{\mathrm{Gr}}^\Sigma(A_{\mathbf{f}}))_{\mathfrak{l}_0}). \tag{4.6}$$

On the other hand, if $\widetilde{\mathfrak{l}} \subseteq \Lambda_{\mathbb{I},R_0}$ is a height one prime mapping to $\mathfrak{l}$ under the specialization map $\Lambda_{\mathbb{I},R_0} \to \Lambda_{\wp,R_0}$ and we set $\widetilde{\mathfrak{l}}_0 := \widetilde{\mathfrak{l}} \cap \Lambda_{\mathbb{I}}$, by Theorem 4.2 we have

$$\mathrm{length}_{(\Lambda_{\mathbb{I}})_{\widetilde{\mathfrak{l}}_0}}(X_{\mathrm{Gr}}^\Sigma(A_{\mathbf{f}})_{\widetilde{\mathfrak{l}}_0}) = \mathrm{ord}_{\widetilde{\mathfrak{l}}}(L_p^\Sigma(\mathbf{f}) \bmod \widetilde{\wp}) = \mathrm{ord}_{\mathfrak{l}}(L_p^\Sigma(f)). \tag{4.7}$$

Since Lemma 4.3 implies the equality

$$\mathrm{length}_{(\Lambda_\wp)_{\mathfrak{l}_0}}((X^\Sigma_{\mathrm{Gr}}(A_{\mathbf{f}})/\widetilde{\wp}_0 X^\Sigma_{\mathrm{Gr}}(A_{\mathbf{f}}))_{\mathfrak{l}_0}) = \mathrm{length}_{(\Lambda_{\mathbb{I}})_{\widetilde{\mathfrak{l}}_0}}(X^\Sigma_{\mathrm{Gr}}(A_{\mathbf{f}})_{\widetilde{\mathfrak{l}}_0}),$$

combining (4.6) and (4.7) we conclude that

$$\mathrm{length}_{(\Lambda_\wp)_{\mathfrak{l}_0}}(X^\Sigma_{\mathrm{Gr}}(E[p^\infty])_{\mathfrak{l}_0}) = \mathrm{ord}_{\mathfrak{l}}(L^\Sigma_p(f))$$

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

$$Ch_\Lambda(X^\Sigma_{\mathrm{Gr}}(E[p^\infty]))\Lambda_{R_0} = (L^\Sigma_p(f)). \tag{4.8}$$

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 $Ch_\Lambda(X^\Sigma_{\mathrm{Gr}}(E[p^\infty])) = Ch_\Lambda(X^\Sigma_{\mathrm{ac}}(E[p^\infty]))$ 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 $E/\mathbf{Q}$ 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 [JSW17, §7.4].

Proof of Theorem A. Choose an imaginary quadratic field $K = \mathbf{Q}(\sqrt{D})$ 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 $p \mid N$ the third condition is redundant.) By Theorem 4.4 and Proposition 3.2 we have the equalities

$$\#\mathbf{Z}_p/f_{\mathrm{ac}}(0) = \#\mathbf{Z}_p/L_p(f,\mathbb{1}) = \left(\#\mathbf{Z}_p/(1 - a_p p^{-1} + \varepsilon_p)\log_{\omega_E} P_K\right)^2, \tag{5.1}$$

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 $\mathrm{ord}_{s=1}L(E,s) = 1$, the nonvanishing of $L(E^D,1)$ implies that $\mathrm{ord}_{s=1}L(E/K,s) = 1$, and so P_K has infinite order, $\mathrm{rank}_{\mathbf{Z}}(E(K)) = 1$ and $\#Ш(E/K) < \infty$ 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 $\#\mathbf{Z}_p/f_{\rm ac}(0)$ that combined with (5.1) immediately leads to

$$\begin{aligned}\tag{5.2} &\mathrm{ord}_p(\#\text{Ш}(E/K)[p^\infty]) \\ &\qquad = 2\cdot\mathrm{ord}_p([E(K):\mathbf{Z}.P_K]) - \sum_{w\mid N^+}\mathrm{ord}_p(c_w(E/K)),\end{aligned}$$

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 $\mathrm{ord}_p(c_w(E/K)) = 0$ for every $w \mid q$ (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

$$\begin{aligned}\tag{5.3} &\mathrm{ord}_p(\#\text{Ш}(E/K)[p^\infty]) \\ &\qquad = 2\cdot\mathrm{ord}_p([E(K):\mathbf{Z}.P_K]) - \sum_{w\mid N}\mathrm{ord}_p(c_w(E/K)).\end{aligned}$$

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

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

up to a p-adic unit,[1] which combined with (5.3) and the immediate relation

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

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

$$\begin{aligned}&\mathrm{ord}_p(\#\text{Ш}(E/K)[p^\infty]) \\ &\quad = \mathrm{ord}_p\biggl(\frac{L'(E,1)}{\Omega_E\cdot\mathrm{Reg}(E/\mathbf{Q})\prod_{\ell\mid N}c_\ell(E/\mathbf{Q})}\cdot\frac{L(E^D,1)}{\Omega_{E^D}\prod_{\ell\mid N}c_\ell(E^D/\mathbf{Q})}\biggr).\end{aligned}$$

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 $\text{Ш}(E/K)[p^\infty] \simeq \text{Ш}(E/\mathbf{Q})[p^\infty]\oplus\text{Ш}(E^D/\mathbf{Q})[p^\infty]$ 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.

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

concluding the proof of the theorem. □

References

[BBV16] Andrea Berti, Massimo Bertolini, and Rodolfo Venerucci, *Congruences between modular forms and the Birch and Swinnerton-Dyer conjecture*, Elliptic curves, modular forms and Iwasawa theory, Springer Proc. Math. Stat., vol. 188, Springer, Cham, 2016, pp. 1–31. MR3629647

[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. MR3053566

[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. MR1086888 (92g:11063)

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

[Cas17b] ______, *On the p-adic variation of Heegner points*, J. Inst. Math. Jussieu, to appear (2017).

[Cas17c] ______, *p-adic heights of Heegner points and Beilinson-Flach classes*, J. Lond. Math. Soc. (2) **96** (2017), no. 1, 156–180. MR3687944

[CÇSS17] Francesc Castella, Mirela Çiperiani, Christopher Skinner, and Florian Sprung, *On two-variable main conjectures for modular forms at non-ordinary primes*, preprint (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. MR3298547

[CW17] Francesc Castella and Xin Wan, *Perrin-Riou's main conjecture for elliptic curves at supersingular primes*, preprint (2017).

[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. MR1754686

[GZ86] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR833192 (87j:11057)

[HB15] Ernest Hunter Brooks, *Shimura curves and special values of p-adic L-functions*, Int. Math. Res. Not. IMRN (2015), no. 12, 4177–4241. MR3356751

[JSW17] Dimitar Jetchev, Christopher Skinner, and Xin Wan, *The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one*, Camb. J. Math. **5** (2017), no. 3, 369–434. MR3684675

[KLZ17] Guido Kings, David Loeffler, and Sarah Zerbes, *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. MR482230

[Och06] Tadashi Ochiai, *On the two-variable Iwasawa main conjecture*, Compos. Math. **142** (2006), no. 5, 1157–1200. MR2264660 (2007i:11146)

[PW11] Robert Pollack and Tom Weston, *On anticyclotomic μ-invariants of modular forms*, Compos. Math. **147** (2011), no. 5, 1353–1381. MR2834724 (2012k:11174)

[Rib90] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476. MR1047143 (91g:11066)

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368

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

[Ski16] ———, *Multiplicative reduction and the cyclotomic main conjecture for* GL_2, Pacific J. Math. **283** (2016), no. 1, 171–200. MR3513846

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

[SU14] Christopher Skinner and Eric Urban, *The Iwasawa Main Conjectures for GL_2*, Invent. Math. **195** (2014), no. 1, 1–277. MR3148103

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

[TW95] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572. MR1333036 (96d:11072)

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

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

[Wan14c] ———, *Iwasawa main conjecture for supersingular elliptic curves*, preprint (2014).

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR1333035 (96d:11071)

[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. MR3237437

[Zha14] Wei Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2** (2014), no. 2, 191–253. MR3295917

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