The Iwasawa Main Conjecture for elliptic curves at odd supersingular primes

Florian Sprung

Abstract

In this paper, we prove the Iwasawa main conjecture for elliptic curves at an odd supersingular prime $p$. Some consequences are the $p$-parts of the leading term formulas in the Birch and Swinnerton-Dyer conjectures for analytic rank 0 or 1.

1. Introduction

Iwasawa theory gained a place in the study of elliptic curves in the 1970’s in the work of Mazur. Given an elliptic curve $E$ over $\mathbb{Q}$ and a prime $p$, the goal (or main conjecture) of this program is to relate a $p$-adic $L$-function attached to $E$ with a Selmer group, which contains information about the arithmetic of $E$ in subfields of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. Understanding why these objects are closely related is difficult because they are very different in nature: Selmer groups are algebraic, while $p$-adic $L$-functions are analytic. The main conjecture has important consequences for the Birch and Swinnerton-Dyer conjectures for $E$.

When $p$ is of good ordinary reduction (i.e. $p \nmid a_p := p + 1 - \#E(\mathbb{F}_p)$), this program is now largely complete. Mazur and Swinnerton-Dyer introduced the $p$-adic $L$-function in [MSD], while Mazur studied the corresponding Selmer group in [Ma72]. In the complex multiplication (CM) case, Rubin [Ru91] proved the main conjecture by finding a suitable Euler system. Kato proved half the main conjecture in the non-CM case by finding his zeta element Euler system, showing that the $p$-adic $L$-function is included in the characteristic ideal associated to the Selmer group [Ka04]. Finally, Skinner and Urban [SU14] gave a converse to Kato’s theorem via a GU(2,2) Eisenstein series method, settling the main conjecture, for a large class of elliptic curves.

The supersingular case (i.e. when $p|a_p$) has been more challenging. The main obstacle was that the objects are not well-behaved: The $p$-adic $L$-function is not an element of the Iwasawa algebra, and correspondingly the Selmer group is not a torsion Iwasawa module. Perrin-Riou [PR90] and Kato [Ka04] made important progress in our understanding of the supersingular case, and formulated main conjectures. For a formulation of the main conjecture in the spirit of the ordinary case, Pollack (when $a_p = 0$ [Po03]) found a pair of $p$-adic $L$-functions $L^\flat$ and $L^\sharp$ inside the Iwasawa algebra (for the general $p|a_p$ case, see [Sp12]). Kobayashi (again when $a_p = 0$ [Ko03]) found two corresponding submodules $\text{Sel}^\flat(E/\mathbb{Q}_\infty)$ and $\text{Sel}^\sharp(E/\mathbb{Q}_\infty)$ of the classical Selmer group, and formulated a pair of main conjectures in terms of these objects (for $p|a_p$, see [Sp12]). Pollack and Rubin [P+R04] settled the case of complex multiplication by adapting Rubin’s Euler system.

2010 Mathematics Subject Classification Primary: 11G40, 11F67. Secondary: 11R23, 11G05

Keywords: Iwasawa Theory, elliptic curve, Birch and Swinnerton-Dyer

This material is based upon work supported by the National Science Foundation under agreement No. DMS-1128155. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.
Relying on Kato’s Euler system, half of the main conjecture was proved \cite{Ko03,Sp12}, i.e. $L^{3/b}$ is each included in the characteristic ideal coming from $\text{Sel}^{3/b}(E/\Q_{\infty})$. In the case $a_p = 0$, Wan \cite{Wa14} settled the main conjecture by giving a converse to this theorem via a $\text{GU}(3,1)$ Eisenstein series method.

The purpose of this paper is to prove the main conjecture in the general supersingular case:

**Theorem 1.1.** Let $E/\Q$ be an elliptic curve and $p > 2$ a prime of supersingular reduction. Assume that $E$ has square-free conductor. Then $L^{3/b}$ are each characteristic power series of the Iwasawa module $\text{Hom}(\text{Sel}^{3/b}(E/\Q_{\infty}), \Q_p/\Z_p)$.

Our corollaries concern the leading term formula in the Birch and Swinnerton-Dyer conjecture.

**Corollary 1.2.** Assume that $L(E, 1) \neq 0$. Then under the assumptions of the theorem, we have

$$\frac{|L(E, 1)|}{\Omega} = \# \text{Sel}(E/\Q) \prod_i c_i,$$

Here, $\text{Sel}(E/\Q)$ is the Tate–Shafarevich group of $E/\Q$, $c_i$ are the Tamagawa numbers, and $\Omega$ is the Néron period. Combined with the corresponding result in the ordinary case \cite[Theorem 3.35]{SU14}, this gives the leading term formula up to powers of 2 and bad primes.

**Corollary 1.3.** Suppose that $\text{ord}_{s=1} L(E, s) = 1$. Then under the assumption of the theorem,

$$\frac{|L'(E, 1)|}{\text{Reg}(E/\Q)\Omega} = \frac{\# \text{Sel}(E/\Q) \prod_i c_i}{\# E(\Q)_{\text{tor}}^2}.$$

Here, $\text{Reg}(E/\Q)$ denotes the regulator of $E$, and $E(\Q)_{\text{tor}}$ is the torsion part of $E(\Q)$. This corollary follows from our theorem combined with forthcoming work of Jetchev, Skinner, and Wan \cite{JSW}, or with the discussion of \cite[Corollary 1.3]{Ko12}.

Note that the Hasse–Weil bound $|a_p| \leq 2\sqrt{p}$ (see e.g. \cite[Chapter 5]{Silv}) forces $p = 2$ or $p = 3$ when $p|a_p \neq 0$, so that in this case $p = 3$, since $p$ is odd. This still covers infinitely many elliptic curves, and we have worked out our methods so that they should generalize to general modular forms of weight two, at least when $\text{ord}_p(a_p) \geq \frac{1}{2p}$: Put differently, the assumption $p = 3$ is not used. About 11% of elliptic curves with good reduction at 3 have $a_3 = \pm 3$.

The global strategy of the proof is to establish an equivalence\footnote{The use of ‘equivalence’ and ‘equivalent’ in the introduction is slightly inaccurate. The equivalence is only given up to powers of $p$ and exceptional primes (Definition \ref{def:equivalence}), but this defect is fixable for our purposes.} of three sets of main conjectures over an auxiliary imaginary quadratic field $K$. The first set (four $\frac{3}{b}$-main conjectures) implies the $\frac{3}{b}$ main conjectures over $\Q$ which we want to prove. We show that these $\frac{3}{b}$-main conjectures are equivalent to a second set of main conjectures formulated in terms of new integral Euler systems $\Delta_3$ and $\Delta_3$, which we construct from the Euler systems $\Delta_3$ and $\Delta_3$ of Kings–Loeffler–Zerbes. We show that this second set is itself equivalent to a third set, consisting of just one Greenberg-type main conjecture. The Greenberg-type main conjecture is amenable to the $\text{GU}(3,1)$-Eisenstein series method of Wan, who has proved one inclusion \cite{Wa14}. We can then carry this inclusion over to the other two sets of main conjectures over $K$, which gives us a result towards half of the $\frac{3}{b}$-main conjecture over $\Q$. Combining this with the known inclusion \cite[Theorem 7.16]{Sp12} completes the proof.
The above situation has an analogue in classical Iwasawa theory. The \( l^*/b\)-\( l^*/b\) main conjectures are analogues of the classical main conjecture with the Kubota–Leopoldt \( p\)-adic \( L\)-function, while the main conjecture in terms of \( \Delta^\sharp \) and \( \Delta^\flat \) is an analogue to the formulation of the classical main conjecture in terms of cyclotomic units. The Greenberg-type main conjecture is (more than just) an analogue to Greenberg’s formulation of the classical main conjecture found in [Gr95].

This strategy generalizes that of Wan for the case \( a_p = 0 \). Initially, a generalization to the full supersingular case was assumed to be not hard, and it was hoped that some of the important arguments would be as similar to the ordinary case as for the case \( a_p = 0 \) (e.g. manifested in the fact that the \( l^*/b\)-main conjectures can be proved separately). However, many of the arguments break down when \( a_p \neq 0 \), and the \( l^*/b\) main conjectures need to be handled together. Another difficulty was that much of the background theory needed for [Wa14] assumed \( a_p = 0 \). We overcome this difficulty by generalizing the appropriate theories to general supersingular primes.

More precisely, we choose a quadratic imaginary field in which \( (p) = pq \) splits. The \( l^*/b\)-\( l^*/b\) main conjectures are generalizations of the \( \pm \)-and-\( \pm \) main conjectures of B.D. Kim (who assumed \( a_p = 0 \)). The essential ingredient in their formulation is a pair of \( l^*/b\)-Coleman maps which give rise to a four-tuple of appropriate modified \( l^*/b\)-\( l^*/b\) Selmer groups, whose Pontrjagin duals \( X^* \) (with each \( * \in \{l^*, b\} \)) are torsion as \( \Lambda_K = \mathbb{Z}_p[[X,Y]]\)-modules. The main conjecture relates these \( X^* \) to Lei’s four \( l^*/b\)-\( l^*/b\) \( p\)-adic \( L\)-functions, which are elements of \( \mathbb{E} \) of \( \Lambda_K \).

Lei’s four \( p\)-adic \( L\)-functions appear in a matrix in the left part of the three-part diagram below which features the analytic objects of the three equivalent main conjectures, below which are the formal statement of some of the main conjectures.

![Diagram]

The Euler systems \( \Delta_\alpha \) and \( \Delta_\beta \) constructed in [KLZ] live in a ring with bad growth properties in the variable \( X \) corresponding to \( p \). We fix this deficit by factoring out an explicit \( 2 \times 2 \)-matrix \( \text{Log}(X) \) responsible for the bad growth properties, and obtain an integral version \( (\Delta^\sharp, \Delta^\flat) \). The \( l^*/b\)-Coleman maps \( \text{Col}^{l^*/b} \) send (the local image at \( q \) of) \( \Delta^\sharp \) and \( \Delta^\flat \) to Lei’s four \( p\)-adic \( L\)-functions, up to some controllable constant. Similarly, we construct \( l^*/b\)-Wan maps \( \text{Wan}^{l^*/b} \) which map each of (the local images at \( p \) of) \( \Delta^\sharp \) and \( \Delta^\flat \) to a \( p\)-adic \( L\)-function \( L^{\psi 0}_p \), up to some controllable elements of \( \Lambda_K \).

We prove this via a higher-dimensional version of the Weierstrass preparation theorem. This may be a cute lemma (Lemma 2.7) for the interested reader.
The character $\Psi$ restricts to a map $LOG^+$ constructed by Wan \cite{Wa14} in the $a_p = 0$ case. Our construction of the Wan maps are backwards from Wan’s, starting with this description of $Ker \text{Col}^{\pm}$ rather than having it as a consequence.

\text{Notation introduced in section 2.2}

$K (\text{and } p, q)$ a quadratic imaginary field of class number coprime to $p$ in which $p$ splits as $pq$

$K_\infty$ the $\mathbb{Z}_p$-extension of $K$

$\Omega_E^+$ and $\Omega_E^-$ the real and imaginary periods of $E$ (see e.g. \cite{SZ14}, Section 9.2)\n
$\Lambda_K$ $\mathbb{Z}_p[\text{Gal}(K_\infty/K)] \cong \mathbb{Z}_p[[X,Y]]$. We identify $1+X$ with a generator of the Galois group of the $p$-ray class field $\text{Gal}(K(p^\infty)/K)$ (and do the same for $1+Y$ and $\text{Gal}(K(q^\infty)/K)$).

$k, O_k$ an unramified extension of $\mathbb{Q}_p$, and its ring of integers

$k^m$ the degree $p^m$ unramified extension of $\mathbb{Q}_p$

$k_n, m_n$ the $\mathbb{Z}/p^m\mathbb{Z}$-subextension of $k(\zeta_{p^{n+1}})$, the maximal ideal in its integer ring.

$k_n,m, m_{n,m}$ the objects above with $k = k^m$.

$\Lambda_{n,m}$ $\mathbb{Z}_p[\text{Gal}(k_{n,m}/\mathbb{Q}_p)]$

$\Lambda$ $\mathbb{Z}_p[[X]] \cong \mathbb{Z}_p[[\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$

\text{Notation introduced in section 2.3}

$U_p$ the group $\text{Gal}(K_{\infty,p}/K_{\text{cyc},p}) \cong \mathbb{Z}_p$; $K_{\text{cyc}}$ is the cyclotomic $\mathbb{Z}_p$-extension of $K$

$U$ the unramified variable, i.e. $1+U$ is identified with a topological generator of $U_p$

$\Lambda_K^+$ the Pontryagin dual of $\Lambda_K$

$\Lambda_K$ $\mathbb{Z}_K^*$ twisted by $\Psi$

$\Lambda_K^*(\Psi)$ $\mathbb{Z}_K^*$ twisted by $\Psi$
Notation introduced in section 2.4

| $\gamma_1, \gamma_2, \cdots, \gamma_p^t$ | Representatives of $\text{Gal}(K_\infty/K)/D_p$, where $D_p$ is the decomposition group of $p$ in $\text{Gal}(K_\infty/K)$. |
| $\pi_\alpha$ and $\pi_\beta$ | The projection maps from $\mathbb{D}_{\text{cris}}(V_f)$ to its $\alpha$-(resp.$\beta$-) eigenspace for the Frobenius action with respect to the basis given by the Néron differential $\omega_E$. |
| $\pi_{\mathcal{F}_0^+}$ | Projection onto $\mathcal{F}_0^+$. ($\mathcal{F}_0^\pm$ are defined in Section 2.4.) $\mathfrak{g}$ is the Hida algebra of CM forms of $\text{Gal}(K_\infty/K)$ with coefficient ring $\mathbb{Z}_p[[T]]$, where $1+T$ is identified with a topological generator of $\text{Gal}(K_\infty/K_{\text{cyc}})$. |
| $\Gamma_{n,\mathfrak{g}}$ | the Galois group of the totally ramified $\mathbb{Z}/p^n\mathbb{Z}$-extension of $K_{\mathfrak{g}}$. |

### 2. Main Conjectures

Iwasawa main conjectures relate analytic objects to algebraic objects. The goal of this section is to state four such main conjectures. The first one (subsection 2.1) is the main conjecture concerning the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, which we want to prove. The other three main conjectures concern $\mathbb{Z}_p$-extensions of imaginary quadratic fields. They are the $\mathbb{Z}/p\mathbb{Z}$-main conjecture (subsection 2.2), the Greenberg-type main conjecture (subsection 2.3), and the main conjecture involving $\mathbb{Z}/p\mathbb{Z}$-Beilinson-Flach elements (subsection 2.4). In section 3, we will prove that the $\mathbb{Z}/p\mathbb{Z}$-main conjecture and the Greenberg-type main conjecture are equivalent to the $\mathbb{Z}/p\mathbb{Z}$-Beilinson-Flach element main conjecture. Since one inclusion of the Greenberg-type main conjecture is known, this then yields the $\mathbb{Z}/p\mathbb{Z}$-main conjecture, from which we can deduce the main theorem.

We first recall in subsection 2.1 the statement of the main conjecture from $\text{Sp12}$. In subsection 2.2 we recall the analytic theory of Lei and Loeffler, and the algebraic theory due to Kim in the case $a_p = 0$, before developing it further to include the case $a_p \neq 0$. Subsection 2.3 is a short exposition on the Greenberg-type main conjecture, and one inclusion of it, Wan’s theorem. In subsection 2.4 we construct $\mathbb{Z}/p\mathbb{Z}$-Beilinson-Flach elements. These are modified versions of the Beilinson-Flach Euler system due to Kings, Loeffler, and Zerbes $\text{KLZ}$. While the appropriate modification in the case $a_p = 0$ is due to Wan, a new idea is needed for the case $a_p \neq 0$. Once they are defined, we are in good shape to formulate the $\mathbb{Z}/p\mathbb{Z}$ Beilinson-Flach element main conjecture.

### 2.1 Statement of the Cyclotomic $\mathbb{Z}/p\mathbb{Z}$ Main Conjecture

We now recall the main conjecture of $\text{Sp12}$ (cf. $\text{Ko03}$ for the case $a_p = 0$).

**The analytic side.** Let $\chi$ be a character of $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ into $\mu_{p\infty}$ sending $\gamma$ to $\zeta_{p^n}$, and let $\tau(\chi)$ be the Gauss sum $\sum_{a \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times} \chi(a)\zeta_{p^{n+1}}^a$.

**Theorem 2.1.** (Amice and Vélu, Višik) There are $p$-adic power series $L_\alpha(X)$ and $L_\beta(X)$ converging on the open unit disk so that for $\xi \in \{\alpha, \beta\}$,

$$L_\xi(\zeta_{p^n} - 1) = \frac{p^{n+1}}{\xi^{n+1}} \frac{L(E, \chi^{-1}, 1)}{\Omega_E} \text{ if } 0 \neq \zeta_{p^n} - 1, \text{ and } L_\xi(0) = \left(1 - \frac{1}{\xi}\right)^2 \frac{L(E, 1)}{\Omega_E}.$$

These power series are determined uniquely under the condition that they are $O(\log_p(1+X)^{1/2})$, cf. $\text{Po03}$, p. 528. (For the definition of growth, see Definition 2.29) We let

$$C_n(X) := \left(-\Phi_{p^n}(1+X)\right)^{1/2},$$
and put

\[ \log(X) := \lim_{n \to \infty} C_1(X)C_2(X) \cdots C_n(X) \left( \frac{a_p 1}{-p 0} \right)^{(n+2)} \left( \frac{1}{1} \right). \]

**Theorem 2.2.** ([Po03] when \( a_p = 0 \), [Sp15] for general \( p | a_p \)) There is a vector of \( p \)-adic \( L \)-functions \((L^\sharp(X), L^\flat(X)) \in \mathbb{Z}_p[[X]]^2\) so that \((L_\alpha(X), L_\beta(X)) := (L^\sharp(X), L^\flat(X))\log(X).\) Further, we have \((L^\sharp(X), L^\flat(X)) \neq (0, 0).\)

Alternatively, the pair of Iwasawa functions is the image of Kato’s zeta element under a pair of Coleman maps, i.e. \((L^\sharp(X), L^\flat(X)) = (\text{Col}_p^\sharp(\mathbf{z}), \text{Col}_p^\flat(\mathbf{z}))\), where \( \mathbf{z} = (z_1^+)_n \in H^1_1(T) := \lim H^1(Q_{p,n}, T) \) is Kato’s zeta element [Ka04 Theorem 12.5]. The Coleman maps \( \text{Col}_p^\sharp \) and \( \text{Col}_p^\flat \) are maps from \( H^1_1(T) \) to \( \mathbb{Z}_p[[X]] \) constructed in [Sp12 Section 5] and will be defined more generally in subsection 2.2. with respect to any if the primes \( p \) or \( q \) above \( p \).

**The algebraic side.** The algebraic object is a modified Selmer group. Let \( * \in \{\sharp, \flat\} \). We put

\[ \text{Sel}^*(E/\mathbb{Q}_\infty) := \ker \left( \text{Sel}(E/\mathbb{Q}_\infty) \to \frac{E(Q_{p,\infty}) \otimes Q_p/\mathbb{Z}_p}{E^*} \right), \]

where \( E^* \) is the exact annihilator of \( \ker \text{Col}_p^* \) under the local Tate pairing

\[ \lim_n H^1(Q_{p,n}, T) \times \lim_n H^1(Q_{p,n}, V/T) \to Q_p/\mathbb{Z}_p. \]

We let \( \mathcal{A}^*(E/\mathbb{Q}_\infty) := \text{Hom}(\text{Sel}^*(E/\mathbb{Q}_\infty), Q_p/\mathbb{Z}_p) \), i.e. the Pontryagin dual of \( \text{Sel}^*(E/\mathbb{Q}_\infty) \).

**The main conjecture.** Putting these together, the Iwasawa main conjecture then states:

**Conjecture 2.3.** ([Ko03], [Sp12 Main Conjecture 7.21]) Choose \( * \in \{\sharp, \flat\} \) so that \( L^*(X) \neq 0 \). Then

\[ \text{Char}(\mathcal{A}^*(E/\mathbb{Q}_\infty)) = (L^*(X)). \]

This is the conjecture we want to prove. Half of this conjecture follows from work of Kato:

**Theorem 2.4.** ([Sp12 Theorem 7.16]) Choose \( * \in \{\sharp, \flat\} \) so that \( L^*(X) \neq 0 \). Then for some integer \( n \), we have

\[ \text{Char}(\mathcal{A}^*(E/\mathbb{Q}_\infty)) \supseteq (p^n L^*(X)). \]

If the \( p \)-adic representation \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2打算, T \) on the automorphism group of the Tate-module is surjective, we may take \( n = 0 \).

### 2.2 The \{\sharp/\flat\} main conjectures for imaginary quadratic fields

In this subsection, we recall the analytic theory of Antonio Lei (which generalizes that of Haran/Loeffler ([Ha87] Theorem 2] and [Lo12 Corollary 2]) for the case \( a_p = 0 \)), and then generalize the algebraic theory of B.D. Kim (who also worked with the assumption \( a_p = 0 \)). We then put the two sides together via a main conjecture.

**The analytic side.** Let \( \xi, \eta \in \{\alpha, \beta\} \), and denote by \( L_{\xi,\eta}(X, Y) \) the \( p \)-adic \( L \)-functions of Haran/Loeffler interpolating the following special values at a character \( \chi \) of \( \text{Gal}(K_\infty/K) \), where the conductor \( f_\chi \) is of the form \( p^n q^{n'} \) for \( n, n' \geq 1 \):

\[ \left( \frac{1}{\xi} \right)^{\text{ord}_p f_\chi} \left( \frac{1}{\eta} \right)^{\text{ord}_q f_\chi} \frac{L(E, \chi, 1)}{\tau(\chi)|f_\chi| \Omega_E \Omega_E^+}. \]
Theorem 2.5 Lei, [Le14]. There exist \( L^\#_\mu, L^\#_p, L^\#_q \in \Lambda_K \otimes \mathbb{Q} \) so that
\[
\begin{pmatrix}
L_{\alpha,\alpha} & L_{\beta,\alpha} \\
L_{\alpha,\beta} & L_{\beta,\beta}
\end{pmatrix} = \text{Log}(Y)^T \begin{pmatrix} L^\#_\mu \ L^\#_p \\ L^\#_q \end{pmatrix} \text{Log}(X).
\]

Proposition 2.6. The matrix \( \begin{pmatrix} L^\#_\mu & L^\#_p \\ L^\#_q & L^\#_q \end{pmatrix} \) is not zero.

Proof. Rohrlich [Ro84 page 1], combined with the above interpolation. \( \square \)

Lemma 2.7 (multivariable p-adic Weierstrass preparation theorem). Let \( O \) be the ring of integers in a p-adic field, and let \( f \in O[[X_1, \cdots, X_n]] \). Then for integers \( \mu \geq 0, \lambda_1 \geq 0, \cdots, \lambda_n \geq 0 \) we have
\[
f = p^\mu \prod_{i=1}^{n-1} (X_i^{\lambda_i} + a_{\lambda_{i-1},i}X_i^{\lambda_{i-1}} + \cdots + a_{1,i}X_i + a_{0,i})U
\]
for a unit \( U \in O[[X_1, \cdots, X_n]]^\times \) and \( a_{l,i} \in (p, X_1, \cdots, X_{i-1}) \).

Proof. We need to prove that such \( f \) can be written as \( f = \prod_{i=0}^{n-1} f_i \), with \( f_0 \in m = (\text{maximal ideal in } O) \), and \( f_i \in m_i \setminus m_{i-1} \) for \( i \geq 1 \), where \( m_i = (\text{maximal ideal in } O[[X_1, \cdots, X_i]]) \). But this follows from induction on the one-variable p-adic Weierstrass preparation theorem [Lang Theorem 7.3], or [Ye03 Corollary 3.2]. \( \square \)

Proposition 2.8. The functions \( L^\#_\mu, L^\#_p, L^\#_q, L^\#_q \) are in \( \Lambda_K \).

Proof. This follows from interpolation at \( X = \zeta_p^n - 1 \) and \( Y = \zeta_p^m - 1 \) for large \( n, m \), in which the \( \mu \)-invariant and the \( \lambda_1 \) and \( \lambda_2 \)-invariant dominate. The positivity of the \( \mu \)-invariant then follows from [Ma73 page 375], which guarantees integrality of the interpolating values. \( \square \)

Choice 2.9. From [Sp12 Proposition 6.14], we see that for a choice \( \bullet \in \{\# \} \), the one-variable p-adic L-function \( L^\bullet \) is non-zero. Then we pick \( K \) so that the \( \bullet \)-adic L-function \( L^\bullet_K \) of the elliptic curve \( E^{(K)} \) (i.e. the quadratic twist by the character corresponding to \( K \)) is also not zero.

We point out that this is possible in view of a positive proportion of elliptic curves having rank 0 [BS15], combined with a positive proportion satisfying the Birch and Swinnerton-Dyer conjecture [BSZ], and [Sp12 Table before Proposition 6.14].

The algebraic side.

Lemma 2.10. We can choose a system of points \( c_{(n,m)} \in \mathcal{E}(m_{n,m}) \) satisfying
\[
\text{tr}_{kn,m+1/kn,m} c_{(n,m+1)} = c_{(n,m)}, \quad \text{and} \quad \text{tr}_{kn,m/kn-1,m} c_{(n,m)} = a_p c_{(n-1,m)} - c_{(n-2,m)}.
\]

This lemma generalizes [Wa14 Lemma 2.2] and the constructions in [Ki07 Proposition 3.12], both of which treat the \( a_p = 0 \) case. Its proof needs the following definitions.

Given \( u \in O_k^\times \), put \( f_u(X) := (u + X)^p - u^p \). Also, we let
\[
(x_k, x_{k-1}) := (1, 0) A_k \times \frac{1}{p^k} \text{ for } k \geq 0,
\]
where \( A = (\begin{smallmatrix} a_p & p \\ -1 & 0 \end{smallmatrix}) \) as in [Sp12 Definition 2.1]. We let \( \varphi \) be the Frobenius on \( k \) and let
\[
f_u^{(k)} := f_u^{(k)}(X) := f_u^{\varphi^{k-1}} \circ f_u^{\varphi^{k-2}} \circ \cdots \circ f_u.
\]
The logarithm giving rise to our formal group via Honda theory is the power series

$$\log f_\omega(X) := \sum_{k \geq 0} x_k f_\omega^{(k)}(X).$$

Now define a sequence $b_i$ via

$$b_1 = 1, b_2 = a_p, \text{ and } b_{i+2} := a_p b_{i+1} - b_i.$$  

This allows us to define the following.

**Definition 2.11.** We put $\lambda_{n,u} := \sum_{i \geq 1} b_i u^{-(n+i+1)} p^{\frac{i}{2}}$.

As in [Ki07 page 54], these elements give rise to points $c_{n,u} \in \hat{E}(\mathfrak{m}_k(\zeta_{p^n}))$ so that

$$\log_{\hat{E}}(c_{n,u}) = \lambda_{n,u} + \log f_\omega^{-n} (u^{\phi^n} \cdot (\zeta_{p^n} - 1)) = \lambda_{n,u} + \sum_{k \geq 0} x_k \pi_{n-k,u}$$

for trace-compatible uniformizers $\pi_{n-k,u} = \pi_{n-k,u} \in m_k(\zeta_{p^n})$, where $\pi_{n-k} = (\zeta_{p^n} - 1)$.

**Proof of Lemma 2.10.** To make the first trace relation work, choose trace-compatible $d := \{d_m\}_m \in \prod_{m} \mathcal{O}_m$ as in [Wa14 Lemma 2.2]. The calculations in the proof of [Wa14 Lemma 2.2] with the $d_m$ expressed as sums of roots of unity then work, once the coefficients of $\log_{\hat{E}}$ are appropriately modified. More precisely, we put

$$\log_{\hat{E}}(c_{n,d_m}) = \sum_i b_i d_m^{-(n+i+1)} + \sum_{k < n} x_k (\zeta_{p^n} - 1) d_m^{x_k^{-n}}.$$  

For the second trace relation, we refer to the calculations in [Ki07 page 54]. To make them work for the case $a_p \neq 0$, note that

$$\text{tr}_{k(\zeta_{p^n})/k(\zeta_{p^n-1})} \log_{\hat{E}}(c_{n,u}) = \text{tr}_{k(\zeta_{p^n})/k(\zeta_{p^n-1})} (\lambda_{n,u} + \pi_{n,u} + \sum_{k \geq 1} x_k \pi_{n-k,u}) = p \lambda_{n,u} - u^{\phi^n} p + \sum_{k \geq 1} x_k \pi_{n-k,u} = a_p (\lambda_{n-1,u} + \sum_{k \geq 1} x_k \pi_{n-k,u}) - \lambda_{n-2,u} + \sum_{k \geq 2} x_k \pi_{n-k,u} = a_p \log_{\hat{E}}(c_{n-1,u}) - \log_{\hat{E}}(c_{n-2,u}).$$

**Definition 2.12.** We define a pairing $P_{(n,m),x} : H^1(k_{n,m}, T) \to \Lambda_{n,m}$ by

$$z \mapsto \sum_{\sigma \in \text{Gal}(k_{n,m}/Q_p)} (x^\sigma, z)_{n,m} \sigma$$

for $x \in F_{ss}(m_{n,m})$, where $(\cdot, \cdot)_{n,m} : F_{ss}(m_{n,m}) \times H^1(k_{n,m}, T) \to H^2(k_{n,m}, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p$ is the pairing coming from the cup product.

**Definition 2.13.** Put $\mathcal{H}_n(X) := -C_1(X)C_2(X) \cdots C_{n-1}(X) \begin{pmatrix} 1 & \Phi_p & 0 \\ 0 & 1 & (1+X) \end{pmatrix}$ and define the endomorphism $h_{n,m}$

$$\Lambda_{n,m} \oplus \Lambda_{n,m} \xrightarrow{h_{n,m}} \Lambda_{n,m} \oplus \Lambda_{n,m} \mathcal{H}_n \subset \Lambda_{n,m} \oplus \Lambda_{n,m}$$  

For BD Kim’s notation, the analogue of $\lambda_{n,u}$ is denoted $\lambda_n$ and that of $c_{n,u}$ is denoted $b_n$. 

---

8
Remark 2.14. The minus sign ensures that our conventions agree with the original ones of Kobayashi, see e.g. [Sp12, Definition 3.8].

Proposition 2.15. There exists a unique map \( \text{Col}_{n,m} \) so that the following commutes:

\[
\begin{array}{cccccc}
H^1(k_{n,m}, T) & \cong & \langle P_{(n,m), e_{n,m} P_{(n,m), e_{n-1,m}} } \rangle & \rightarrow & \Lambda_{n,m} \oplus \Lambda_{n,m} & \leftarrow & h_{n,m} \rightarrow \Lambda_{n,m} \oplus \Lambda_{n,m} \\
& & & & \text{ker } h_{n,m} & \text{ker } h_{n,m} & \\
\end{array}
\]

Proof. [Sp12, Proposition 5.3] proves this in the case in which \( k^m = \mathbb{Q}_p \), relying on the arguments from [Sp12, Section 3]. These arguments work for our purposes since the pairing \( P_{(n,m), x} \) is available in the \( k^m \) case as well.

Lemma 2.16. The Coleman maps are compatible in the unramified direction, i.e. the following diagram commutes:

\[
\begin{array}{cccccc}
H^1(k_{n,m+1}, T) & \xrightarrow{\text{Col}_{n,m+1}} & \Lambda_{n,m+1} \oplus \Lambda_{n,m+1} & \leftarrow & \text{ker } h_{n,m+1} & \rightarrow & \Lambda_{n,m} \oplus \Lambda_{n,m} \\
& & & & \text{ker } h_{n,m} & \text{ker } h_{n,m} & \\
H^1(k_{n,m}, T) & \xrightarrow{\text{Col}_{n,m}} & \Lambda_{n,m} \oplus \Lambda_{n,m} & \leftarrow & \text{ker } h_{n,m} & \rightarrow & \Lambda_{n,m} \oplus \Lambda_{n,m} \\
\end{array}
\]

Proof. This follows from the first trace-compatibility stated in lemma 2.10.

Proposition 2.17. The Coleman maps are compatible in the totally ramified direction, i.e. the following diagram also commutes:

\[
\begin{array}{cccccc}
H^1(k_{n+1,m}, T) & \xrightarrow{\text{Col}_{n+1,m}} & \Lambda_{n+1,m} \oplus \Lambda_{n+1,m} & \leftarrow & \text{ker } h_{n+1,m} & \rightarrow & \Lambda_{n,m} \oplus \Lambda_{n,m} \\
& & & & \text{ker } h_{n,m} & \text{ker } h_{n,m} & \\
H^1(k_{n,m}, T) & \xrightarrow{\text{Col}_{n,m}} & \Lambda_{n,m} \oplus \Lambda_{n,m} & \leftarrow & \text{ker } h_{n,m} & \rightarrow & \Lambda_{n,m} \oplus \Lambda_{n,m} \\
\end{array}
\]

Proof. This is [Sp12, Corollary 5.6] in the case \( k^m = \mathbb{Q}_p \). We note that the arguments for this corollary apply in the \( k^m \) case as well.

Lemma 2.18. We have \( \lim_{m \leftarrow n} \lim_{m \leftarrow n} \Lambda_{n,m} \oplus \Lambda_{n,m} \text{ker } h_{n,m} \cong \Lambda \oplus \Lambda \).

Proof. The arguments in [Sp12, Proposition 5.7] show that \( \lim_{m \leftarrow n} \Lambda_{n,m} \oplus \Lambda_{n,m} \text{ker } h_{n,m} \cong \Lambda \oplus \Lambda \). This is enough since \( \text{Gal}(k_{n,m}/k^m) \cong \text{Gal}(\mathbb{Q}_p,n/\mathbb{Q}_p) \).

Definition 2.19. We define the pair of Coleman maps as

\[
(\text{Col}^\sharp, \text{Col}^\flat) := \lim_{m \leftarrow n} \lim_{m \leftarrow n} \text{Col}_{n,m} : \lim_{m \leftarrow n} \lim_{m \leftarrow n} H^1(k_{n,m}, T) \rightarrow \Lambda \oplus \Lambda.
\]

Definition 2.20. Let \( \star \in \{\sharp, \flat\} \). We denote by \( E^\star \) the exact annihilator of \( \ker \text{Col}_\star \) under the Tate pairing

\[
\lim_{m \leftarrow n} \lim_{m \leftarrow n} H^1(k_{n,m}, T) \times \lim_{m \leftarrow n} \lim_{m \leftarrow n} H^1(k_{n,m}, V/T) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p.
\]
We denote by \( k_{n,m}(p) \) (resp. \( k_{n,m}(q) \)) the local field isomorphic to \( k_{n,m} \) with initial layer \( k_{0,0} \) obtained by completing \( K \) at \( p \) (resp. \( q \)) and climbing up to the appropriate layer of the cyclotomic extension and the unramified tower.

**Definition 2.21.** We now define the four Selmer groups \( \text{Sel}^\sharp(E/K_\infty) \), \( \text{Sel}^\flat(E/K_\infty) \), \( \text{Sel}^\sharp(E/K_\infty) \), and \( \text{Sel}^\flat(E/K_\infty) \). For \( *, \circ \in \{\sharp, \flat\} \), put

\[
\text{Sel}^{\circ}(E/K_\infty) := \ker \left( \text{Sel}(E/K_\infty) \to \lim_{\overset{\longrightarrow}{m}} \lim_{\overset{\longrightarrow}{n}} H^1(k_{n,m}(p), V/T) \oplus \lim_{\overset{\longrightarrow}{m}} \lim_{\overset{\longrightarrow}{n}} H^1(k_{n,m}(q), V/T) \right).
\]

**Definition 2.22.** Given \( *, \circ \in \{\sharp, \flat\} \), put \( \mathcal{X}^{\circ} := \text{Hom}(\text{Sel}^{\circ}(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p) \).

**Proposition 2.23.** Choose \( *, \circ \in \{\sharp, \flat\} \) so that \( L^{\circ}(X, Y) \neq 0 \). Then the Selmer group \( \mathcal{X}^{\circ} \) is torsion as a \( \Lambda \)-module.

**Proof.** The arguments in [Sp12, Theorem 7.14] with the appropriate adjustments work.

Denote by \( t \) the anticyclotomic variable. If we pick \( K \) and \( \bullet \in \{\sharp, \flat\} \) as in our Choice 2.9 denote by \( \mathcal{X}_K^\bullet \) the \( \bullet \)-Selmer group dual of the elliptic curve \( E(K) \).

**Proposition 2.24.** We have \( \mathcal{X}^{\bullet \bullet} \otimes \Lambda_K/(t) \cong \mathcal{X}^\bullet \oplus \mathcal{X}_K^\bullet \).

**Proof.** Tensoring with \( \Lambda_K/(t) \) in each step of the construction of \( \mathcal{X}^{\bullet \bullet} \) gives an isomorphism between \( \mathcal{X}^{\bullet \bullet} \otimes \Lambda_K/(t) \) and the \( \bullet \)-Selmer group dual in the cyclotomic variable with base field \( K \). This \( \bullet \)-Selmer group dual is isomorphic to \( \mathcal{X}^\bullet \oplus \mathcal{X}_K^\bullet \), since \( E/K \cong E/Q \oplus E^{(K)}_Q \).

**The main conjecture.**

**Conjecture 2.25.** For \( *, \circ \in \{\sharp, \flat\} \) so that \( L^{\circ}(X, Y) \neq 0 \),

\[
\text{Char}(\mathcal{X}^{\circ}(E/K_\infty)) = (L^{\circ}(X, Y)).
\]

**2.3 A Greenberg-type main conjecture**

**The analytic side.** We let \( L^{\circ,0}_p \in \text{Frac} \Lambda_K \) be the \( p \)-adic \( L \)-function denoted \( L'_{f,K} \) in [Wa14, discussion before Theorem 2.13], where \( f \) is the modular for associated to \( E \). More precisely, define \( F_{d,p} \in \mathbb{Z}_p[[U]] \) as

\[
F_{d,p} = \lim_{\overset{\longrightarrow}{m}} \sum_{\sigma \in U_p/p^m U_p} d_{m}^\sigma \cdot \sigma^2,
\]

where the \( d_m \) are as in the proof of [Wa14, Lemma 2.2]. Let \( \varphi \in S \), where \( S \) is a Zariski dense set of arithmetic points inside

\[
\{ \varphi \in \text{Spec} \Lambda : \xi_\varphi \text{ is the avatar of a Hecke character of infinity type } \left( \frac{\kappa}{2}, -\frac{\kappa}{2} \right) \text{ with } \kappa \geq 6 \},
\]

and \( \xi_\varphi := \varphi \circ \Psi \). Then \( \varphi(L^{\circ,0}_p \cdot F_{d,p}) \) interpolates the algebraic parts of (certain) values \( L(K, \pi_E, \xi_\varphi, \frac{\kappa}{2}, -\frac{\kappa}{2}) \) coming from twists of the automorphic representation \( \pi_E \) associated to \( E \). We refer to [Wa14, Section 2.3] for the notation and details since they won’t be needed in our paper.

**The algebraic side.** The algebraic object is the following “fine at \( p \) but empty at \( q \)” Selmer group.
Definition 2.26.
\[ \text{Sel}_{p}^0 := \ker \left( H^1(K, T \otimes \Lambda^{*} (\Psi)) \to \prod_{v \mid p} H^1(K_v, T \otimes \Lambda^{*} (\Psi)) \times H^1(K_{p}, T \otimes \Lambda^{*} (\Psi)) \right). \]

We then put \( \mathcal{X}^0 := \text{Hom}(\text{Sel}_{p}^0, \mathbb{Q}_p / \mathbb{Z}_p). \)

The main conjecture. The main conjecture is full equality in the following theorem of Wan [Wa14+, Theorem 1.1] (see also [Wa14, Theorem 2.13]):

Theorem 2.27. Let \( E \) have square-free conductor \( N \) that has at least one prime divisor \( l \mid N \) not split in \( K \), and suppose that \( E[p]|_{G_K} \) is absolutely irreducible. Then as (fractional) ideals of \( \Lambda_K \otimes \mathbb{Q}_p \), we have
\[ \text{Char}(\Lambda^0) \subseteq (\mathcal{L}_p^0). \]

2.4 The \( \sharp/\flat \)-Beilinson-Flach main conjectures

The analytic side.

Definition 2.28. Fix \( 0 < r < 1 \). For \( f(X) \in \mathbb{C}_p[[X]] \) convergent on the open unit disc of \( \mathbb{C}_p \), let
\[ |f(X)|_r := \sup_{|z|_p < r} |f(z)|_p \]
with normalization \( |p|_p = \frac{1}{p} \).

Definition 2.29. Let \( f(X), g(X) \in \mathbb{C}_p[[X]] \) converge on the open unit disc of \( \mathbb{C}_p \). Then we say that \( f(X) \) is \( O(g(X)) \) if
\[ |f(X)|_r \text{ is } O(|g(X)|_r) \text{ as } r \to 1^- \]
If in addition, \( g(X) \) is \( O(f(X)) \), then we say that \( f(X) \sim g(X) \).

Definition 2.30. We denote by \( D_{K}^{x,y} \) the distributions of order \( x, y \) for non-negative real numbers \( x, y \) in the variables \( X \) and \( Y \), i.e. power series convergent on the open unit disk which are \( O(\log^x) \) in the variable \( X \) and \( O(\log^y) \) in the variable \( Y \).

Convention 2.31. Given a column vector of functions \( \left( \begin{array}{c} f_1 \\ f_2 \end{array} \right) \) an a row vector of elements \( (x_1, x_2) \), we denote by \( \left( \begin{array}{c} f_1 \\ f_2 \end{array} \right) \circ (x_1, x_2) \) the matrix \( \left( \begin{array}{cc} f_1(x_1) & f_1(x_2) \\ f_2(x_1) & f_2(x_2) \end{array} \right) \).

We now construct integral Euler systems \( \Delta_{\sharp}, \Delta_{\flat} \) out of the Beilinson–Flach Euler systems \( \Delta_{\alpha}, \Delta_{\beta} \) due to Kings, Loeffler, and Zerbes, constructed from the \( p \)-stabilizations \( f_\alpha \) and \( f_\beta \) of \( f \) (see [LLZ14, 6.4.4] and [LZ16, Thm A]).

Theorem 2.32. [LZ16, Loeffler, Zerbes, Thm A]

There exist Euler systems \( \Delta_{\alpha}, \Delta_{\beta} \in H^1(K, T \otimes \Lambda_K(\Psi))^2 \otimes D_{K}^{\frac{1}{2},0} \) and maps
\[ \mathcal{L}_{\alpha}, \mathcal{L}_{\beta} : H^1(K_q, T \otimes \Lambda_K(\Psi)) \otimes D_{K}^{\frac{1}{2},0} \to D_{K}^{\frac{1}{2},0} \]
so that
\[ \left( \begin{array}{c} \mathcal{L}_{\alpha} \\ \mathcal{L}_{\beta} \end{array} \right) \circ (\Delta_{\alpha}, \Delta_{\beta}) = \left( \begin{array}{cc} L_{\alpha \alpha} & L_{\alpha \beta} \\ L_{\beta \alpha} & L_{\beta \beta} \end{array} \right). \]
Proposition 2.33. There exist integral Euler systems $\Delta_\alpha, \Delta_\beta \in H^1(K, T \otimes \Lambda_{K}(\Psi))^2$ so that

$$h \cdot (\Delta_\alpha, \Delta_\beta) = (\Delta_\alpha, \Delta_\beta) \Log(X)$$

for some element $h \in \mathbf{Z}_p[[X, U]]$.

Lemma 2.34. The entries of $\Log(X)$ are $O(\log p(1 + X)^{1/2})$.

Proof. [Sp15] Proposition 4.20 (Growth Lemma). \qed

Definition 2.35. We now choose a $\Lambda_K$-basis $(v_1, v_2)$ of $H^1(K_{q}, T \otimes \Lambda(\Psi))$.

Definition 2.36. Choose $\xi \in \{\alpha, \beta\}$. We choose integral $(v_1, v_2)$-coordinates of the $q$-localized Beilinson–Flach element $(\Delta_\xi)_q = \loc_q(\Delta_\xi)$ by $\delta_{\xi i}$ with $i \in \{1, 2\}$ so that

$$((\Delta_\alpha)_q, (\Delta_\beta)_q) = (v_1, v_2) \left( \begin{array}{cc} \delta_{\alpha 1} & \delta_{\beta 1} \\ \delta_{\alpha 2} & \delta_{\beta 2} \end{array} \right) \frac{1}{f},$$

where

$$\delta_{\xi i} \in D_{K}^{1, 0}$$

and $f \in \mathbf{Z}_p[[T]]$ is nonzero.

Proof of Proposition 2.33. From Theorem 2.5 and Proposition 2.8 we know that

$$\Log(Y)^T \left( \begin{array}{cc} L^{\alpha \alpha} & L^{\beta \alpha} \\ L^{\alpha \beta} & L^{\beta \beta} \end{array} \right) \Log(X) = \left( \begin{array}{cc} L^{\alpha \alpha} & L^{\beta \alpha} \\ L^{\alpha \beta} & L^{\beta \beta} \end{array} \right) \circ (\Delta_\alpha, \Delta_\beta)_q$$

(1)

$$= \left( \begin{array}{cc} L^{\alpha \alpha} & L^{\beta \alpha} \\ L^{\alpha \beta} & L^{\beta \beta} \end{array} \right) \circ (v_1, v_2) \left( \begin{array}{cc} \delta_{\alpha 1} & \delta_{\beta 1} \\ \delta_{\alpha 2} & \delta_{\beta 2} \end{array} \right) \frac{1}{f}$$

(2)

$$= \left( \begin{array}{cc} L^{\alpha \alpha}(v_1) & L^{\beta \alpha}(v_2) \\ L^{\alpha \beta}(v_1) & L^{\beta \beta}(v_2) \end{array} \right) \left( \begin{array}{cc} \delta_{\alpha 1} & \delta_{\beta 1} \\ \delta_{\alpha 2} & \delta_{\beta 2} \end{array} \right) \frac{1}{f}$$

(3)

The strategy of [Wal14] Lemma 7.3 can now be generalized. Thus, there exists an $a \in p\mathbf{Z}_p$ so that

$$\left( \begin{array}{cc} \delta_{\alpha 1} & \delta_{\beta 1} \\ \delta_{\alpha 2} & \delta_{\beta 2} \end{array} \right) \Log(X)^{ad} \bigg|_{y = a} \in \log_p(X) \times M_2(\Frac \mathbf{Z}_p[[X]])$$

by the growth property. Here, $\Log(X)^{ad}$ denotes the adjugate of $\Log(X)$.

We use [LZ14] Proposition 4.9 which shows that

$$\left( \begin{array}{cc} L^{\alpha \alpha}(v_1) & L^{\beta \alpha}(v_2) \\ L^{\alpha \beta}(v_1) & L^{\beta \beta}(v_2) \end{array} \right) \in D_{K}^{0, \frac{1}{2}},$$

so that the determinant is in $\mathbf{Q}_p$. \qed

We now choose $h \in \mathbf{Z}_p[[X, U]]$ so that

$$\left( \begin{array}{cc} \delta_{\alpha 1} & \delta_{\beta 1} \\ \delta_{\alpha 2} & \delta_{\beta 2} \end{array} \right) \Log(X)^{ad} \in \log_p(X) \times M_2(\Lambda_K).$$

Corollary 2.37. The coordinates of the Beilinson–Flach elements are divisible by $\Log(X)$ after correcting by $h$, i.e.

$$h \left( \begin{array}{cc} \delta_{\alpha 1} & \delta_{\beta 1} \\ \delta_{\alpha 2} & \delta_{\beta 2} \end{array} \right) = \left( \begin{array}{cc} \delta_{1 1} & \delta_{1 2} \\ \delta_{2 1} & \delta_{2 2} \end{array} \right) \Log(X)$$

for some $\delta_{\xi i} \in \mathbf{Z}_p[[X, U, T]] \otimes \Frac \mathbf{Z}_p[[T]] \otimes \mathbf{Q}$ for $\xi \in \{\alpha, \beta\}$ and $i \in \{1, 2\}$. 

12
Proof. After multiplying by the adjugate of \( \log(X) \), we know that the entries vanish at \( p \)-power roots of unity.

**Corollary 2.38.** The elements \((\Delta_q, \Delta_p) := h(\Delta_\alpha, \Delta_\beta)\log(X)^{-1}\) are well-defined as elements of \(H^1(\Q_\infty, V_f^* \otimes M(\mathfrak{a})^*) \cong H^1_{iw}(K_\infty, V_f^*)\).

**Proof.** This follows from Proposition 2.8.

**The algebraic side.** The objects here are the \( \hat{\mathfrak{a}}/\mathfrak{b} \) Selmer groups:

**Definition 2.39.** For \( \mathfrak{a} \in \{\hat{\mathfrak{a}}, \mathfrak{b}\} \), put

\[
\text{Sel}^{0} := \ker \left( H^1(K_\infty, V_f^* \otimes \Lambda_K(\Psi) \otimes (\Lambda_K)^*) \to \prod_{\mathfrak{p} \mid \mathfrak{p}} H^1(I_v, V_f^* \otimes \Lambda_K(\Psi) \otimes (\Lambda_K)^*) \times \frac{H^1_p}{E^\infty} \times H^1_q \right),
\]

where \( H^1 := H^1(K_\infty, V_f^* \otimes \Lambda_K(\Psi) \otimes (\Lambda_K)^*) \) and \( H^1_q \) is defined analogously.

We then put

\[
\mathcal{X}^0 := \text{Hom}(\text{Sel}^{0}, \Q_p/\Z_p).
\]

**The main conjecture.** To set up the main conjecture, we need one more definition on the analytic side (i.e. the side in which the Beilinson-Flach elements live): These are the \( \text{“dual } \hat{\mathfrak{a}}/\mathfrak{b} \text{ Selmer groups:} \)

**Definition 2.41.** We choose \( K \) so that we can make a choice \( \bullet \in \{\hat{\mathfrak{a}}, \mathfrak{b}\} \) as in Choice 2.9 and let

\[
\mathcal{X}^{\bullet \mathfrak{a}} := \ker \left( H^1(K, T_f \otimes \Lambda_K(-\Psi)) \to \prod_{\mathfrak{p} \mid \mathfrak{p}} H^1(I_v, T_f \otimes \Lambda_K(-\Psi)) \times \frac{H^1(K_p, T_f \otimes \Lambda_K(-\Psi))}{\ker(\text{Col}^\bullet)} \right).
\]

**Proposition 2.42.** Given \( \bullet \in \{\hat{\mathfrak{a}}, \mathfrak{b}\} \) (and \( K \)) as in Choice 2.9 \( \mathcal{X}^{\bullet \mathfrak{a}} \) is a free rank one \( \Lambda_K \)-module.

**Proof.** Note that we then have \( \text{Col}^\bullet_p \) is non-zero. The freeness follows from the irreducibility of the mod \( p \) representation. First we show that the \( \Lambda_K \)-rank of \( \mathcal{X}^{\bullet \mathfrak{a}} \) is at most one. We know from the construction of Coleman maps that

\[
\text{rk}_{\Lambda_K} \frac{H^1(K_q, T \otimes \Lambda_K(-\Psi))}{H^1_{\bullet}(K_q, T \otimes \Lambda_K(-\Psi))} = 1.
\]

But again from the construction of the Coleman maps, we see that the specialization of

\[
\mathcal{N} := \ker \left( \mathcal{X}^{\bullet \mathfrak{a}} \to \frac{H^1(K_q, T \otimes \Lambda_K(-\Psi))}{H^1_{\bullet}(K_q, T \otimes \Lambda_K(-\Psi))} \right)
\]

to the \( \Q \)-cyclotomic line has rank zero, by equation (3) in [Sp12] Proof of Theorem 7.14. Thus \( \mathcal{N} \) itself must be of rank zero, whence \( \mathcal{X}^{\bullet \mathfrak{a}} \) has rank at most one. To see that the rank is at least one, consider the composed map

\[
\mathcal{X}^{\bullet \mathfrak{a}} \to \frac{H^1(K_q, T \otimes \Lambda_K(-\Psi))}{H^1_{\bullet}(K_q, T \otimes \Lambda_K(-\Psi))} \text{Col}^\bullet \to \Lambda_K
\]

and note that we have chosen \( \bullet \) so that \( \text{Col}^\bullet(\Delta_\bullet) \neq 0 \).

**Proposition 2.43.** Given \( K \) and \( \bullet \in \{\hat{\mathfrak{a}}, \mathfrak{b}\} \) as in Choice 2.9 \( \mathcal{X}^{\bullet 0} \) is a finitely generated torsion \( \Lambda_K \)-module.
Proof. The inclusion $\text{Sel}^{\bullet\bullet} \hookrightarrow \text{Sel}^{\bullet\circ}$ gives rise to a surjection

$$\mathbb{X}^{\bullet\bullet} \twoheadrightarrow \mathbb{X}^{\bullet\circ} \twoheadrightarrow 0.$$ 

To prove that $\mathbb{X}^{\bullet\circ}$ is finitely generated torsion, it thus suffices to prove that $\mathbb{X}^{\bullet\bullet}$ is. This follows from Proposition 2.24 since any free part of $\mathbb{X}^{\bullet\bullet}$ would cause $\mathbb{X}^{\bullet\bullet} \otimes \Lambda_K/(t)$ to be free, where $t$ is the anticyclotomic variable. Note that since $\text{Col}_p^\bullet \neq 0$, we necessarily have that the corresponding one-variable Coleman map is not zero: $\text{Col}^\bullet \neq 0$ at $p$. \hfill \Box

CONJECTURE 2.44. (The $\sharp/\flat$ Beilinson-Flach element main conjecture) Given $\circ \in \{\sharp, \flat\}$, we have that

$$\text{Char}(\mathbb{X}^{\bullet\circ}/\Delta_\circ \Lambda_K) = \text{Char}(\mathbb{X}^{\bullet\circ}).$$

3. Connecting the main conjectures together

3.1 The $\sharp/\flat$-Beilinson-Flach conjectures are equivalent to the Greenberg-type one

The aim of this subsection is to prove an equivalence of these main conjectures up to powers of $p$ and certain primes which we term exceptional. We do this by constructing maps $\text{Wan}^\sharp$ and $\text{Wan}^\flat$, which generalize Wan’s map $LOG^+$. Put

$$\mathcal{H}_n(X) = \left( \begin{array}{c} \omega_n^\sharp \Phi_p^n \omega_n^\sharp -1 \\ \omega_n^\flat \Phi_p^n \omega_n^\flat -1 \end{array} \right).$$

We can describe $\ker(h_{n,m})$, defined in Definition 2.13 explicitly by $\ker(h_{n,m}) = (\Lambda_{n,m} \otimes \Lambda_{n,m})H^\perp_n$, where

$$H^\perp_n = X\left( \begin{array}{c} \omega_n^\flat \\ \Phi_p^n \omega_n^\flat -1 \end{array} \right).$$

(See [Sp12] Lemma 5.8) for the $\Lambda_n$-module case. The same arguments apply to the $\Lambda_{n,m}$-module case as well.

REMARK 3.1. Similarly, the kernel of multiplying by $H^\perp_n$ is $(\Lambda_{n,m} \otimes \Lambda_{n,m})H_n$.

LEMMA 3.2. We have $(c_{n,m}, c_{n-1,m})H^\perp_n = (0,0)$.

Proof. $\Lambda_{n,m}$-bilinearity of the pair of pairings $(P_{n,m,c_{n,m}}, P_{n,m,c_{n-1,m}})$. \hfill \Box

PROPOSITION 3.3. We can choose $(b^\sharp_{n,m}, b^\flat_{n,m}) \in H^1(k_{n,m}, T)^{\oplus 2}$ so that:

(i) \hspace{1cm} $(b^\sharp_{n,m}, b^\flat_{n,m})H_n = (c_{n,m}, c_{n-1,m})$

(ii) \hspace{1cm} $\text{tr}_{k_{n,m}/k_{n-1,m}} b^\flat_{n,m} = b^\flat_{n-1,m}$, and $\text{tr}_{k_{n,m}/k_{n,m-1}} b^\flat_{n,m} = b^\flat_{n,m-1}$.

Proof. The existence of such $(b^\sharp_{n,m}, b^\flat_{n,m})$ satisfying (i) follows from Lemma 3.2 and the remark.

For (ii), the trace compatibility with respect to $m$ follows from that of $(c_{n,m}, c_{n-1,m})$. For that with respect to $n$, note that

$$\text{tr}_{n/n-1} \left( (b^\sharp_{n,m}, b^\flat_{n,m})H_n \right) = \left( \text{tr}_{n/n-1} b^\sharp_{n,m}, \text{tr}_{n/n-1} b^\flat_{n,m} \right) H_{n-1} \left( \begin{array}{c} a_{n} \p \\ -1 \p \end{array} \right),$$

while $\text{tr}_{n/n-1} (c_{n,m}, c_{n-1,m}) = (c_{n-1,m}, c_{n-2,m}) \left( \begin{array}{c} a_{n} \p \\ -1 \p \end{array} \right)$. \hfill \Box
DEFINITION 3.4. We denote by $H^1_\sharp(k_{n,m}, T)$ the rank one $\Lambda_{n,m}$-submodule of $H^1(k_{n,m}, T)$ generated by $b_{n,m}^\sharp$, and define $H^1_\flat(k_{n,m}, T)$ analogously.

PROPOSITION 3.5. We have $H^1_\sharp := \varprojlim_{n,m} H^1_\sharp(k_{n,m}, T) = \ker \text{Col}^\sharp$ and $H^1_\flat := \varprojlim_{n,m} H^1_\flat(k_{n,m}, T) = \ker \text{Col}^\flat$.

Proof. For $(b_{n,m}^\sharp, b_{n,m}^\flat) \in H^1(k_{n,m}, T)$, we have $\text{Col}_{n,m}(b_{n,m}^\sharp, b_{n,m}^\flat) = 0$ in $\frac{\Lambda_{n,m} \oplus \Lambda_{n,m}}{\ker H_{n,m}}$ by construction. Thus, we have $H^1_\sharp \subset \ker \text{Col}^\sharp$ and $H^1_\flat \subset \ker \text{Col}^\flat$. To prove equality, we show that $\frac{\ker \text{Col}^\sharp}{H^1_\sharp} = 0$. By Nakayama’s lemma, it suffices to do this for the Coleman map at level 0: By [Sp12, discussion before Definition 7.2], we have $\text{Col}_{0,m} = (\text{Col}_{0,m}, \text{Col}_{0,m}^\flat) = (-a_0 P_{0,m,c_0} + P_{0,m,c_0} - P_{c_0}, P_{0,m,b_0})$.

But $b_{0,m}^\flat$ annihilate themselves under the cup product, so $\ker \text{Col}_{0,m}^\flat$ is generated by $b_{0,m}^\flat$. The $\flat$ case is proved similarly.

Proof. For $(b_{n,m}^\sharp, b_{n,m}^\flat) \in H^1(k_{n,m}, T)$, we have $\text{Col}_{n,m}(b_{n,m}^\sharp, b_{n,m}^\flat) = 0$ in $\frac{\Lambda_{n,m} \oplus \Lambda_{n,m}}{\ker H_{n,m}}$ by construction. Thus, we have $H^1_\sharp \subset \ker \text{Col}^\sharp$ and $H^1_\flat \subset \ker \text{Col}^\flat$. To prove equality, we show that $\frac{\ker \text{Col}^\sharp}{H^1_\sharp} = 0$. By Nakayama’s lemma, it suffices to do this for the Coleman map at level 0: By [Sp12, discussion before Definition 7.2], we have $\text{Col}_{0,m} = (\text{Col}_{0,m}, \text{Col}_{0,m}^\flat) = (-a_0 P_{0,m,c_0} + P_{0,m,c_0} - P_{c_0}, P_{0,m,b_0})$.

By Nakayama’s lemma, it suffices to do this for the Coleman map at level 0: By [Sp12, discussion before Definition 7.2], we have $\text{Col}_{0,m} = (\text{Col}_{0,m}, \text{Col}_{0,m}^\flat) = (-a_0 P_{0,m,c_0} + P_{0,m,c_0} - P_{c_0}, P_{0,m,b_0})$.

But $b_{0,m}^\flat$ annihilate themselves under the cup product, so $\ker \text{Col}_{0,m}^\flat$ is generated by $b_{0,m}^\flat$. The $\flat$ case is proved similarly.

DEFINITION 3.6. The maps $\text{Wan}^\sharp$ and $\text{Wan}^\flat$ map elements of $H^1_{\sharp/\flat}(k_{n,m})$ to their coordinates, i.e. we put:

$$\text{Wan}^\sharp : H^1_\sharp = \varprojlim_{n,m} H^1_\sharp(k_{n,m}, T) \to \Lambda, (f_{n,m}^{\sharp/\flat}, b_{n,m}^{\sharp/\flat})_{n,m} \mapsto (f_{n,m}^{\sharp/\flat})_{n,m}$$

and define $\text{Wan}^\flat$ similarly.

PROPOSITION 3.7. Recall we have chosen $\bullet \in \{\sharp, \flat\}$ so that $\Delta_\bullet \neq 0$. For such a choice, we have $\text{Wan}^\bullet(\Delta_\bullet) = L^\sigma \times h \times H$,

where $h$ is the constant chosen just before Corollary 2.3.7 and $H \in \text{Frac } \Lambda_0$.

Proof. In this proof, we let $\sum$ denote $\sum_{\sigma \in \Gamma_{n,m} \times U_m}$, where $U_m = U/p^m U$. Denote by $x_{n,m}^{\sharp/\flat}$ the image of $\Delta_{\sharp/\flat}$ in $H^1_{\sharp/\flat}(k_{n,m}, T)$. Note that we have $\sum \log x_{n,m}^{\sharp/\flat} \sigma \varphi(\sigma) = \left( \sum \log b_{n,m}^{\sharp/\flat} \sigma \varphi(\sigma) \right) \varphi(f_{n,m}^{\sharp/\flat})$.

We also put $g_n(\varphi) := \sum \log E(c_{n,m})^\sigma \varphi(\sigma) = \tau(\varphi|_{\Gamma_n}) \varphi(u) \times \sum_{v \in U_m} \varphi(u)v_{d_m}$ for a generator $v \in U_m$. For convenience, we abbreviate $\sum \left( \log b_{n,m}^{\sharp/\flat} \sigma \varphi(\sigma), \log b_{n,m}^{\sharp/\flat} \sigma \varphi(\sigma) \right)$ by $\varphi(\sum \log \overline{b})$. By combining [LZ16] Proposition 7.1.4 and Proposition 7.1.5 (cf. also [Wa14, Proposition 7.6]) with the fact that $\varphi \left( \sum \log \overline{b} \right) \mathcal{H}_n(\varphi(\gamma)) \times \varphi(L^\sigma_p) = \sum \left( \log E(c_{n,m})^\sigma, \log E(c_{n-1,m})^\sigma \right) \varphi(\sigma) \times \varphi(L^\sigma_p)$,

we conclude that at any such $\varphi$, there is an element $H' \in \text{Frac } \Lambda_0$ so that $\varphi \left( \frac{-1}{H'} \right) \varphi \left( \sum \log \overline{b} \right) \left( \begin{array}{cc} \varphi(f^{\sharp})g_n - \varphi(L^\sigma_p) & 0 \\ \varphi(f^{\flat})g_n - \varphi(L^\sigma_p) & \end{array} \right) \mathcal{H}_n(\varphi(\gamma)) = (0, 0)$,

---

Footnote 5: This is a direct calculation on group-like elements. Note that in the corresponding [Wa14, Proposition 6.11], the bar is missing.
so that either the first (second) entry of \( \varphi \left( \sum \log(\tilde{b}) \right) \) is zero, or the difference between the terms in the first (second) diagonal entry \( \varphi(f^{\sharp/\♭}) - \varphi(L_p^{\sharp/\♭}) \) is. Thus, we can interpolate at the \( i \)th component of the collection of vectors \( \varphi \left( \sum \log(\tilde{b}) \right) \) as \( n \) and \( m \) vary, and encounter infinitely many non-zero values. The non-triviality of \( L_p^{\sharp/\♭} \) allows us to conclude that \( f^\bullet \) and \( L_p^{\sharp/\♭} \) agree at infinitely many points up to the elements \( h \) and \( H' \). Now when giving \( M(g)^* \) a \( \Lambda_q \)-integral structure, we use different normalizations at \( p \) and \( q \) (corresponding to the basis elements \( v^+ \) and \( cv^- \) at the top of [Wa14, page 39]), so we are off by another factor \( H'' \in \text{Frac} \Lambda_p \). We let \( H := H'H'' \).

**Remark 3.8.** If one of \( \Delta_\sharp \) or \( \Delta_\flat \) were zero, then this would imply that the \( c_{n,m}^{\sharp/\flat} \) and \( c_{n-1,m}^{\sharp/\flat} \) would be linearly dependent, much in the spirit of the ordinary case, in which they are norm-compatible. But this would mean that the arithmetic information of \( E \) would be encoded in just one Iwasawa function. Thus, the \( a_p \neq 0 \) case has a bit of an ordinary flavor.

**Definition 3.9.** We call any height one prime ideal that is a pullback to \( \Lambda_K \) of a height one prime ideal of \( \mathbb{Z}_p[[\text{Gal}(K_{\infty}/K^{\text{cyc}})]] \) a strong prime (ideal).

**Theorem 3.10.** The Greenberg-type main conjecture, i.e. full equality in Theorem 2.24 is equivalent to the \( \sharp/\♭ \)-Beilinson-Flach main conjecture Conjecture 2.44, up to powers of \( p \) and strong primes. The same can be said about each of the two halves (i.e. inclusion in just one direction between the algebraic and analytic sides) of the main conjectures.

**Proof.** We have that \( (\Delta_\sharp, \Delta_\flat) \in H^1_{\sharp} \oplus H^1_{\flat} = \text{ker} \text{Col}^0_p \oplus \text{ker} \text{Col}^0_p \), since the image of \( (\Delta_\alpha, \Delta_\beta) = (\Delta_\sharp, \Delta_\flat) \text{Log} \) at any \( \varphi \in \Gamma_{n,p} \times U_m \) is in the kernel of the pairing \( \langle P_{n,m,c_{n,m}}, P_{n,m,c_{n-1,m}} \rangle \) (cf. Proposition 2.15). We use a four-term exact sequence that follows from the Poitou-Tate exact sequence

\[
0 \rightarrow \mathcal{X}^{\sharp/\♭} \rightarrow H^1_{\bullet}(K_p, T \otimes \Lambda_K(-\Psi)) \rightarrow \mathcal{X}^{\sharp/\♭} \rightarrow 0,
\]

where the injectivity of the map \( \mathcal{X}^{\sharp/\♭} \rightarrow H^1_{\bullet}(K_p, T \otimes \Lambda_K(-\Psi)) \) follows from the nontrivially of \( \text{Wan}^\bullet \). By our choice of \( \bullet \in \{\sharp, \flat\} \), we have \( \text{Col}^\bullet(\Delta_\bullet) \neq 0 \), so that \( H^1_{\bullet} \neq 0 \) as well. We then have an exact sequence

\[
0 \rightarrow \mathcal{X}^{\sharp/\♭}/\Delta_\bullet \rightarrow \Lambda_K \otimes \mathbb{Q}_p/\text{Wan}^\bullet(\Delta_\bullet) \rightarrow \mathcal{X}^{\sharp/\♭} \rightarrow \mathcal{X}^{\sharp/\♭} \rightarrow 0.
\]

Since characteristic ideals are multiplicative in exact sequences, we conclude that the main conjectures are equivalent to each other up to strong primes, the discrepancy between \( \text{Wan}^\bullet(\Delta_\bullet) \) and \( L_p^{\sharp/\♭} \) (i.e. the factor \( H \) in Proposition 3.7).

**3.2 The \( \sharp/\♭ \)-Beilinson-Flach conjectures are equivalent to the \( \sharp/\♭ \)-\( \sharp/\♭ \) conjectures**

**Proposition 3.11.** Let \( h \in \mathbb{Q}_p \otimes \mathbb{Z}_p[[X, U]] \) be the element from Proposition 2.33. Then there exists a \( c \in \mathbb{Q}_p^\times \) so that

\[
\begin{pmatrix}
\text{Col}_p^\sharp(\Delta_\sharp) \\
\text{Col}_p^\flat(\Delta_\flat)
\end{pmatrix}
= h \cdot c \cdot
\begin{pmatrix}
L_{2H} & L_{01} \\
L_{2p} & L_{00}
\end{pmatrix}.
\]
Proof. It suffices to show that
\[
\log(Y)^T \left( \begin{array}{cc} \Lambda_1^T & \Lambda_2^T \\ \Lambda_1^T & \Lambda_2^T \end{array} \right) \log(X) = \log(Y)^T \times h \times \left( \begin{array}{cc} L_{\alpha\alpha} & L_{\beta\alpha} \\ L_{\alpha\beta} & L_{\beta\beta} \end{array} \right) \log(X)
\]
(4)
\[
= \left( \begin{array}{cc} L_{\alpha\alpha} & L_{\beta\alpha} \\ L_{\alpha\beta} & L_{\beta\beta} \end{array} \right)
\]
(5)

Since the entries of \(\log()\) are \(O(\log \frac{1}{x})\), we need to prove that (4) holds at all cyclotomic points in the variables \(X\) and \(Y\), i.e. at \(X = \zeta_{p^n} - 1\) and \(Y = \zeta_{p^m} - 1\).

For evaluation at \(Y = \zeta_{p^n} - 1\), we can relate \(\log(\zeta_{p^n} - 1)\) to the pairing \(P_{n,0,0}(\Delta_{i,j})\) by the proof of [Sp12, Proposition 6.5]. Using the relation
\[
(\Delta_{i,j}, \Delta_{k,l}) = (\Delta_{i,j}, \Delta_{k,l}) \log(X),
\]
the claim then follows from Proposition 2.15, the identity
\[
P_{n,m,x}(z) = \left( \sum_{\sigma \in \Gamma_{x,m} \times U_{m}} \log_p(x^\sigma) \sigma \right) \left( \sum_{\sigma \in \Gamma_{x,m} \times U_{m}} \exp_q^*(e^\sigma) \sigma^{-1} \right)
\]
and the explicit reciprocity law of Loeffler and Zerbes ([LZ16, Theorem 7.1.4 and Theorem 7.1.5]), which says that up to a constant in \(\mathbb{Q}_p^\times\),
\[
\pi_{x}^+ \left( \begin{array}{c} \pi_x^+ \\ \pi_y^+ \end{array} \right) \circ \exp^* \circ \varphi \circ (\Delta_{x}, \Delta_{y}) = \epsilon(x_{\varphi^{-1}}) \left( \begin{array}{cc} a^{-n} \eta_x^* \otimes \varphi(\omega_x^*) & 0 \\ 0 & \beta^{-n} \eta_y^* \otimes \varphi(\omega_y^*) \end{array} \right) \left( \begin{array}{cc} \varphi(L_{\alpha,\alpha}) & \varphi(L_{\beta,\alpha}) \\ \varphi(L_{\alpha,\beta}) & \varphi(L_{\beta,\beta}) \end{array} \right),
\]
where \(\varphi\) corresponds to a primitive character of \(\Gamma_{x,m} \times U_{m}\) with \(n > 0\). Here, \(\eta_x^*\) and \(\eta_y^*\) are the projections along the \(\alpha\)- and \(\beta\)-eigencomponents of \(\eta_q^*\), which are the duals of the element used in [KLZ]. Similarly, we \(\omega_x^*\) is the dual of the corresponding element in [KLZ], cf. [Wa14, Discussion in the middle of page 37]. Finally, we put \(\epsilon(x_{\varphi^{-1}}) = \int_{\mathbb{Q}_p^\times} \chi_{\varphi^{-1}}(x^{-1}) \lambda(x) dx\), where \(\lambda\) is (any) additive character so that \(\ker(\lambda) = \mathbb{Z}_p\) and \(\lambda \left( \frac{1}{p^n} \right) = \zeta_{p^n}\), and \(\chi_{\varphi}\) denotes composition of \(\Psi\) and \(\varphi\).

The constant \(c \in \mathbb{Q}_p^\times\) is chosen as in [Wa14, Corollary 7.5], where it is denoted \(H_1\).

\[\square\]

**Theorem 3.12.** The \(\ell/\ell\)-main conjecture (Conjecture 2.23) is equivalent to the \(\ell/\ell\)-Beilinson–Flach main conjecture, Conjecture 2.44 up to strong primes.

Proof. From the Poitou–Tate sequence, we have
\[
\chi^{\psi'} \rightarrow H^1(K_2, T \otimes \Lambda_k(-\Psi)) \rightarrow \chi^{\psi} \rightarrow \chi^{\psi'} \rightarrow 0.
\]
Recall we have chosen \(K\) so that neither \(\text{Col}^*\) nor \(\Delta_\bullet\) are zero. Since we thus have \(\text{Col}^*(\Delta_\bullet) \neq 0\) and \(\chi^{\psi'}\) is free of rank 1 (cf. Proposition 2.42), the first map in the above exact sequence being injective as a \(\Lambda_K\)-module is equivalent to its non-triviality.

Thus, taking quotients by the signed Beilinson–Flach elements rec. their images, we have the following exact sequence:
\[
0 \rightarrow \chi^{\psi'}/\Delta_\bullet \rightarrow \Lambda_K/\text{Col}^*(\Delta_\bullet) \rightarrow \chi^{\psi'} \rightarrow \chi^{\psi'} \rightarrow 0
\]
Now by multiplicativity of characteristic ideals, we get the desired equivalence of main conjectures.

3.3 Completing the argument

We want to carry over the inclusion of Theorem 2.27. First, we have the following consequence of Theorems 3.10 and 3.12:

**Proposition 3.13.** Under the assumptions of Theorem 2.27, we have \( \text{length}_P \mathcal{X}^{\ast} \geq \text{ord}_P L^{\ast} \) for any height one prime \( P \) that is neither \((p)\) nor the pullback of the augmentation ideal of \( \mathbb{Z}_p[[K_\infty/K_{cyc}]] \).

**Proof.** For the strong primes, note that the discussion of [Wa14, Lemma 8.4] applies since it does not assume \( a_p = 0 \). We thus conclude that this direction of the Greenberg-type main conjecture is true at such primes. For the four term exact sequence in the proof of Theorems 3.10 and 3.12, we thus have at any such strong prime \( P \) that:

\[
\text{length}_P \text{Char} \mathcal{X}^{\ast} \geq \text{ord}_P L^{\ast} \geq \text{ord}_P \text{Wan}^{\ast}(\Delta,),
\]

which by Theorem 3.10 implies that

\[
\text{length}_P \text{Char} \mathcal{X}^{\ast} \geq \text{length}\left(\frac{\mathcal{X}^{\ast}}{\Delta}\right),
\]

which in turn implies by Theorem 3.12 that

\[
\text{length}_P \text{Char} \mathcal{X}^{\ast} \geq \text{ord}_P \text{Col}^{\ast}(\Delta, \Delta) \geq \text{ord}_P L^{\ast}.
\]

This is The goal of this subsection is to take care of the prime \( p \) and the exceptional prime ideals.

For the prime \( p \), we first prove that the \( \mu \)-invariants of the \( p \)-adic \( L \)-functions \( L^{\ast} \) for \( \circ, \ast \in \{\# , \flat\} \) are zero.

**Proposition 3.14.** Suppose we have chosen the right \( K \) and \( \bullet \in \{\# , \flat\} \) as in Choice 2.9. Suppose \( N \) is a product of distinct unramified primes, an odd number of which are inert, so that for any such inert \( q \mid N, \overline{p} \mid G_q \) is ramified. Then \( \text{ord}_P L^{\circ} = 0 \) for \( \circ, \ast \in \{\# , \flat\} \) chosen so that \( L^{\circ} \neq 0 \).

**Proof.** By interpolation, it suffices to prove this for \( L^{\ast} \). As in [Wa14 Prop. 4.6], this follows from the vanishing of the \( \mu \)-invariants for the specialization of \( L^{\ast} \) to the anticyclotomic line. Note that the assumptions of [PW11] are not necessary in our case, cf. the discussion in [Wa14 Proposition 8.6] following a result of Chan-Ho Kim [Ki16]. In the case \( a_p = 0 \), this follows from [PW11 Theorem 2.5]. In the case \( a_p = 0 \), the anticyclotomic \( p \)-adic \( L \)-functions \( L^{\pm}_{\text{anti}} \) were constructed by combining sequences \( \{L_n\}_{n \geq 1} \) satisfying certain three-term relations with Kobayashi’s construction of the \( \pm \)-Coleman maps [Ko03 Section 8]. The sequences \( \{L_n\} \) have no \( a_p = 0 \) assumption, so that we can combine their construction (word for word in the same way) with that of the \( \# /\flat \)-Coleman maps in [Sp12 Section 5] to arrive at anticyclotomic \( p \)-adic \( L \)-functions \( L^{\pm}_{\text{anti}} \). The arguments in [PW11 Proof of Theorem 2.5] then show that \( \mu(L_n) = 0 \) for \( n \gg 0 \). But [PR03 discussion at the end of page 165] shows that the \( \mu_\# /\mu_\flat \)-invariants of Perrin-Riou are then 0. By [Sp15 Corollary 8.9], we conclude that the \( \mu \)-invariant of \( L^{\ast}_{\text{anti}} \) is zero.
Recall that we denoted by $L^{(K)\bullet}$ the $\bullet$ $p$-adic $L$-function for the elliptic curve $E^{(K)}$.

**Corollary 3.15.** Under the assumptions of Proposition 3.14 and the further assumption that the anticyclotomic root number is $-1$ (so that the restriction of $L^{\bullet\bullet}$ to the anticyclotomic line is nonzero), we have

$$\text{Char}(\mathcal{X}^{\bullet}) \text{ Char}(\mathcal{X}_K^{\bullet}) \subseteq (L^{\bullet} L^{(K)\bullet})$$

*Proof.* First, note that $L^{\bullet\bullet}|_{t=0} = L^{(K)\bullet}$. This can be seen as follows:

From the interpolation property, we have that restriction to the cyclotomic line (setting $X=Y$) yields

$$\left( \begin{array}{cc} L_{\alpha\alpha} & L_{\beta\alpha} \\ L_{\alpha\beta} & L_{\beta\beta} \end{array} \right) = \left( \begin{array}{c} L_{\alpha} \\ L_{\beta} \end{array} \right) \left( \begin{array}{cc} L^{(K)}_{\alpha\alpha} & L^{(K)}_{\beta\alpha} \\ L^{(K)}_{\alpha\beta} & L^{(K)}_{\beta\beta} \end{array} \right),$$

where $L^{(K)}_{\bullet}$ is the $L$-function of $E$ by the quadratic twist by $K$.

But we know that

$$\left( \begin{array}{c} L_{\alpha} \\ L_{\beta} \end{array} \right) = \text{Log}^T \left( \begin{array}{c} L^z_{\alpha} \\ L^z_{\beta} \end{array} \right)$$

and

$$\left( L^{(K)}_{\alpha\alpha}, L^{(K)}_{\beta\beta} \right) \text{Log}.$$

Restricting $\text{Log}(Y)^T \left( \begin{array}{cc} L^z_{\alpha\alpha} & L^z_{\beta\alpha} \\ L^z_{\alpha\beta} & L^z_{\beta\beta} \end{array} \right) \text{Log}(X)$ and factoring out the $\text{Log}$ matrices then yields

$$\left( \begin{array}{cc} L^z_{\alpha\alpha} & L^z_{\beta\alpha} \\ L^z_{\alpha\beta} & L^z_{\beta\beta} \end{array} \right) |_{t=0} = \left( \begin{array}{c} L^z_{\alpha} \\ L^z_{\beta} \end{array} \right) \left( L^{(K)}_{\alpha\alpha}, L^{(K)}_{\beta\beta} \right).$$

No exceptional prime divides $L^{\bullet\bullet}$ since the pullback of the augmentation ideal of the anticyclotomic line does not include $L^{\bullet\bullet}$, which follows from the fact that its specialization to the cyclotomic line is not zero by Choice 2.9. The corollary up to the prime $p$ thus follows from combining Theorem 2.27 and the equivalences of main conjectures Theorem 3.10, and for the correct power of $p$ we use Proposition 3.14. \qed

### 4. Conclusion

We are now ready to prove our main theorem.

**Theorem 4.1.** Let $E/\mathbb{Q}$ be an elliptic curve and $p > 2$ a prime of supersingular reduction. Assume that $E$ has square-free conductor. Choose $\bullet \in \{\sharp, \flat\}$ so that $L^{\bullet} \neq 0$. Then $L^{\bullet}$ is a characteristic power series of the Iwasawa module $\text{Hom}(\text{Sel}^\bullet(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$.

*Proof.* From [Sp12, Theorem 7.16], we know that $\text{Char}(\mathcal{X}^{\bullet}) \supseteq (L^{\bullet})$ and $\text{Char}(\mathcal{X}^{\bullet}_K) \supseteq (L^{(K)\bullet})$ Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) surjects onto $\text{Aut} E[p]$. Since $N$ is square-free, we only need $E[p]|_{\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ to be absolutely irreducible, as explained in [Sk14][discussion after Theorem 2.5.2]. This irreducibility is part of a theorem of Fontaine [Fo79]. For the entire theorem, see [E92, Theorem 2.6]. A proof can be found in [E92, Section 6.8]. Now we can choose our auxiliary $K$ so that it satisfies the assumptions for Proposition 3.13 [Wa14 Proof of Theorem 1.3, pg. 19], Choice 2.9 and the assumption on the anticyclotomic root number (cf. Corollary 3.15). By the square-free assumption
of $N$ and Ribet’s level-lowering theorem [Ri Theorem 8.2], $E[p]|_{\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ is ramified at some prime $q$. Now choose $K$ so that $p$ and all prime divisors of $N$ different from $q$ split while $q$ is inert. All this only inflicts congruence conditions on roc choice of $K$, so that Corollary 8.15 till holds. Thus, we have $\text{Char}(\mathcal{X}^*) \text{Char}(\mathcal{X}_K^*) = (L^*)(L(K)^*)$, whence $\text{Char}(\mathcal{X}^*) = (L^*)$ for our chosen $K$.

We now prove the corollaries concerning the leading term formula in the Birch and Swinnerton-Dyer conjecture.

THEOREM 4.2. (Birch and Swinnerton-Dyer formula at $p$ for rank 1)

Let $E$ be an elliptic curve with square-free conductor $N$ with supersingular reduction at $p \neq 2$. Suppose that $\text{ord}_{s=1} L(E, s) = 1$. Then

$$\left| \frac{L'(E, 1)}{\text{Reg}(E/\mathbb{Q})} \right|_p = \left| \frac{\#\text{III}(E/\mathbb{Q}) \prod_l c_l}{\#E(\mathbb{Q})^2_{\text{tor}}} \right|_p$$

Proof. The Iwasawa main conjecture is the only missing ingredient in the discussion of [Ko12, Proof of Corollary 1.3].

THEOREM 4.3. (Birch and Swinnerton-Dyer formula at $p$ for rank 0)

Let $E$ be an elliptic curve with square-free conductor $N$ with supersingular reduction at $p \neq 2$. Assume that $L(E, 1) \neq 0$. Then

$$\left| \frac{L(E, 1)}{\Omega} \right|_p = \left| \frac{\#\text{III}(E/\mathbb{Q}) \prod_l c_l}{\#E(\mathbb{Q})^2_{\text{tor}}} \right|_p$$

Here, $\text{III}(E/\mathbb{Q})$ is the Tate–Shafarevich group of $E/\mathbb{Q}$, $c_l$ are the Tamagawa numbers, and $\Omega$ is the Néron period. The proof of this theorem will occupy the final subsection of this paper. Combined with the corresponding result in the ordinary case [SU14, Theorem 3.35], this gives the leading term formula up to powers of 2 and bad primes.

4.1 Proof of the Birch and Swinnerton-Dyer formula at $p$ in the rank 0 case

We now prove Theorem 4.3. We denote by $E_{\infty,p}^\sharp$ (resp. $E_{\infty,p}$) the exact annihilator of the Coleman maps in the $\mathbb{Q}$-cyclotomic case $\ker \text{Col}_p^\sharp$ (resp. $\ker \text{Col}_p$) under the local Tate pairing. Similarly, we let $E_{0,p}^\sharp$ (resp. $E_{0,p}^\sharp$) be the exact annihilator of $\ker \text{Col}_p^\sharp$ resp. $\ker \text{Col}_{0,p}$.

Note that $E_{0,p}^\sharp = E_{0,p}^\vee = E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. We let

$$G^\bullet(Q_n) = \text{Im} \left( H^1(Q_n, E[p^\infty]) \rightarrow \frac{H^1(Q_{n,p}, E[p^\infty])}{E_{n,p}^\bullet} \times \prod_{v \neq p} \frac{H^1(Q_{n,v}, E[p^\infty])}{E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

for $n = 0$ or $n = \infty$. We denote $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ by $\Gamma$.

We then have a commutative diagram with exact sequences with right vertical map $g$:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \text{Sel}(E, \mathbb{Q})_p & \longrightarrow & H^1(Q, E[p^\infty]) & \longrightarrow & G^\bullet(Q) & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow g & & \\
0 & \longrightarrow & \text{Sel}^\bullet(E, Q_{\infty})_p & \longrightarrow & H^1(Q_{\infty}, E[p^\infty])_\Gamma & \longrightarrow & G^\bullet(Q_{\infty})_\Gamma & & \\
\end{array}$$

The maps $\text{Col}_{0,p}$ are denoted simply $\text{Col}_0$ in [Sp12].
For convenience, we let $P_E(Q_n) := \prod_{v \neq p} H^1(Q_{n,v}, E[p^\infty])$.

We denote the map $P_E(Q_0) \rightarrow P_E(Q_\infty)$ by $r$.

**Lemma 4.4.** We have:

$$\left| \text{Sel}^\bullet(E, Q_\infty)_p^{\text{Gal}(Q_\infty/Q)} \right| = \frac{|\text{Sel}(E, Q)_p|}{\# E(Q)_p} \times |\ker g|$$

**Proof.** The proof of [Gr95, Lemma 4.3] with “Sel" replaced by “Sel*" works, taking into account Lemma 4.6 below. □

**Lemma 4.5.** Denote by $c_l^{(p)}$ the $p$-component of the Tamagawa number $c_l$. We then have:

$$\frac{1}{\left| \text{Sel}^\bullet(E, Q_\infty)_p^{\text{Gal}(Q_\infty/Q)} \right|} = \prod_{l \text{ bad}} c_l^{(p)} \times \frac{1}{\# E(Q)_p \times |\ker g|}$$

**Proof.** The lemma with the Tamagawa factors $\prod_{l \text{ bad}} c_l^{(p)}$ replaced with $|\ker(r)|$ follows from the proof of [Gr95, Lemma 4.7], again with “Sel" replaced with “Sel*". Thus, it remains to prove that

$$|\ker(r)| = \prod_{l \text{ bad}} c_l^{(p)},$$

which we do prime by prime. Let $r_v$ be the component of $r$ at $v$.

If $v \neq p$ is a good reduction prime, we know that $\ker(r_v)$ is trivial by [Gr95, Proof of Lemma 3.3].

If $v = l$ is a bad reduction prime, the discussion after [Gr95, Lemma 3.3] shows that $|\ker(r_l)| = c_l^{(p)}$.

It thus remains to treat the case $v = p$. (Note that the methods in [Gr95, Lemma 3.4] do not apply since ordinarity is a key assumption there.) We want to show that the map

$$\frac{H^1(Q_p, E[p^\infty])}{E(Q_p) \otimes Q_p/\mathbb{Z}_p} \xrightarrow{r_p} \frac{H^1(Q_{p,\infty}, E[p^\infty])}{E_{\infty,p}}$$

is injective.

As in [Ko03, Proof of Proposition 9.2], we consider the following commutative diagram with exact sequences, were $X$ is the cyclotomic variable:

$$\begin{array}{c}
\ker \text{Col}^\bullet \rightarrow \mathbb{H}^1 \rightarrow \frac{\mathbb{H}^1_{\text{Col}^\bullet}}{\ker \text{Col}^\bullet} \rightarrow 0 \\
0 \rightarrow \ker \text{Col}^\bullet_{p,0} \rightarrow H^1(k_0, T) \rightarrow \frac{H^1(k_0, T)}{\ker \text{Col}^\bullet_{p,0}} \\
\end{array}$$

where $\mathbb{H}^1_{\text{Col}^\bullet} = \lim \mathbb{H}^1(Q_{p,n}, T)$.

By construction, the right vertical map is an isomorphism. The middle vertical map is a surjection by [Sp12, Lemma 2.3]. The snake lemma thus shows that the left vertical map is surjective. Taking Pontryagin duals, we see that $r_p$ is injective, as claimed. □

**Lemma 4.6.** $\text{Sel}^\bullet(E, Q_\infty)_p^{\text{Gal}(Q_\infty/Q)}$ is finite if $L(E, 1) \neq 0$. 21
Proof. It suffices to prove that $\mathcal{X}^*/X\mathcal{X}^*$ is finite. This follows from the small control theorem below, which implies that $\mathcal{X}^*/X\mathcal{X}^*$ is finite if and only if $\mathcal{X}^0*/X\mathcal{X}^0$ is, where $\mathcal{X}^0$ = $\text{Hom}(\text{Sel}^*(E, \mathbb{Q}), \mathbb{Q}_p/\mathbb{Z}_p)$. $\mathcal{X}^0*/X\mathcal{X}^0$ being finite is automatic by our assumption. One can also show that $\mathcal{X}^*/X\mathcal{X}^*$ is finite directly by observing that $L(E, 1) \neq 0$ implies that $f^*(0) \neq 0$ using [[Sp12|Sp12] table before Proposition 6.14].

**Lemma 4.7.** (Small Control Theorem) The natural morphism $\mathcal{X}^*/X\mathcal{X}^* \to \mathcal{X}^0*/X\mathcal{X}^0$ is surjective and has finite kernel.

**Proof.** The proof of [Ko03, Theorem 9.3] with $n = 0$ with the adjustment that $r_p$ is injective (cf. Lemma 4.5) works. (Note that in [Ko03, diagram on top of page 27], the terms on the right should be $\mathcal{P}_E(\mathbb{Q})$ and $\mathcal{P}_E(\mathbb{Q}_\infty)$ rather than $\prod_v \mathcal{H}^+(K_{n,v})$.)

**Lemma 4.8.** Let $f^*$ be a generator of the characteristic ideal of $\mathcal{X}^*$. Then

$$|f(0)|_p = \frac{|\text{Sel}^*(E, \mathbb{Q}_\infty)_{\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}|}{|\text{Sel}^*(E, \mathbb{Q}_\infty)_{\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}|}.$$  

**Proof.** This is a general fact about finitely generated $\Lambda$-modules, using the assumption that $\text{Sel}^*(E, \mathbb{Q}_\infty)_{\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}$ is finite, which Lemma 4.6 guarantees. See [[Gr95, Lemma 4.2]]

**Proof.** (Proof of Theorem) The theorem now follows using Lemma 4.8 and multiplying the terms in Lemma 4.4 and Lemma 4.5, and noting that since $E[p]$ is irreducible as a Galois representation, we necessarily have $|E(\mathbb{Q})_p| = 1$. The fact that we can replace Sel by III then follows from [Ko88, Sledstvie 2].

**Acknowledgments** We are grateful to Xin Wan for being very pessimistic about the feasibility of the $a_p \neq 0$ case, and for patiently answering numerous questions. We also thank Christopher Skinner for helpful discussions, and Richard Taylor who suggested doing a small seminar on this topic. Our thanks also go to Masato Kurihara, Antonio Lei, Yuichi Hirano, Wei Zhang, and Masataka Chida for pointing out inaccuracies in an earlier version of the manuscript. We thank Tadashi Ochiai for improving an earlier version, for a helpful piece of advice about the exposition, and for pointing out some errors in said earlier version of this work.
References

BS15 M. Bhargava, A. Shankar: *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Annals of Mathematics 181 (2015), no 2, 587-621.

BSZ M. Bhargava, C. Skinner, W. Zhang: *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture*, preprint. Available at [http://arxiv.org/abs/1407.1826](http://arxiv.org/abs/1407.1826).

E92 B. Edixhoven, *The weight in Serre’s conjectures on modular forms*, Inventiones Mathematicae 109, vol. 1 (1992), pp. 563–594.

El87 N. Elkies: *The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$*, Inventiones Mathematicae 89 (1987), no. 3, 561-567.

Fo79 J.-M. Fontaine: *Two letters to Serre*

Gr97 R. Greenberg:*Iwasawa theory for elliptic curves*, Lecture Notes in Mathematics, pp. 51–144. Arithmetic theory of elliptic curves. Lectures from the 3rd C.I.M.E. Session held in Cetraro, July 12–19, 1997. Edited by C. Viola. Lecture Notes in Mathematics, 1716. Springer-Verlag, Berlin; Centro Internazionale Matematico Estivo (C.I.M.E.), Florence, 1999.

Gr95 R. Greenberg:*Iwasawa theory and $p$-adic deformations of motives*. Motives (Seattle, WA, 1991), 19–223. Proc. Sympos. Pure Math., 55, Part 2, Amer. Math. Soc., Providence, RI, 1994.

Ha87 S. Haran: *$p$-adic L-functions for modular forms*, Compositio Mathematica, 62, no.1 (1987), p. 31-46.

JSW D. Jetchev, C. Skinner, X. Wan: *The Birch-Swinnerton-Dyer Formula For Elliptic Curves of Analytic Rank One and Main Conjectures*, [http://arxiv.org/pdf/1512.06894v1.pdf](http://arxiv.org/pdf/1512.06894v1.pdf).

Ko03 S. Kobayashi: *Iwasawa theory for elliptic curves at supersingular primes*, Inventiones Mathematicae 152 (2003), no.1, 1-36.

Ko12 S. Kobayashi: *The $p$-adic Gross-Zagier formula at supersingular primes*, Inventiones Mathematicae 191 (2013), no. 3, 527–629.

Ko88 V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $\text{III}(E, \mathbb{Q})$ for a subclass of Weil curves*, Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaia 52(3): pp 522-540, 670–671.

Ku03 M. Kuribara: *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I*, Inventiones Mathematicae 149 (2002), 195-224.

Lang S. Lang: *Cyclotomic Fields*, Graduate Texts in Mathematics 121 (1990), Springer, New York.

Le14 A. Lei: *Factorisation of two-variable $p$-adic L-functions*, Canadian Mathematical Bulletin, 57(4), 2014, 845-852.

LLZ14 A. Lei, D. Loeffler, S. Zerbes: *Euler systems for Rankin–Selberg convolutions of modular forms*, Ann. of Math. 180 (2014), no. 2, 653–771.

LZ16 D. Loeffler, S. Zerbes: *Rankin–Eisenstein classes in Coleman families*, submitted. [http://arxiv.org/abs/1506.06703](http://arxiv.org/abs/1506.06703).

LZ14 D. Loeffler, S. Zerbes: *Iwasawa theory and $p$-adic L-functions over $\mathbb{Z}_p^\infty$-extensions*, Int. J. Number Theory 10 (2014), no. 8, 2045–2095.
The Iwasawa Main Conjecture for elliptic curves at odd supersingular primes

Lo12 D. Loeffler: *p*-adic integration on ray class groups and non-ordinary *p*-adic *L*-functions, in Iwasawa Theory 2012, Contributions in Mathematical an dComputational Sciences, Vol. 7, pg. 357–378.

Ma73 Ju. Manin: *Periods of Parabolic Forms and p-adic Hecke series*, Sbornik 21 (1973), no. 3.

Ma72 B. Mazur: *Rational points of abelian varieties with values in towers of number fields*, Inventiones Mathematicae 18 (1972), 183-266.

MSD B. Mazur, P. Swinnerton-Dyer: *Arithmetic of Weil curves*, Inventiones Mathematicae 25 (1974), 1-61.

Po03 R. Pollack: *The *p*-adic *L*-function of a modular form at a supersingular prime*, Duke Mathematical Journal 118 (2003), no.3, 523-558.

PR03 B. Perrin-Riou: *Arithmétique des courbes elliptiques à réduction supersingulière*, Experimental Mathematics 12 (2003), 155-186.

PR90 B. Perrin-Riou: *Théorie d’Iwasawa *p*-adique locale et globale*, Invent. Math. 99, 247–292 (1990).

P+R04 R. Pollack, K. Rubin: *The main conjecture for CM elliptic curves at supersingular primes*, Annals of Mathematics 159 (2004), no.1, 447 -464.

PW11 R. Pollack, T. Weston: *Mazur–Tate elements of non-ordinary modular forms*, Duke Mathematical Journal 156 (2011) no. 3, 349–385.

Ri K. Ribet: *On modular representations of Gal$\overline{\mathbb{Q}}/\mathbb{Q}$ arising from modular forms*, Inventiones Mathematicae, 100 (1990),no. 2, pp. 431–476.

Ro84 D. Rohrlich: *On *L*-functions of elliptic curves and cyclotomic towers*, Inventiones Mathematicae 75 (1984), 409-423.

Ru91 K. Rubin: *The “main conjectures” of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), 25–68.

Silv J. Silverman: *The Arithmetic of Elliptic Curves*, Second Edition, Graduate Texts in Mathematics 106 (2009), Springer, New York.

Sk14 C. Skinner: *Multiplicative reduction and the cyclotomic main conjecture for GL$_2$* [arXiv:1407.1093]

SU14 C. Skinner, E. Urban: *The Iwasawa main conjectures for GL$_2$*, Inventiones Mathematicae 195 (2014), no. 1, 1–277.

SZ14 C. Skinner, W. Zhang: *Indivisibility of Heegner points in the multiplicative case*, [http://arxiv.org/pdf/1407.1099v1.pdf](http://arxiv.org/pdf/1407.1099v1.pdf)

Sp12 F. Sprung: *Iwasawa theory for elliptic curves at supersingular primes: A pair of Main Conjectures*, Journal of Number Theory 132 (2012), no. 7.

Sp15 F. Sprung: *On pairs of *p*-adic *L*-functions of modular forms of weight two*, submitted.

Ve03 O. Venjakob: *A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory*, Journal für die reine und angewandte Mathematik (Crelle’s Journal), 559 (2003), 153–191.

Wa14 X. Wan: *Iwasawa Main Conjecture for Supersingular Elliptic Curves*, [http://arxiv.org/abs/1411.6352](http://arxiv.org/abs/1411.6352)

Wa14+ X. Wan: *Iwasawa Main Conjecture for Rankin-Selberg *p*-adic *L*-functions: non-ordinary case*, [http://arxiv.org/abs/1408.4044](http://arxiv.org/abs/1408.4044)

Florian Sprung  fsprung@math.princeton.edu
Princeton University and the Institute for Advanced Study, School of Mathematics, 1 Einstein Dr or 304 Fine Hall, Princeton, NJ 08540, USA