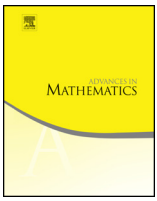
Advances in Mathematics 449 (2024) 109741

Contents lists available at ScienceDirect

Advances in Mathematics

journal homepage: www.elsevier.com/locate/aim



On Iwasawa main conjectures for elliptic curves at supersingular primes: Beyond the case $a_p = 0$ ☆

Florian Ito Sprung

Arizona State University, 901 S Palm Walk, Wexler Hall, Tempe, AZ 85287, United States of America

ARTICLE INFO

Article history:
Received 19 August 2021
Received in revised form 12 May 2024
Accepted 15 May 2024
Available online xxxx
Communicated by Kartik Prasanna

In memory of John Coates and Zhihuan Wang

MSC:
primary 11G40, 11F67
secondary 11R23, 11G05

Keywords:
Iwasawa theory
Elliptic curve
Birch and Swinnerton-Dyer

ABSTRACT

We reduce the chromatic Iwasawa main conjecture for elliptic curves to the conjectured existence of certain Beilinson–Flach classes in the supersingular case. This generalizes the method of Wan in which $a_p = 0$ was assumed; the main innovation of this paper consists in the new 2-dimensional technique to overcome this condition. We also derive the 3-part of the leading term formula in the Birch and Swinnerton-Dyer conjecture for analytic rank 0 or 1 from the main conjecture. Another consequence is that among those elliptic curves with a prescribed number of solutions modulo any fixed prime, infinitely many would satisfy the full Birch and Swinnerton-Dyer conjecture.

☆ This material is based upon work supported by the National Science Foundation under agreement No. DMS-1128155, and also ERC Grant 34061684. 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.

E-mail address: ian.sprung@gmail.com.

https://doi.org/10.1016/j.aim.2024.109741

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ and $p > 2$ be a prime of good reduction. The Iwasawa theory for elliptic curves is suitable for shedding light on the p-primary part of the BSD formula (BSD_p), which appears in the refined conjecture of Birch and Swinnerton-Dyer concerning the leading term of the Hasse–Weil L-function. The main conjecture of Iwasawa theory is mostly known in the case of ordinary reduction [25,63]. In this paper, we focus on the case of supersingular reduction, i.e. we require $p|a_p := p + 1 - \#\tilde{E}(\mathbb{F}_p)$ and investigate three Iwasawa main conjectures:

(i) a Greenberg-type main conjecture (representation-theoretic)
(ii) a formulation in terms of integral cohomology classes
(iii) the chromatic formulation (involving the chromatic, i.e. $\sharp/\flat$-objects)

These three conjectures are main conjectures for $\mathbb{Z}_p^2$-extensions of imaginary quadratic fields (also known as "two-variable main conjectures"), taking as additional ingredient a quadratic imaginary field K in which p is split. The last main conjecture (iii) is closest to BSD_p, and the finale of the paper is the implication (iii) $\implies BSD_p$ when the analytic rank is at most one, and is intended to be readable in its own right.[1]

The main part of the paper proves two equivalences

$$(i) \iff (ii) \iff (iii),$$

under the assumption:

Conjecture (*) There exist appropriate two-variable Beilinson–Flach classes. Here, 'appropriate' means that the Beilinson–Flach classes satisfy certain reciprocity laws at the two primes above p. See Conjecture 3.33 in the main part for the precise formulation.[2]

In fact, our conclusion is stronger: Each of the three main conjectures is an equality of ideals of the form (analytic object) = (algebraic object), and we prove that the three statements of the form (analytic object) $\subset$ (algebraic object) are equivalent to each other. We also prove that the three statements concerning the reverse conclusion are equivalent to each other. The inclusion (analytic object) $\supset$ (algebraic object) in the context of (i) follows from a recent result of [11], originally announced in [74]. What our paper accomplishes under Conjecture (*) is then to transfer their result over to the context of (iii): We have (analytic object) $\supset$ (algebraic object) in a chromatic formulation of the two-variable Iwasawa main conjecture, which we recall concerns the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field K. By choosing this K judiciously, we use this to conclude that (analytic object) $\supset$ (algebraic object) holds for the one-variable chromatic main

[1] We invite the interested reader to study this two-dimensional argument first, reflecting the arithmetic of elliptic curves as two-dimensional Galois representations.

[2] These are believed to exist, and according to referee#2, a construction in the ordinary case and the case $a_p = 0$ is currently in progress (joint work of Burungale, Skinner, Tian, and Wan).

conjecture [64, Conj. 7.21] over $\mathbb{Q}$. Together with the known inclusion (analytic object) $\subset$ (algebraic object) due to Kato [25], we conclude that the one-variable chromatic main conjecture holds under Conjecture (*) and some mild assumptions.

As for the applications to (BSD_p), the general supersingular case is more involved than the $a_p = 0$ case: In the $a_p = 0$ subcase, the $\pm$-theory reduces the result in essentially two lines [74] to an argument of Greenberg [18]. When $a_p \neq 0$, in which case $p = 3$, the analogue of these two lines is the last subsection of this paper before the coda, reflecting the complexity for the general supersingular case.

The main results in the context of classical results. One important consequence of the Iwasawa main conjecture for a prime p in its classical form (analytic object)= (algebraic object) is the p-part of the Birch and Swinnerton-Dyer Formula, when the rank part of the conjecture is known (currently in the case of analytic rank at most one). See [75, page 32] for a description of the full Birch and Swinnerton-Dyer conjectures. One strategy for proving the Birch and Swinnerton-Dyer Formula is thus to prove the main conjecture at every prime p.

When p is of good ordinary reduction (i.e. $p \nmid a_p := p + 1 - \#\widetilde{E}(\mathbb{F}_p)$), this program is now largely complete. Mazur and Swinnerton-Dyer introduced the analytic object, the (ideal generated by) the p-adic L-function in [47]. On the algebraic side, Mazur studied the corresponding Selmer group in [44], whose characteristic ideal is the algebraic object. In the complex multiplication (CM) case, Rubin [59] proved the main conjecture by finding a suitable Euler system. Kato proved half the main conjecture in the non-CM case by constructing an Euler system (for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$) using Siegel units, showing that the p-adic L-function is included in the characteristic ideal associated to the Selmer group [25]. Finally, Skinner and Urban [63] 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 analytic object, either of the two p-adic L-functions due to Amice–Vélu [1] and Vishik [70] (see also [45]) is not an element of the Iwasawa algebra, and correspondingly the Selmer group is not a cotorsion Iwasawa module. Perrin-Riou [51] and Kato [25] made important progress in our understanding of the supersingular case, and formulated main conjectures. When $a_p = 0$, the work of Pollack and Kobayashi gave rise to a formulation of the main conjecture in the spirit of the ordinary case: Pollack [50] found a pair of p-adic L-functions L^+ and L^- inside the Iwasawa algebra, while Kobayashi found two corresponding submodules $\mathrm{Sel}^-(E/\mathbb{Q}_\infty)$ and $\mathrm{Sel}^+(E/\mathbb{Q}_\infty)$ of the classical Selmer group,[3] and formulated a pair of main conjectures in terms of these *signed* p-adic L-functions and *signed* Selmer groups. Here, $\mathbb{Q}_\infty$ denotes the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Relying on Kato's Euler system, he proved one inclusion [32]. Pollack and Rubin [54] settled the main conjecture in the case of complex multiplication (in which automatically $a_p = 0$) by adapting Rubin's Euler system [59].

[3] The reversal of signs is no typo!

Finally, Wan [74] started a program to settle the main conjecture in the non-CM case *but assuming that* $a_p = 0$ by giving a converse to this theorem via a U(3,1) Eisenstein series method. One crucial piece of progress in the program is the main result of [11]. Note that the Hasse–Weil bound $|a_p| \leqslant 2\sqrt{p}$ implies that for $p \geqslant 5$, p being supersingular and $a_p = 0$ are equivalent. This means that the methods for the ordinary case and the $a_p = 0$ case are sufficient to formulate and prove the main conjecture when $p \geqslant 5$.

However, we are interested in proving the Birch and Swinnerton-Dyer formula, for which every prime is important. In view of recent progress on the 2-part [10] (using non-Iwasawa theoretic methods specific to $p = 2$), a complete understanding of the 3-part is desirable. As stated above, the current techniques can only handle five out of the seven possible a_3's of E – they apply when $a_3 \in \{2, 1, 0, -1, -2\}$ but not when $a_3 \in \{3, -3\}$. Counting elliptic curves mod 3, we see that 18 out of the possible 162 elliptic curves (i.e. a proportion of $\frac{1}{9}$) are excluded. The purpose of this paper is to fix this unfortunate state of affairs and give a proof of the main conjecture in the general supersingular case, at every odd prime, assuming the existence of an Euler system of Beilinson–Flach classes. We denote this assumption throughout the paper by (*).

The $\pm$-theory of Pollack and Kobayashi for the case $a_p = 0$ has been generalized by the author to the general supersingular case ($p|a_p$). The generalizations of Pollack's $L^{\pm}$ are denoted $L^{\sharp/\flat}$ [66] and those of Kobayashi's $\mathrm{Sel}^{\mp}(E/\mathbb{Q}_\infty)$ are denoted $\mathrm{Sel}^{\sharp/\flat}(E/\mathbb{Q}_\infty)$ [64]. We call $\mathrm{Sel}^{\sharp/\flat}(E/\mathbb{Q}_\infty)$ the *chromatic* Selmer groups.[4] The main conjecture connects $L^{\sharp/\flat}(E)$ and $\mathrm{Sel}^{\sharp/\flat}(E/\mathbb{Q}_\infty)$, and is the main theorem of this paper:

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve and $p > 2$ a prime of supersingular reduction. Assume that E has square-free conductor and that Conjecture 3.33 holds. Then $L^{\sharp/\flat}(E)$ are each characteristic power series of the Iwasawa module* $\mathrm{Hom}(\mathrm{Sel}^{\sharp/\flat}(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$.

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,*

$$\left|\frac{L(E,1)}{\Omega}\right|_p = \left|\#Ш(E/\mathbb{Q})\prod_l c_l\right|_p.$$

Without Conjecture (*), we can say

$$\left|\frac{L(E,1)}{\Omega}\right|_p \leqslant \left|\#Ш(E/\mathbb{Q})\prod_l c_l\right|_p.$$

[4] The notation $\sharp/\flat$ was introduced because Kobayashi's and Pollack's sign conventions differed.

Here, $Ш(E/\mathbb{Q})$ is the Šafarevič–Tate group of $E/\mathbb{Q}$, c_l are the Tamagawa numbers, and Ω is the Néron period. The second statement follows from [64, Theorem 7.16], and a new argument is needed to deduce (BSD_p) from an integral main conjecture, which the reader can find in subsection 5.2. (In the ordinary case, the corresponding argument is [18, Section 4], and the modification for the $a_p = 0$ case is two lines in [74].)

Combining the first statement with the corresponding result in the ordinary case [63, Theorem 3.35], this gives the leading term formula up to powers of 2 and bad primes.

As for the analytic rank one case, we have analogously:

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

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

Without Conjecture (*),

$$\left| \frac{L'(E,1)}{\mathrm{Reg}(E/\mathbb{Q})\Omega} \right|_p \leqslant \left| \frac{\#Ш(E/\mathbb{Q}) \prod_l c_l}{\#E(\mathbb{Q})^2_{\mathrm{tor}}} \right|_p .$$

Here, $\mathrm{Reg}(E/\mathbb{Q})$ denotes the regulator of E, and $E(\mathbb{Q})_{\mathrm{tor}}$ is the torsion part of $E(\mathbb{Q})$. This corollary is [33, Corollary 1.3], where the only assumption is our main theorem.

For a different approach in the rank one case that needs the assumption $a_p = 0$, see [24, Theorem 1.2.1].

In the coda, we discuss some numerical examples and infinite families of elliptic curves that satisfy the full Birch and Swinnerton-Dyer conjecture:

Corollary 1.4. *Assume (*). Then there are infinitely many elliptic curves* E *with* $a_3(E) = 3$ *that satisfy the full Birch and Swinnerton-Dyer conjecture, and the same is true for* $a_3(E) = -3$.

This corollary follows from the main theorem and work of [10] to treat the even prime. The explicit algorithm for finding the infinitely many elliptic curves involves quadratic twists and was originally developed in [10]. We are grateful to S. Zhai for providing us with the Examples A.3 and A.5 of such families.

We note that the case $a_3 = \pm 3$ is the last theoretical obstacle for finding infinitely many families of elliptic curves with a fixed Frobenius trace at some chosen prime. Thus, this corollary says that the following holds:

Corollary 1.5. *Assume (*). Pick any prime* p *and any integer* $n \in (p+1-2\sqrt{p}, p+1+2\sqrt{p})$ *of possible number of solutions of elliptic curves modulo* p. *Then infinitely many elliptic curves with* n *solutions modulo* p *satisfy the full Birch and Swinnerton-Dyer conjecture.*

Raw ingredients for the proof. The known inclusion of $L^{\sharp/\flat}$ into the characteristic ideal coming from $\mathrm{Sel}^{\sharp/\flat}$ follows [32,64] from an equivalent inclusion in terms of Kato's Euler system – thus the main goal of this paper is to study the other inclusion.
For the other inclusion, we introduce a quadratic imaginary field K so that $(p) = \mathfrak{pq}$ splits, much like [63]. Much of the arithmetic of E along the $\mathbb{Z}_p^2$-extension K_∞ of K should be encoded in a pair of cohomology classes – Beilinson–Flach classes $\Delta_\alpha, \Delta_\beta$ similar to the classes due to Kings, Loeffler, and Zerbes (KLZ), found in [30], cf. also its sequel [31] – that generalize Kato's Euler system.

Conjecture 3.33 This assumption not only encompasses the existence of Δ_α and Δ_β, but also their reciprocity laws. The KLZ reciprocity law connects the $\mathfrak{q}$-local component of $\Delta_{\alpha/\beta}$ to p-adic L-functions $L_{\alpha\alpha}, L_{\alpha\beta}, L_{\beta\alpha}$, and $L_{\beta\beta}$ (whose construction goes back to Haran [20]) that interpolate twists of the special value of the complex L-function by characters factoring through $\mathrm{Gal}(K_\infty/K)$. Another part of the assumption is a reciprocity law that connects the $\mathfrak{p}$-local part of $\Delta_{\alpha/\beta}$ to a p-adic L-function $L^{\forall 0}$ associated to E and a Hida family of CM forms associated to K_∞/K.

The function $L^{\forall 0}$ has bounded coefficients and a main conjecture can be formulated in its classical form.
Thus, one may hope to use the reciprocity laws to connect this other inclusion to a statement relating Haran's p-adic L-functions with arithmetic information of E along $\mathrm{Gal}(K_\infty/K)$. This statement involving K should project to $\mathbb{Q}$ and become the connection that is the "hard" inclusion, i.e. (algebraic object) $\subset$ (analytic object), of the main conjecture over $\mathbb{Q}$. However, there is a crucial obstacle – it is that the Beilinson-Flach classes $\Delta_{\alpha/\beta}$ and Haran's $L_{\alpha\alpha}$ etc. are not in the classical form since they are not integral, i.e. not elements of a ring of power series with bounded coefficients. Pottharst's theory [56] could overcome this obstacle (but this is not the approach we follow).

Wan's contributions ($a_p = 0$). Motivated by Pollack's construction of integral power series $L^{\pm}$, Wan took a normalized average of Δ_α and Δ_β to arrive[5] at integral classes. Under a map $\mathrm{Col}_{\mathfrak{q}}^+$ due to BD Kim [28], the $\mathfrak{q}$-local image of Δ_+ maps to an Iwasawa function L^{++} due to Loeffler [42]. This integral L^{++} is a normalized average of Haran's functions, and the work of Kim and Loeffler supplies us with the integral '++ main conjecture' relating L^{++} and the arithmetic of E along K_∞/K in the form of an integral Selmer group whose local condition at $\mathfrak{q}$ (resp. $\mathfrak{p}$) comes from $\ker \mathrm{Col}_{\mathfrak{q}}^+$ (resp. $\ker \mathrm{Col}_{\mathfrak{p}}^+$). Recall that for $\mathbb{Q}_\infty/\mathbb{Q}$, there were two equivalent formulations of main conjectures; in terms of (Kato's) Euler systems, and in terms of p-adic L-functions (the $L^{\sharp/\flat}$). Taking this as a hint, Wan formulated a main conjecture for K_∞/K in terms of Δ_+ and showed equivalence to the ++ main conjecture. Relying on an explicit description of Δ_+ and $\ker \mathrm{Col}_{\mathfrak{p}}^+$ at finite layers in the local $\mathbb{Z}_p^2$-extension, he was able to define a map LOG^+ [74, Definition 2.9] that sends Δ_+ to $L^{\forall 0}$, which can be regarded as an integral version of the reciprocity law in [40, Theorem 7.1.4 and 7.1.5]. Via his map LOG^+, he showed

[5] Here, Wan implicitly assumed that Δ_α and Δ_β existed, i.e. Wan assumed Conjecture (*).

that the integral main conjecture involving $L^{\forall 0}$ is equivalent to the one in terms of Δ_+, obtaining in summary an equivalence of main conjectures (MC)

$$++\text{MC} \xLeftrightarrow{\text{Kim's } \mathrm{Col}_{\mathfrak{q}}^{+}} \text{MC in terms of } \Delta_+ \xLeftrightarrow{\text{Wan's } LOG^{+}} \text{MC in terms of } L^{\forall 0}.$$

He then used this equivalence to carry the known inclusion of the MC involving $L^{\forall 0}$ over to a corresponding inclusion of the ++ MC, and specialized from K to $\mathbb{Q}$ to prove the 'other inclusion' of the +main conjecture of Kobayashi. A completely analogous construction lets one prove Kobayashi's −main conjecture.

Analogy with classical Iwasawa theory. The equivalence of the three main conjectures above has an analogue in classical Iwasawa theory:

$$\left(\begin{smallmatrix}\text{MC involving}\\ \text{Kubota–Leopoldt}\\ p\text{-adic } L\text{-function}\end{smallmatrix}\right) \iff \left(\begin{smallmatrix}\text{MC in terms of}\\ \text{cyclotomic units}\end{smallmatrix}\right) \iff \left(\begin{smallmatrix}\text{Greenberg's}\\ \text{formulation of MC}\end{smallmatrix}\right).$$

Greenberg's formulation of the classical main conjecture is representation-theoretic [18], as is the main conjecture in terms of the Greenberg-type p-adic L-function $L_p^{\forall 0}$.

New ideas ($p|a_p$). The idea for $p|a_p$ is to come up with a similar equivalence as in the $a_p = 0$ case, but a crucial difference with both classical Iwasawa theory and with the $a_p = 0$ theory is that the number of main conjectures in each of the three categories is important: There are four (=two squared), two, and one.

To handle the general supersingular case, four sets of ideas must be introduced. These are the $\sharp/\flat$ Coleman maps, 2-dimensionality, zero-function avoidance, and most importantly the $\sharp/\flat$ Perrin-Riou–Wan logarithm maps[6] $\mathscr{L}^{\sharp/\flat}$.

$\sharp/\flat$ Coleman maps: Kim's construction of ±Coleman maps relied on $a_p = 0$ [28]. We generalize this to the $p|a_p$ case by constructing $\mathrm{Col}^{\sharp/\flat}$ at $\mathfrak{p}$ and $\mathfrak{q}$, much in the spirit of [64], and use these maps to define four doubly-chromatic Selmer groups $\mathrm{Sel}^{\sharp\sharp}, \mathrm{Sel}^{\sharp\flat}, \mathrm{Sel}^{\flat\sharp}, \mathrm{Sel}^{\flat\flat}$. We formulate four analogues of the ++ main conjectures. These are the $\sharp\sharp, \sharp\flat, \flat\sharp$, and $\flat\flat$ main conjectures that relate the doubly-chromatic Selmer groups to doubly-chromatic p-adic L-functions $L^{\sharp\sharp}, L^{\sharp\flat}, L^{\flat\sharp}, L^{\flat\flat}$ due to Lei [35], which generalize Loeffler's construction to $p|a_p$.

2-dimensionality: Recall that the analytic arithmetic information of E along K_∞/K was packaged into Haran's four p-adic L-functions $L_{\alpha\alpha}$ etc. A theorem of Lei says that his doubly chromatic functions can be linearly recombined to obtain those of Haran [35, Theorem 2.2]. One idea of this paper is a simpler formulation of Lei's theorem in the form

$$\begin{pmatrix} L_{\alpha\alpha} & L_{\beta\alpha} \\ L_{\alpha\beta} & L_{\beta\beta} \end{pmatrix} = \mathcal{L}og(Y)^T \begin{pmatrix} L^{\sharp\sharp} & L^{\flat\sharp} \\ L^{\sharp\flat} & L^{\flat\flat} \end{pmatrix} \mathcal{L}og(X).$$

Thus, Lei's doubly-chromatic functions should be thought of as a 2×2 matrix, and the linear combinations can be described by multiplying by the logarithm matrices $\mathcal{L}og$

[6] We called these Wan maps $\mathrm{Wan}^{\sharp/\flat}$ in an earlier version of this paper.

(which are explicit 2×2 matrices, see e.g. [66, Section 4.1]) on both sides. When $a_p = 0$, these logarithm matrices are essentially diagonal, which is why Wan was able to avoid this matrix formulation of affairs completely and only consider the function L^{++} without losing information. For the general case $p|a_p$, the entries in the middle matrix can not be constructed separately, so that we need to consider all of them. Taking this matrix as a hint, we construct an analogue of Wan's integral cohomology class Δ_+. Our analogue is a row vector $(\Delta_\sharp, \Delta_\flat)$ of integral cohomology classes that factors out the non-integral part from a vector $(\Delta_\alpha, \Delta_\beta)$ consisting of the Beilinson-Flach classes. The reason this is the correct analogue is that the statement 'Kim's $\mathrm{Col}_{\mathfrak{q}}^{+}$ sends the $\mathfrak{q}$-local image of Wan's Δ_+ to Loeffler's L^{++}' becomes the following 2-dimensional statement when $p|a_p$[7]: Up to some controllable constants,

$$\begin{pmatrix} L^{\sharp\sharp} & L^{\flat\sharp} \\ L^{\sharp\flat} & L^{\flat\flat} \end{pmatrix} = \begin{pmatrix} \mathrm{Col}_{\mathfrak{q}}^{\sharp}(\Delta_\sharp) & \mathrm{Col}_{\mathfrak{q}}^{\sharp}(\Delta_\flat) \\ \mathrm{Col}_{\mathfrak{q}}^{\flat}(\Delta_\sharp) & \mathrm{Col}_{\mathfrak{q}}^{\flat}(\Delta_\flat) \end{pmatrix} = \text{“} \begin{pmatrix} \mathrm{Col}_{\mathfrak{q}}^{\sharp} \\ \mathrm{Col}_{\mathfrak{q}}^{\flat} \end{pmatrix} \circ (\Delta_\sharp, \Delta_\flat).\text{”}$$

These ideas are then developed further to show an 'equivalence[8]' of sets of main conjectures

$$\text{four MC's } (\sharp\sharp,\ \sharp\flat,\ \flat\sharp, \text{ and } \flat\flat) \quad \xleftrightarrow{\begin{pmatrix} \mathrm{Col}_{\mathfrak{q}}^{\sharp} \\ \mathrm{Col}_{\mathfrak{q}}^{\flat} \end{pmatrix}} \quad \text{two MC's (in terms of } \Delta_\sharp \text{ resp. } \Delta_\flat),$$

where each Coleman map provides an equivalence between two MC's on the left and one on the right.[9] Below we will see that the two MC's on the right are equivalent to each other as well, so that all six conjectures encode the same statement. However, this equivalence only works for objects that are non-zero.

Zero-function avoidance: When $a_p \neq 0$, we can only say that at least one of the four functions $L^{\sharp\sharp}, L^{\sharp\flat}$ etc. is nonzero. Thus, we are only guaranteed that one of the integral cohomology classes $\Delta_\sharp$ and $\Delta_\flat$ is nonzero, unlike in the case $a_p = 0$, where both are nonzero. This becomes an issue when specializing from the $\mathbb{Z}_p^2$-extension of K to the cyclotomic $\mathbb{Z}_p$-extension, where we need either $L^{\sharp\sharp}$ or $L^{\flat\flat}$ to be nonzero. We can guarantee this by choosing K so that $L(E^{(K)}, 1) \neq 0$, invoking results of Waldspurger or Bhargava–Shankar.

The $\sharp/\flat$ Perrin-Riou–Wan logarithm maps $\mathscr{L}^{\sharp/\flat}$ are needed for the 'equivalence' between the main conjectures involving $\Delta_{\sharp/\flat}$ and the main conjecture involving $L^{\forall 0}$:

$$\text{any of the MC's in terms of } \Delta_\sharp \text{ resp. } \Delta_\flat \quad \xleftrightarrow{\mathscr{L}^{\sharp} \text{ resp. } \mathscr{L}^{\flat}} \quad \text{the MC involving } L^{\forall 0},$$

but a crucial difficulty arises in the case $a_p \neq 0$. For $a_p = 0$, Wan connected the integral cohomology classes $\Delta_\sharp$ and $\Delta_\flat$ to the Greenberg-type p-adic L-function $L^{\forall 0}$ by 'evaluat-

[7] Here, we abuse notation a bit and denote by $\Delta_{\sharp/\flat}$ their $\mathfrak{q}$-local images.
[8] Equivalence up to some controllable primes, as explained at the end of the introduction.
[9] For example, the $\sharp\sharp$-MC and $\sharp\flat$-MC on the left are equivalent to the MC in terms of $\Delta_\sharp$, and thus equivalent to each other.

ing' it – invoking a KLZ reciprocity law. This was possible because the domain of $\Delta_\sharp$ and $\Delta_\flat$ could be described explicitly at the finite layers of the associated tower of number fields, and so could the coordinates of $\Delta_\sharp$ and $\Delta_\flat$. This gave rise to a quick and natural construction of his connecting map LOG^+. None of this is possible when $a_p \neq 0$.

We overcome these difficulties as follows: First, we perform a guess for indirectly describing the domain of $\Delta_\sharp$ and $\Delta_\flat$ at the infinite layer, and prove this guess is the right one. This information may not allow us to explicitly describe the domain at finite level, but it provides us with coordinates of the vector $(\Delta_\sharp, \Delta_\flat)$ at finite level.

The second difficulty was the inability to 'evaluate' the coordinates of $(\Delta_\sharp, \Delta_\flat)$ at finite characters. The reason for this difficulty is that the evaluation of coordinates is indirect to begin with, as 'evaluation' means 'taking the image under the KLZ reciprocity map.' The reciprocity map does not evaluate the coordinates themselves, but rather their product with a certain 2×2 matrix $\mathcal{H}_n$. When $a_p = 0$, this is no problem, since the matrix is diagonal or antidiagonal, so that Wan can easily get a handle on the coordinates. The reason the case $a_p \neq 0$ is hard is that in general, all entries of $\mathcal{H}_n$ are non-zero (for $n > 0$).

We overcome this difficulty by showing that *the two coordinates of the integral cohomology classes are equal*, and thus can be thought of as one scalar matrix. The coordinates thus commute with $\mathcal{H}_n$, allowing us to shift the difficulty over into a setting that allows us to invoke the Kings–Loeffler–Zerbes reciprocity law. At heart lies a trace computation in the form of a matrix identity that makes use of a *six-periodicity* coming from the fact that the roots of the Hecke polynomial $X^2 - a_pX + p$ are normalized fourth or sixth roots of unity.

The reason we put the term 'equivalence' in quotes is that the equivalences only hold up to certain prime factors. Invoking a result of Pollack and Weston, we are able to control these primes. Combined with the right choice of K, we obtain enough information about the doubly-chromatic main conjecture so that projecting down to $\mathbb{Q}$ results in our main theorem.

Outlook. Since earlier versions of this paper were made available (e.g. the arxiv post [67]), our results and ideas have been generalized in various directions. Büyükboduk and Lei [5] have adapted the ideas of this paper, e.g. the construction of integral $\sharp/\flat$ cohomology classes to formulate a two-variable main conjecture for weight two modular forms and prove one inclusion, using the theory of Wach modules.

In a beautiful development, Büyükboduk, Lei, Loeffler, and Venkat [7] have been developing an Iwasawa theory of Ranking-Selberg products of p-supersingular modular forms, in which they give an algebraic construction of non-bounded Beilinson-Flach elements, and work towards constructing their doubly-chromatic integral versions in the spirit of this paper. (See also partial results towards this in the case $a_p = 0$ in [6]).

For some ingredients towards a proof of the chromatic main conjectures in the case of modular forms of weight two relying on some of the methods in this paper, see [12].

2. Notation

Notation first used in section 3.1

$\mathbb{Q}_\infty$	the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$
$\Phi_{p^n}(Y)$	the p^nth cyclotomic polynomial $\sum_{i\geqslant 0}^{p-1} Y^{p^{n-1}i}$
ζ_{p^n}	a primitive p^nth root of unity
γ	a topological generator of $1+2p\mathbb{Z}_p$, or its image in a quotient
α and β	the roots of the Hecke polynomial $Y^2 - a_p Y + p$
Ω_E	the real Néron period of E
T and V	$T =$ the p-adic Tate-module for E, and $V = \mathbb{Q}_p \otimes T$
$\mathbb{Q}_{p,n}$	the nth layer in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$

Notation first used in section 3.2

K	a quadratic imaginary field in which p splits as $\mathfrak{pq}$
K_∞, K_{cyc} , K_{anti}	the $\mathbb{Z}_p^2$-extension, the cyclotomic $\mathbb{Z}_p$-extension, and the anticyclotomic $\mathbb{Z}_p$-extension of K
Ω_E^+ and Ω_E^-	the real and imaginary periods of E
$K(\mathfrak{p}^\infty)$; $K(\mathfrak{q}^\infty)$	the $\mathfrak{p}^\infty$ ray class field; the $\mathfrak{q}^\infty$ ray class field
Λ_K	$\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \cong \mathbb{Z}_p[[X,Y]]$. We identify $1+X$ with a generator of $\mathrm{Gal}(K(\mathfrak{p}^\infty)\cap K_\infty/K)$ and $1+Y$ with one for $\mathrm{Gal}(K(\mathfrak{q}^\infty \cap K_\infty)/K)$.
k, O_k	an unramified extension of $\mathbb{Q}_p$ and its ring of integers
$k_{0,m}$	the degree p^m unramified extension of $\mathbb{Q}_p$
$k_n, \mathfrak{m}_n$	the $\mathbb{Z}/p^n\mathbb{Z}$-subextension of $k(\zeta_{p^{n+1}})$, the maximal ideal in its integer ring
$k_{n,m}, \mathfrak{m}_{n,m}$	the objects above with $k = k_{0,m}$
U	the unramified variable, i.e. $1+U$ is identified with a topological generator of $\varprojlim_m \mathrm{Gal}(k_{0,m}/k)$.
$\Lambda_{n,m}$	$\mathbb{Z}_p[\mathrm{Gal}(k_{n,m}/\mathbb{Q}_p)]$
Λ	$\mathbb{Z}_p[[X]] \cong \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$
t_{anti}	the anticyclotomic variable

Notation first used in sections 3.3 and 3.4

$U_\mathfrak{p}$	the group $\mathrm{Gal}(K_{\infty,\mathfrak{p}}/K_{cyc,\mathfrak{p}}) \cong \mathbb{Z}_p$; K_{cyc} is the cyclotomic $\mathbb{Z}_p$-extension of K
Λ_K^*	the Pontryagin dual of Λ_K
Ψ	the character $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K_\infty/K) \to \Lambda_K^\times$
$\Lambda_K^*(\Psi)$	Λ_K^* twisted by Ψ
$\mathcal{W}$ and $\mathcal{T}$	$T \otimes \Lambda_K^*(\Psi)$ and $T \otimes \Lambda_K(-\Psi)$
S	a finite set of places containing p, ∞, and the bad primes of E
L^S	the maximal extension of a number field L that is unramified outside S

Notation first used in section 4

$\Gamma_{n,\mathfrak{q}}$	the Galois group of the cyclotomic $\mathbb{Z}/p^n\mathbb{Z}$-extension of $K_\mathfrak{q}$
$U_{m,\mathfrak{q}}$	the Galois group of the unramified $\mathbb{Z}/p^m\mathbb{Z}$-extension of $K_\mathfrak{q}$

3. 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 3.1) 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 "doubly-chromatic main conjectures" (or "$\sharp/\flat$-$\sharp/\flat$ main conjectures" – subsection 3.2), the Greenberg-type main conjecture (subsection 3.3), and the main conjecture involving integral cohomology classes of $\sharp/\flat$-Beilinson-Flach elements (subsection 3.4). In

section 4, we will prove that the ♯/♭-♯/♭ main conjectures and the Greenberg-type main conjecture are equivalent to the ♯/♭-Beilinson-Flach element main conjecture, and that the same can be said about either halves (i.e. inclusion in one fixed direction between the algebraic and analytic sides). The known inclusion of the Greenberg-type main conjecture (including the algebraic objects in the analytic object) then yields an inclusion in the statement of the ♯/♭-♯/♭ main conjecture which implies the main theorem.

We first recall in subsection 3.1 the statement of the main conjecture from [64]. In subsection 3.2, 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 3.3 is a short exposition on the Greenberg-type main conjecture, and one inclusion of it [11, Theorem 8.2.1]. In subsection 3.4, we construct ♯/♭-Beilinson-Flach elements. These are modified versions of the Beilinson-Flach elements due to Kings, Loeffler, and Zerbes [30]. 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 ♯/♭-Beilinson-Flach element main conjecture.

3.1. Statement of the cyclotomic ♯/♭ main conjecture

We now recall the main conjecture of [64] (cf. [32] for the case $a_p = 0$).

The analytic side.

We denote by ζ_{p^n} a primitive p^nth root of unity, γ a topological generator of $1+2p\mathbb{Z}_p$ (or its image in a quotient), by α and β the roots of the Hecke polynomial $Y^2 - a_p Y + p$, and by Ω_E^+ the real Néron period of E.

Theorem 3.1. *(Amice and Vélu [1], Višik [70]) Let χ be a character of $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ into μ_{p^∞} sending γ to ζ_{p^n} that is trivial on the tame part, and let $\tau(\chi)$ be the Gauß sum $\sum_{a\in(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times} \chi(a)\zeta_{p^{n+1}}^a$. There are p-adic power series $L_\alpha(X)$ and $L_\beta(X)$ converging on the open unit disk so that for $\xi \in \{\alpha, \beta\}$,*

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

$$L_\xi(0) = \left(1 - \frac{1}{\xi}\right)^2 \frac{L(E,1)}{\Omega_E^+}.$$

These power series live in a subset $\mathcal{H}_{\frac{1}{2}}$ of $\mathbb{C}_p[[X]]$. This subring is defined by growth properties.

Definition 3.2. Fix $0 < r < 1$. For $f(X) \in \mathbb{C}_p[[X]]$ convergent on the open unit disc of $\mathbb{C}_p$ with normalization $|p|_p = \frac{1}{p}$, let

$$|f(X)|_r := \sup_{|z|_p < r} |f(z)|_p.$$

Definition 3.3. 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 $f(X) \sim g(X)$.

Elements in $\mathcal{H}_{\frac{1}{2}}$ are the analytic functions converging on the open unit disk and are uniquely determined under the condition that they are $O(\log_p(1+X)^{\frac{1}{2}})$, i.e. $\mathcal{H}_{\frac{1}{2}}$ is the set of $\frac{1}{2}$-admissible measures, cf. [52, 1.1.1] and [50, p. 528]. We denote by $\Phi_{p^n}(Y)$ the p^nth cyclotomic polynomial $\sum_{i=0}^{p-1} Y^{p^{n-1}i}$. We let

$$C_n(X) := \begin{pmatrix} a_p & 1 \\ -\Phi_{p^n}(1+X) & 0 \end{pmatrix},$$

and put

$$\mathcal{L}og(X) := \lim_{n\to\infty} C_1(X)C_2(X)\cdots C_n(X) \begin{pmatrix} a_p & 1 \\ -p & 0 \end{pmatrix}^{-(n+2)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}.$$

Theorem 3.4. *([50] when $a_p = 0$, [66] for general $p \mid a_p$)*
There is a vector of p-adic L-functions $(L^\sharp(X), L^\flat(X)) \in \mathbb{Z}_p[[X]]^{\oplus 2}$ so that $(L_\alpha(X), L_\beta(X)) := (L^\sharp(X), L^\flat(X))\mathcal{L}og(X)$. 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. $(L^\sharp(X), L^\flat(X)) = (\mathrm{Col}_p^\sharp(\mathbf{z}), \mathrm{Col}_p^\flat(\mathbf{z}))$, where

$$\mathbf{z} = (z_n^+)_n \in \mathbf{H}^1_{\mathrm{Iw}}(T) := \varprojlim H^1(\mathbb{Q}_{p,n}, T)$$

is Kato's zeta element [25, Theorem 12.5]. Here, T is the p-adic Tate module of E. The Coleman maps $\mathrm{Col}_p^\sharp$ and $\mathrm{Col}_p^\flat$ are maps from $\mathbf{H}^1_{\mathrm{Iw}}(T)$ to $\mathbb{Z}_p[[X]]$ constructed in [64, Section 5] and will be defined more generally in subsection 3.2, with respect to any of the primes $\mathfrak{p}$ or $\mathfrak{q}$ above p.

The algebraic side. The algebraic object in the main conjecture is any of two modified ('chromatic') Selmer groups. They generalize the constructions of the signed Selmer groups of Kobayashi (whose definition needed $a_p = 0$.) Let $\star \in \{\sharp, \flat\}$. Denote by $\mathbb{Q}_\infty$ (resp. $\mathbb{Q}_{p,\infty}$) the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ (resp. $\mathbb{Q}_p$). We put

$$\mathrm{Sel}^\star(E/\mathbb{Q}_\infty) := \ker\left(\mathrm{Sel}(E/\mathbb{Q}_\infty) \to \frac{E(\mathbb{Q}_{p,\infty}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^\star}\right),$$

where $E^\star$ is the exact annihilator of $\ker \mathrm{Col}_p^\star$ under the local Tate pairing

$$\varprojlim_n H^1(\mathbb{Q}_{p,n}, T) \times \varinjlim_n H^1(\mathbb{Q}_{p,n}, V/T) \to \mathbb{Q}_p/\mathbb{Z}_p,$$

where $V = \mathbb{Q}_p \otimes T$ and $\mathbb{Q}_{p,n}$ the nth layer in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$.

We let $\mathcal{X}^\star(E/\mathbb{Q}_\infty) := \mathrm{Hom}(\mathrm{Sel}^\star(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$, i.e. the Pontryagin dual of $\mathrm{Sel}^\star(E/\mathbb{Q}_\infty)$.

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

Conjecture 3.5. *([32], [64, Main Conjecture 7.21]) Choose $\star \in \{\sharp, \flat\}$ so that $L^\star(X) \neq 0$. Then we have an equality of $\mathbb{Z}_p[[X]]$-ideals*

$$\mathrm{Char}(\mathcal{X}^\star(E/\mathbb{Q}_\infty)) = (L^\star(X)).$$

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

Theorem 3.6. *([64, Theorem 7.16]) Choose $\star \in \{\sharp, \flat\}$ so that $L^\star(X) \neq 0$. Then for some integer $n \geqslant 0$, we have*

$$\mathrm{Char}(\mathcal{X}^\star(E/\mathbb{Q}_\infty)) \supseteq (p^n L^\star(X)).$$

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

3.2. The $\sharp/\flat$-$\sharp/\flat$ main conjectures for imaginary quadratic fields

In this subsection, we recall the analytic theory of Antonio Lei (which generalizes that of Haran/Loeffler ([20, Theorem 2] and [42, 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. We denote by K a quadratic imaginary field and for the rest of the article, we assume p splits as $\mathfrak{pq}$ with $\mathfrak{p} \neq \mathfrak{q}$. We denote by K_∞ the $\mathbb{Z}_p^2$-extension of K. We let $K(\mathfrak{p}^\infty)$ and $K(\mathfrak{q}^\infty)$ be the $\mathfrak{p}^\infty$ ray class field; the $\mathfrak{q}^\infty$ ray class field, and let Λ_K equal to $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \cong \mathbb{Z}_p[[X, Y]]$. We identify $1 + X$ with a generator of $\mathrm{Gal}(K(\mathfrak{p}^\infty) \cap K_\infty/K)$ and $1 + Y$ with one for $\mathrm{Gal}(K(\mathfrak{q}^\infty \cap K_\infty)/K)$.

The analytic side.

Definition 3.7. We denote by $D_K^{x,y}$ the distributions of $\mathbb{Z}_p^2 \simeq \mathrm{Gal}(K_\infty/K)$ 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 $\mathcal{O}(\log^x)$ in the variable X and $\mathcal{O}(\log^y)$ in the variable Y. Equivalently, $D_K^{x,y}$ is the completed tensor product of the one-variable power series with their respective growth conditions. (See Definition 3.3 for the definition of growth, and also [35, Discussion before Lemma 2.1].)

We use the same symbol for the local distributions, i.e. for those on the $\mathbb{Z}_p^2$-extensions of $K_\mathfrak{p}$ and $K_\mathfrak{q}$, which Wan in [74] denotes by $\mathcal{H}^{x,y}$.

Let $\xi, \eta \in \{\alpha, \beta\}$, and denote by $L_{\xi,\eta}(X,Y) \in D_K^{\frac{1}{2},\frac{1}{2}}$ the p-adic L-functions of Haran [20] and Loeffler [42], normalized so that they interpolate the special values

$$\left(\frac{1}{\xi}\right)^{\mathrm{ord}_{\mathfrak{p}}\,\mathfrak{f}_\chi}\left(\frac{1}{\eta}\right)^{\mathrm{ord}_{\mathfrak{q}}\,\mathfrak{f}_\chi}\frac{L(E,\chi,1)}{\tau(\chi)|\mathfrak{f}_\chi|\Omega_E^+\Omega_E^-}$$

at a character χ of $\mathrm{Gal}(K_\infty/K)$, where the conductor $\mathfrak{f}_\chi$ is of the form $\mathfrak{p}^n\mathfrak{q}^{n'}$ for $n, n' \geqslant 1$ and Ω_E^- is the imaginary period of E.

Theorem 3.8 *(Lei, [35]). There exist $L^{\sharp\sharp}, L^{\sharp\flat}, L^{\flat\sharp}, L^{\flat\flat} \in \Lambda_K \otimes \mathbb{Q}$ so that*

$$\begin{pmatrix} L_{\alpha,\alpha} & L_{\beta,\alpha} \\ L_{\alpha,\beta} & L_{\beta,\beta} \end{pmatrix} = \mathcal{L}og(Y)^T \begin{pmatrix} L^{\sharp\sharp} & L^{\flat\sharp} \\ L^{\sharp\flat} & L^{\flat\flat} \end{pmatrix} \mathcal{L}og(X).$$

Proposition 3.9. *The matrix $\begin{pmatrix} L^{\sharp\sharp} & L^{\flat\sharp} \\ L^{\sharp\flat} & L^{\flat\flat} \end{pmatrix}$ is not zero.*

Proof. This follows from applying a theorem of Rohrlich found in [58, page 1], combined with the above interpolation. □

Proposition 3.10. *The functions $L^{\sharp\sharp}, L^{\sharp\flat}, L^{\flat\sharp}, L^{\flat\flat}$ are in Λ_K.*

Proof. From integrality of the interpolating values [43, page 375], we know that the entries of the matrix N_{ij} all have p-adic valuation $\geqslant 0$, where

$$N_{ij} := \begin{pmatrix} \alpha^{(j+1)} & 0 \\ 0 & \beta^{(j+1)} \end{pmatrix} \begin{pmatrix} L_{\alpha,\alpha} & L_{\beta,\alpha} \\ L_{\alpha,\beta} & L_{\beta,\beta} \end{pmatrix}\Big|_{X=\zeta_{p^i}-1, Y=\zeta_{p^j}-1} \begin{pmatrix} \alpha^{(i+1)} & 0 \\ 0 & \beta^{(i+1)} \end{pmatrix}.$$

We would like to prove that if any of the our chromatic functions were not in Λ_K, then some entry of N_{ij} would have p-adic valuation < 0 for some i, j, deriving a contradiction. To analyze the p-adic valuations of the entries, we recall just enough of the discussion of [65, Section 4.1 on Valuation Matrices]:

Given a matrix M with entries in $\mathbb{C}_p$, denote by $[M]$ it valuation matrix, i.e. the matrix consisting of the p-adic valuation of the entries of M, as first defined in [65, Definition 4.4] (see also [66, Definition 4.9]).

Denote a matrix M with entries in $\mathbb{C}_p[[s]]$ evaluated at $s = \zeta_{p^i} - 1$ by $M^{(i)}$.

We have that

$$\begin{aligned} \mathcal{L}og_i &= C_1^{(i)} \cdots C_i^{(i)} \begin{pmatrix} a_p & -1 \\ p & 0 \end{pmatrix}^{-(i+2)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix} \\ &= C_1^{(i)} \cdots C_{i-1}^{(i)} \begin{pmatrix} -1 & -1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha^{-(i+1)} & 0 \\ 0 & \beta^{-(i+1)} \end{pmatrix}. \end{aligned} \tag{1}$$

By Theorem 3.8, we thus have that

$$[N_{ij}] = \left[\left(C_1^{(j)} \cdots C_{j-1}^{(j)} \begin{pmatrix} -1 & -1 \\ 0 & 0 \end{pmatrix} \right)^T \begin{pmatrix} L^{\sharp\sharp} & L^{\flat\sharp} \\ L^{\sharp\flat} & L^{\flat\flat} \end{pmatrix}\Big|_{X=\zeta_{p^i}-1, Y=\zeta_{p^j}-1} C_1^{(i)} \cdots C_{i-1}^{(i)} \begin{pmatrix} -1 & -1 \\ 0 & 0 \end{pmatrix} \right].$$

The valuation matrix of $C_1^{(i)} \cdots C_{i-1}^{(i)} \left(\begin{smallmatrix} -1 & -1 \\ 0 & 0 \end{smallmatrix}\right)$ is of the form $\left(\begin{smallmatrix} e_i & e_i \\ f_i & f_i \end{smallmatrix}\right)$, where

- for odd i, we have $e_i < \frac{1}{p} + \frac{1}{p^2} < \frac{1}{2} < f_i$ and
- for even i, we have $f_i < \frac{1}{p} + \frac{1}{p^2} < \frac{1}{2} < e_i$,

see [65, Lemma 4.5].[10]

Recall that we want to derive a contradiction, assuming that at least one of the four chromatic functions is not in Λ_K. We define a μ-invariant: For $\{\bullet, \circ\} \in \{\sharp, \flat\}$, write $L^{\bullet\circ} = \sum_{i,j} a_{i,j}^{\bullet\circ} X^i Y^j$ with $a_{i,j} \in \mathbb{Z}_p$ and define

$$\mu^{\bullet\circ}(E, K) := \min_{i,j} \operatorname{ord}_p(a_{i,j}^{\bullet\circ}). \tag{2}$$

We also define

$$\mu(E, K) := \min_{\bullet,\circ \in \{\sharp,\flat\}} \mu^{\bullet\circ}(E, K). \tag{3}$$

Our task is now to show that $\mu(E, K) \geqslant 0$.

Assume on the contrary that $\mu(E, K) \leqslant -1$ – without loss of generality, assume that we have

$$\mu(E, K) = \mu^{\sharp\flat}(E, K) < 0.$$

Evaluating $L^{\sharp\flat}$ at $X = \zeta_{p^i} - 1$ and $Y = \zeta_{p^j} - 1$, we then have for all but possibly finitely many i, j that $\operatorname{ord}_p(L^{\sharp\flat}(\zeta_{p^i} - 1, \zeta_{p^j} - 1)) = \mu(E, K) + \frac{1}{p^{i-1}(p-1)} + \frac{1}{p^{j-1}(p-1)}$. Among those i and j, we have infinitely many choices for which $i > 3$ is odd and $j > 3$ even. For any such i and j, the entry in the first column and second row[11] of N_{ij} then has valuation

$$\mu(E, K) + \frac{1}{p^{i-1}(p-1)} + \frac{1}{p^{j-1}(p-1)} + e_i + f_j$$

by minimality of $\mu^{\sharp\flat}(E, K)$ and the fact that $e_j - f_j > \frac{1}{2} - \left(\frac{1}{p} + \frac{1}{p^2}\right)$ and the same estimate for $f_i - e_i$. But

$$e_i + f_j < \frac{2}{p} + \frac{2}{p^2} \leqslant 1 - \frac{1}{p^2(p-1)} - \frac{1}{p^2(p-1)} \leqslant 1 - \frac{1}{p^{i-1}(p-1)} - \frac{1}{p^{j-1}(p-1)}.$$

Thus, this would imply that the entry of N_{ij} in question has negative p-adic valuation, QEA. □

[10] The exact values, which [65, Lemma 4.5] gives, do not matter in our proof.

[11] i.e. the same position as $L^{\sharp\flat}$.

Given a quadratic imaginary field K, we denote by $L_K^\sharp$ and $L_K^\flat$ the p-adic L-functions corresponding to the elliptic curve $E^{(K)}$ which is the quadratic twist of E by the character corresponding to K.

Lemma 3.11. *For at least one $\bullet \in \{\sharp, \flat\}$, there is a quadratic imaginary field K so that both one-variable p-adic L-functions $L^\bullet$ and $L_K^\bullet$ are non-zero.*

Proof. From [64, Proposition 6.14], we see that for a choice $\bullet \in \{\sharp, \flat\}$, the one-variable p-adic L-function $L^\bullet$ is non-zero. To pick K so that $L_K^\bullet$ is also not zero, we pick K so that $E^{(K)}$ has analytic rank zero, and use [64, Table before Proposition 6.14]. This is possible in view of [4, Theorem ii], where the set denoted S of split primes consists of p, or [13] (for a direct proof using multiple Dirichlet series), see also [72,71] and [49,23]. Alternatively, use the fact that a positive proportion of elliptic curves has rank 0 [8] even when restricting to congruence conditions, combined with a positive proportion satisfying the Birch and Swinnerton-Dyer conjecture [9]. □

Choice 3.12. *Following Lemma 3.11, we choose $\bullet \in \{\sharp, \flat\}$ and K so that both $L^\bullet$ and $L_K^\bullet$ are non-zero.*

The algebraic side.

Given an unramified extension k of $\mathbb{Q}_p$ we denote by O_k its ring of integers. We denote by $k_{0,m}$ the degree p^m unramified extension of $\mathbb{Q}_p$, k_n the $\mathbb{Z}/p^n\mathbb{Z}$-subextension of $k(\zeta_{p^{n+1}})$, and by $\mathfrak{m}_n$ the maximal ideal in its integer ring. We let $k_{n,m}$ and $\mathfrak{m}_{n,m}$ be the objects above with $k = k_{0,m}$. Finally, we let $\Lambda_{n,m}$ be equal to $\mathbb{Z}_p[\mathrm{Gal}(k_{n,m}/\mathbb{Q}_p)]$.

Lemma 3.13. *Let $n, m \geqslant 0$. The $\Lambda_{n,m}$-modules $\widehat{E}(\mathfrak{m}_{n,m})$ are each generated by two elements $c_{n,m} \in \widehat{E}(\mathfrak{m}_{n,m})$ and $c_{n-1,m} \in \widehat{E}(\mathfrak{m}_{n-1,m}) \subset \widehat{E}(\mathfrak{m}_{n,m})$ (where we let $(\mathfrak{m}_{-1,m}) := (\mathfrak{m}_{0,m})$), and which satisfy for $n > 0$ and $m \geqslant 0$*

$$\mathrm{tr}_{k_{n,m+1}/k_{n,m}} c_{n,m+1} = c_{n,m}, \text{ and}$$
$$\mathrm{tr}_{k_{n,m}/k_{n-1,m}} c_{n,m} = a_p c_{n-1,m} - c_{n-2,m}.$$

This lemma generalizes [74, Lemma 2.2] and the constructions in [27, Proposition 3.12], both of which treat the $a_p = 0$ case. Its proof needs the following definitions.

Given $u \in \mathcal{O}_{k_{0,m}}^\times$, put $f_u(X) := (u + X)^p - u^p$. Also, we let

$$(x_k, x_{k-1}) := (1, 0)A^k \times \frac{1}{p^k} \text{for } k \geqslant 0,$$

where $A = \left(\begin{smallmatrix} a_p & p \\ -1 & 0 \end{smallmatrix}\right)$ as in [64, Definition 2.1]. We let φ be the Frobenius on $k_{0,m}$ and let

$$f_u^{(k)} := f_u^{(k)}(X) := f_u^{\varphi^{k-1}} \circ f_u^{\varphi^{k-2}} \circ \cdots \circ f_u,$$

where k is an integer.

The logarithm giving rise to our formal group via Honda theory is the power series

$$\log_{f_u}(X) := \sum_{k \geqslant 0}^{\infty} x_k f_u^{(k)}(X).$$

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 3.14. We put $\lambda_{n,u} := \sum_{i \geqslant 1}^{\infty} b_i u^{\varphi^{-(n+i+1)}} p^{\lceil \frac{i}{2} \rceil}$ for $n \geqslant 0$.

As in [27, page 54], these elements give rise to points[12] $c_n^u \in \widehat{E}\left(\mathfrak{m}_{k_{0,m}(\zeta_{p^n})}\right)$ for $n \geqslant 0$ so that

$$\begin{aligned} \log_{\widehat{E}}(c_n^u) &= \lambda_{n,u} + \log_{f_u^{\varphi^{-n}}}(u^{\varphi^{-n}} \cdot (\zeta_{p^n} - 1)) \\ &= \lambda_{n,u} + \textstyle\sum_{k \geqslant 0}^{\infty} x_k \pi_{n-k,u} \end{aligned}$$

for trace-compatible uniformizers $\pi_{n-k,u} = \pi_{n-k} u$ in $\mathfrak{m}_{k_{0,m}(\zeta_{p^n})}$, where $\pi_{n-k} = \left(\zeta_{p^{n-k}} - 1\right)$.

We let U be the unramified variable, i.e. $1+U$ is identified with a topological generator of $\varprojlim_m \mathrm{Gal}(k_{0,m}/k)$.

Proof of Lemma 3.13. To make the first trace relation work, choose a $\mathbb{Z}_p[[U]]$-generator $d := \{d_m\}_m \in \varprojlim_m \mathcal{O}_{k_{0,m}}$ as in [74, Proof of Lemma 2.2]. The calculations in the proof of [74, Lemma 2.2] with the d_m expressed as sums of roots of unity then work to produce elements that are trace-compatible in the m-direction, except the coefficients of $\log_{\widehat{E}}$ are appropriately modified (to remove the $a_p = 0$ assumption): If $d_m = \sum_j a_{m,j}\zeta_j$ with $a_{m,j} \in \mathbb{Z}_p$, note that for $n \geqslant 0$

$$\log_{\hat{E}}\left(\sum_j a_{m,j} c_n^{\zeta_j}\right) = \sum_i b_i d_m^{\varphi^{-(n+i+1)}} p^{\lceil \frac{i}{2} \rceil} + \sum_{k<n} x_k (\zeta_{p^{n-k}} - 1) d_m^{\varphi^{k-n}}$$

is trace-compatible with respect to the map $\mathrm{tr}_{k_{0,m}(\zeta_{p^n})/k_{0,m-1}(\zeta_{p^n})}$. We can now argue as in [27, Discussion before Proposition 3.12] and put $\mathrm{tr}_\Delta := \mathrm{tr}_{k_{0,m}(\zeta_{p^n})/k_{n-1,m}}$ to define

$$c_{n-1,m} := \sum_j a_{m,j} \,\mathrm{tr}_\Delta\, c_n^{\zeta_j}$$

[12] For BD Kim's notation, the analogue of $\lambda_{n,u}$ is denoted λ_n and that of c_n^u is denoted b_n. The analogue of $c_{n,m}$ is e_n.

which are trace-compatible in the m-direction.

(Note that [74] calls both $\sum_j a_{m,j} c_n^{\zeta_j}$ and $\sum_j a_{m,j} \operatorname{tr}_\Delta c_n^{\zeta_j}$ by the same symbol, namely $c_{n,m}$, cf. [74, Discussion after Lemma 2.1]. We have opted to follow Kim's convention instead.)

In particular, this gives that

$$c_{-1,m} = [p-1] \sum_j a_{m,j} c_0^{\zeta_j},$$

where we made the convention that $k_{-1,m} = k_{0,m}$.

For the second trace relation, we refer to the calculations in [27, page 54]. To make them work for the case $a_p \neq 0$, note that (denoting $\operatorname{tr}_{k_{0,m}(\zeta_{p^n})/k_{0,m}(\zeta_{p^{n-1}})}$ by tr)

$$\begin{aligned} \operatorname{tr} \log_{\widehat{E}}(c_n^u) = &\quad \operatorname{tr}(\lambda_{n,u} + \pi_{n,u} + \textstyle\sum_{k\geqslant 1}^{\infty} x_k \pi_{n-k,u}) \\ = &\quad p\lambda_{n,u} - u^{\varphi^{-n}} p + \textstyle\sum_{k\geqslant 1}^{\infty} x_k \pi_{n-k,u} \\ = &\quad a_p(\lambda_{n-1,u} + \textstyle\sum_{k\geqslant 1}^{\infty} x_{k-1}\pi_{n-k,u}) - \lambda_{n-2,u} - \textstyle\sum_{k\geqslant 2}^{\infty} x_{k-2}\pi_{n-k,u} \\ = &\quad a_p \log_{\widehat{E}}(c_{n-1}^u) - \log_{\widehat{E}}(c_{n-2}^u). \end{aligned}$$

Finally, the fact that $c_{n,m}$ and $c_{n-1,m}$ generate $\widehat{E}(\mathfrak{m}_{n,m})$ as a $\Lambda_{n,m}$-module follows from combining [64, Theorem 2.2] with [27, Discussion after 3.12] and [28, Proof of Proposition 2.6]. □

Definition 3.15. We define a pairing $P_{(n,m),x} : H^1(k_{n,m}, T) \to \Lambda_{n,m}$ by

$$z \mapsto \sum_{\sigma \in \operatorname{Gal}(k_{n,m}/\mathbb{Q}_p)} (x^\sigma, z)_{n,m} \sigma \text{ for } x \in \hat{E}(\mathfrak{m}_{n,m}), \text{ where}$$

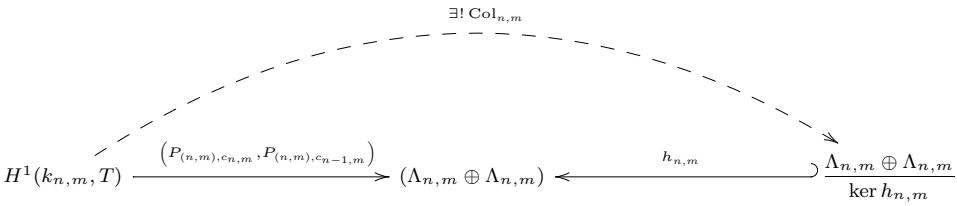
$(\quad,\quad)_{n,m} : \hat{E}(\mathfrak{m}_{n,m}) \times H^1(k_n, T) \to H^2(k_{n,m}, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p$ is the pairing coming from the cup product.

Definition 3.16. Put $\mathcal{H}_n(X) := -C_1(X)C_2(X)\cdots C_{n-1}(X) \begin{pmatrix} 1 & 0 \\ 0 & \Phi_{p^n}(1+X) \end{pmatrix}$ and define the endomorphism $h_{n,m}$ by

$$\begin{array}{ccccc} \Lambda_{n,m} \oplus \Lambda_{n,m} & \xrightarrow{h_{n,m}} & \Lambda_{n,m} \oplus \Lambda_{n,m}\mathcal{H}_n & \subset & \Lambda_{n,m} \oplus \Lambda_{n,m} \\ (a,b) & \mapsto & (a,b)\mathcal{H}_n. & & \end{array}$$

Remark 3.17. The minus sign ensures that our conventions agree with the original ones of Kobayashi, see e.g. [64, Definition 3.8].

Proposition 3.18. *There exists a unique* Λ*-linear map* $\operatorname{Col}_{n,m}$ *so that the following commutes:*



Proof. [64, Proposition 5.3] proves this in the case in which $k_{0,m}=\mathbb{Q}_p$, relying on the arguments from [64, Section 3]. These arguments work for our purposes since the pairing $P_{(n,m),x}$ is available in the $k_{0,m}$ case as well. □

Lemma 3.19. *The Coleman maps are compatible in the unramified direction, i.e. the following diagram commutes:*

$$\begin{array}{ccc} H^1(k_{n,m+1},T) & \xrightarrow{\mathrm{Col}_{n,m+1}} & \dfrac{\Lambda_{n,m+1}\oplus\Lambda_{n,m+1}}{\ker h_{n,m+1}} \\ \Big\downarrow{\scriptstyle \mathrm{cor}} & \circlearrowleft & \Big\downarrow{\scriptstyle \mathrm{proj}} \\ H^1(k_{n,m},T) & \xrightarrow{\mathrm{Col}_{n,m}} & \frac{\Lambda_{n,m}\oplus\Lambda_{n,m}}{\ker h_{n,m}} \end{array}$$

Proof. This follows from the first trace-compatibility stated in Lemma 3.13. □

Proposition 3.20. *The Coleman maps are compatible in the totally ramified direction, i.e. the following diagram also commutes:*

$$\begin{array}{ccc} H^1(k_{n+1,m},T) & \xrightarrow{\mathrm{Col}_{n+1,m}} & \dfrac{\Lambda_{n+1,m}\oplus\Lambda_{n+1,m}}{\ker h_{n+1,m}} \\ \Big\downarrow{\scriptstyle \mathrm{cor}} & \circlearrowleft & \Big\downarrow{\scriptstyle \mathrm{proj}} \\ H^1(k_{n,m},T) & \xrightarrow{\mathrm{Col}_{n,m}} & \dfrac{\Lambda_{n,m}\oplus\Lambda_{n,m}}{\ker h_{n,m}} \end{array}$$

Proof. This is [64, Corollary 5.6] in the case $k_{0,m}=\mathbb{Q}_p$. We note that the arguments for this corollary apply in the $k_{0,m}$ case as well. □

We denote by Λ the Iwasawa algebra $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$.

Lemma 3.21. *We have* $\varprojlim_m \varprojlim_n \frac{\Lambda_{n,m}\oplus\Lambda_{n,m}}{\ker h_{n,m}} \cong \Lambda\oplus\Lambda$.

Proof. The arguments in [64, Proposition 5.7] show that $\varprojlim_n \frac{\Lambda_{n,m}\oplus\Lambda_{n,m}}{\ker h_{n,m}} \cong \Lambda\oplus\Lambda$. This is enough since $\mathrm{Gal}(k_{n,m}/k_{0,m})\cong\mathrm{Gal}(\mathbb{Q}_{p,n}/\mathbb{Q}_p)$. □

Definition 3.22. We define the pair of Coleman maps as

$$(\mathrm{Col}^\sharp, \mathrm{Col}^\flat) := \varprojlim_n \varprojlim_m \mathrm{Col}_{n,m} : \varprojlim_n \varprojlim_m H^1(k_{n,m}, T) \to \Lambda \oplus \Lambda.$$

Definition 3.23. Let $\star \in \{\sharp, \flat\}$. We denote by $E^\star$ the exact annihilator of $\ker \mathrm{Col}^\star$ under the Tate pairing

$$\varprojlim_n \varprojlim_m H^1(k_{n,m}, T) \times \varinjlim_n \varinjlim_m H^1(k_{n,m}, V/T) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

We denote by $k_{n,m}(\mathfrak{p})$ (resp. $k_{n,m}(\mathfrak{q})$) the local field isomorphic to $k_{n,m}$ with initial layer $k_{0,0}$ obtained by completing K at $\mathfrak{p}$ (resp. $\mathfrak{q}$) and climbing up to the appropriate layer of the cyclotomic extension and the unramified tower.

Definition 3.24. We now define the four Selmer groups $\mathrm{Sel}^{\sharp\sharp}(E/K_\infty)$, $\mathrm{Sel}^{\sharp\flat}(E/K_\infty)$, $\mathrm{Sel}^{\flat\sharp}(E/K_\infty)$, and $\mathrm{Sel}^{\flat\flat}(E/K_\infty)$. For $\star, \circ \in \{\sharp, \flat\}$, put $\mathrm{Sel}^{\star\circ}(E/K_\infty) :=$

$$\ker\left(\mathrm{Sel}(E/K_\infty) \to \bigoplus_{v|\mathfrak{p}} \frac{\varinjlim_{m,n} H^1(k_{n,m}(\mathfrak{p}), V/T)}{E^\star} \oplus \bigoplus_{v|\mathfrak{q}} \frac{\varinjlim_{m,n} H^1(k_{n,m}(\mathfrak{q}), V/T)}{E^\circ}\right).$$

To handle all of the places $v|p$ in K_∞ as in the direct sum above, we make the convention that the map Col stands for a direct sum of Coleman maps of the primes above $\mathfrak{p}$ or $\mathfrak{q}$, e.g. for the prime $\mathfrak{p}$, we make the following definition:

Definition 3.25. Let $\{\gamma_v\}_{v|\mathfrak{p}}$ be representatives of the p-group $\mathrm{Gal}(K_\infty/K)/D_p$, where D_p is the decomposition group at $\mathfrak{p}$. For $\star \in \{\sharp, \flat\}$, we put $\mathrm{Col}^\star_{\mathfrak{p}}(x) := \sum_{v|\mathfrak{p}} \mathrm{Col}^\star(x_v) \cdot \gamma_v$, where x_v is the v-local component of x via the isomorphism

$$H^1(K_{\mathfrak{p}}, T \otimes \Lambda_K) \cong \bigoplus_{v|\mathfrak{p}} H^1(K_{\mathfrak{p}}, T \otimes \mathbb{Z}_p[[D_p]])\gamma_v.$$

Definition 3.26. Given $\star, \circ \in \{\sharp, \flat\}$, put $\mathcal{X}^{\star\circ} := \mathrm{Hom}(\mathrm{Sel}^{\star\circ}(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$.

The main conjecture.

Conjecture 3.27. *For $\star, \circ \in \{\sharp, \flat\}$ so that $L^{\star\circ}(X, Y) \neq 0$, $\mathcal{X}^{\star\circ}$ is Λ_K-torsion and we have the equality of Λ_K-ideals*

$$\mathrm{Char}(\mathcal{X}^{\star\circ}) = (L^{\star\circ}(X, Y)).$$

3.3. A Greenberg-type main conjecture

The analytic side. From [15], it follows that there is a p-adic L-function in $\mathrm{Frac}\,\Lambda_K$ interpolating p-adic avatars of Hecke characters associated to K, cf. [11, (1.0.3)]. We

denote it by $L_p^{\forall 0}$ to reflect the corresponding conditions on the algebraic side at $\mathfrak{p}$ and $\mathfrak{q}$. (In [74, discussion before Theorem 2.15], this is denoted by $L'_{f,K}$.)

The algebraic side. The algebraic object is the following "coarse at $\mathfrak{p}$ but fine at $\mathfrak{q}$" Selmer group. Here, I_v is the inertia group at the place v. We let $\mathcal{W} := T \otimes \Lambda_K^*(\Psi)$, where Λ_K^* is the Pontryagin dual of Λ_K, Ψ the character $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K_\infty/K) \to \Lambda_K^\times$, and $\Lambda_K^*(\Psi)$ is Λ_K^* twisted by Ψ.

Definition 3.28.

$$\mathrm{Sel}_p^{\forall 0}(K, \mathcal{W}) := \ker\left(H^1(K, \mathcal{W}) \to \prod_{v \nmid p} H^1(I_v, \mathcal{W}) \times H^1(K_\mathfrak{q}, \mathcal{W}) \right).$$

We then put $\mathcal{X}^{\forall 0} := \mathrm{Hom}(\mathrm{Sel}_p^{\forall 0}, \mathbb{Q}_p/\mathbb{Z}_p)$.

The reason we work with $\mathcal{W}$, a deformation of V/T (which is often denoted by W) is for that it allows for more convenient local conditions because of the absence of an inverse limit, cf. e.g. [18, Proposition 3.2].

The Greenberg-type main conjecture. The Greenberg-type main conjecture is full equality in the following theorem.

Theorem 3.29. *[11, Theorem 8.2.1][74, Theorem 2.15] Let E have square-free conductor N that has at least one prime divisor $l|N$ not split in K, and suppose that $E[p]|_{G_K}$ is absolutely irreducible. Then as $\Lambda_K \otimes \mathbb{Q}_p$-ideals of* $\mathrm{Frac}\,\Lambda_K$*, we have*

$$(a)\,\mathrm{Char}(\mathcal{X}^{\forall 0}) \subseteq (L_p^{\forall 0}),$$

for some $a \in \Lambda_K$ satisfying $(a) = \prod \mathfrak{P}_i$, where the prime ideals $\mathfrak{P}_i$ of Λ_K are all pullbacks of height one primes of $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K_{anti})]]$.

3.4. The ♯/♭-Beilinson-Flach main conjectures

The analytic side.

Convention 3.30. *Given a column vector of functions $\begin{pmatrix} f_1 \\ f_2 \end{pmatrix}$ and a row vector of elements (x_1, x_2), we denote by $\begin{pmatrix} f_1 \\ f_2 \end{pmatrix} \circ (x_1, x_2)$ the matrix $\begin{pmatrix} f_1(x_1) & f_1(x_2) \\ f_2(x_1) & f_2(x_2) \end{pmatrix}$.*

We now construct integral cohomology classes $\Delta_\sharp, \Delta_\flat$ assuming the existence of certain Beilinson–Flach classes $\Delta_\alpha, \Delta_\beta$ which should compare favorably to those due to Lei, Loeffler, and Zerbes, constructed from the p-stabilizations f_α and f_β of the normalized weight two eigenform f (see [38, 6.4.4] and [40, Thm A]).

We now let $\mathcal{T} := T \otimes \Lambda_K(-\Psi)$. The images of the Néron differential in the α- and β-eigenspaces in $D_{\mathrm{cris}}(V)$ of the action of Frobenius φ give us a basis with respect to

which we can consider projections π_α and π_β. Here, $D_{\mathrm{cris}}(V)$ is the filtered φ-module associated to V by the theory of Fontaine, see e.g. [3, Section 2.1] and [16, 2.3]. Now let $\mathcal{L}_\alpha := \pi_\alpha \circ \mathcal{L}$, where $\mathcal{L}$ is as in [41, Theorem 4.7], but where we abuse notation as in Definition 3.25, i.e. we let the symbol $\mathcal{L}$ (and consequently $\mathcal{L}_\alpha$) stand for its direct sum along v-components. Also, we put $(\Delta_\alpha)_{\mathfrak{q}} := \mathrm{loc}_{\mathfrak{q}}(\Delta_\alpha)$, and define $\mathcal{L}_\beta$ and $(\Delta_\beta)_{\mathfrak{q}}$ similarly.

Below, we let $\Gamma_{n,\mathfrak{p}}$ be the Galois group of the cyclotomic $\mathbb{Z}/p^n\mathbb{Z}$-extension of $K_{\mathfrak{p}}$, $U_{m,\mathfrak{p}}$ be the Galois group of the unramified $\mathbb{Z}/p^m\mathbb{Z}$-extension of $K_{\mathfrak{p}}$, and we denote by γ a topological generator of $\varprojlim_n \Gamma_{n,\mathfrak{p}}$, and by u a topological generator of $\Upsilon := \varprojlim_m U_{m,\mathfrak{p}}$.

Convention 3.31. *For φ a finite order character so that $\varphi(\gamma)$ and $\varphi(u)$ are primitive p^nth and p^mth roots of unity, we put*

$$\tilde{\varphi}(\_) := \sum_{\sigma \in \Gamma_{n,\mathfrak{p}} \times U_{m,\mathfrak{p}}} \log(\_)^\sigma \varphi(\sigma),$$

where log *is the formal group logarithm. If $\tilde{\varphi}$ is defined on components of a vector (x, y), we denote $(\tilde{\varphi}(x), \tilde{\varphi}(y))$ simply by $\tilde{\varphi}(x, y)$.*

Definition 3.32. Letting $\Lambda' := \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K_{cyc})]]$, we define:

$\mathcal{R} := \{x \in \mathrm{Frac}\,\Lambda' : \mathrm{ord}_{\mathfrak{P}}(x) \leqslant 0$ for any height one prime $\mathfrak{P} \neq (p)$ of Λ_K so that $\mathfrak{P}$ is not the pullback to Λ_K of the augmentation ideal of $\Lambda'\}$.

Conjecture 3.33. *There are elements $\Delta_\alpha, \Delta_\beta \in H^1(K, \mathcal{T}) \otimes D_K^{\frac{1}{2},0}$ so that:*

(*exp$_{\mathfrak{q}}$) *the images under*

$$\mathcal{L}_\alpha, \mathcal{L}_\beta : \frac{1}{\nu} H^1(K_{\mathfrak{q}}, \mathcal{T}) \otimes D_K^{\frac{1}{2},0} \to D_K^{\frac{1}{2},\frac{1}{2}} \text{ satisfy}$$

$$\begin{pmatrix} \mathcal{L}_\alpha \\ \mathcal{L}_\beta \end{pmatrix} \circ ((\Delta_\alpha)_{\mathfrak{q}}, (\Delta_\beta)_{\mathfrak{q}}) = \begin{pmatrix} L_{\alpha\alpha} & L_{\beta\alpha} \\ L_{\alpha\beta} & L_{\beta\beta} \end{pmatrix}.$$

(*exp$_{\mathfrak{p}}$) *The $\mathfrak{p}$-local images are geometric, i.e. we have*

$$\begin{pmatrix} \mathcal{L}_\alpha \\ \mathcal{L}_\beta \end{pmatrix} \circ ((\Delta_\alpha)_{\mathfrak{p}}, (\Delta_\beta)_{\mathfrak{p}}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(*log$_{\mathfrak{p}}$) *For a finite-order character φ of $\mathrm{Gal}(K_\infty/K)$ of conductor p^n at $\mathfrak{p}$, we have*

$$\tilde{\varphi}((\Delta_\alpha)_{\mathfrak{p}}, (\Delta_\beta)_{\mathfrak{p}}) = \left(\alpha^{-n}, \beta^{-n}\right) \times \varphi(L_p^{\forall 0} H) \times \tau(\varphi|_{\Gamma_{n,\mathfrak{p}}}),$$

where $\tau(\varphi|_{\Gamma_{n,\mathfrak{p}}})$ is the Gaußsum and $H \in \mathcal{R}$.

Remark 3.34.

(i) In ($^*\exp_{\mathfrak{q}}$), the image is in $D_K^{\frac{1}{2},\frac{1}{2}}$ by [41, Proposition 4.9].
(ii) The reason for the name ($^*\log_{\mathfrak{p}}$) is that we expect there to be a logarithm map $\log_{\mathfrak{p}}$ so that we have the (stronger) reciprocity law

$$\left(\log_{\mathfrak{p}}(\Delta_\alpha)_{\mathfrak{p}}, \log_{\mathfrak{p}}(\Delta_\beta)_{\mathfrak{p}}\right) = (L_p^{\forall 0}, L_p^{\forall 0}).$$

(iii) In the ($^*\log_{\mathfrak{p}}$) part of the conjecture, we allowed an error coefficient $H \in \Lambda'$. We expect this Λ' to be the coefficient ring of a suitable Hida family.[13]

Remark 3.35. A related reciprocity law of Loeffler and Zerbes [40, Theorem B, 7.1.5] states that there are appropriate classes Δ_α^{LZ} and Δ_β^{LZ} which can be related in (Coleman) families to Urban's 3-variable p-adic L-function constructed in [68].

We let S be a finite set of places containing p, ∞, and the bad primes of E, and L^S be the maximal extension of a number field L that is unramified outside S.

Proposition 3.36. *Assume Conjecture 3.33. Then there exist integral (up to the factor ν) cohomology classes*

$$\Delta_\sharp, \Delta_\flat \in \frac{1}{\nu} H^1\left(K^S, \mathcal{T}\right)$$

so that

$$h \cdot (\Delta_\alpha, \Delta_\beta) = (\Delta_\sharp, \Delta_\flat)\mathcal{L}og(X)$$

for some element $h \in \Lambda_K$.

Before proving this proposition, we make an observation and fix some notation.

Lemma 3.37. *The entries of $\mathcal{L}og(X)$ are $O(\log_p(1+X)^{\frac{1}{2}})$.*

Proof. [66, Proposition 4.20 (Growth Lemma)]. □

Lemma 3.38. *The Λ_K-module $H^1(K_{\mathfrak{q}}, \mathcal{T})$ is free of rank two.*

Proof. This follows from [74, Lemma 2.7], which proves that $\varprojlim_n \varprojlim_m H^1(k_{n,m}, T)$ is a free $\mathbb{Z}_p[[\Gamma_p]]$-module, combined with the isomorphism from Definition 3.25.[14] □

[13] in view of [73], which scrutinizes [21] and [26].
[14] We briefly sketch the proof of [74, Lemma 2.7]. Since T/pT is irreducible, $H^1(k_{n,m}, T)$ surjects onto $H^1(k_{n-1,m-1}, T)$, so that the assertion follows from $H^1(k_{n,m}, T)$ being a free $\Lambda_{n,m}$-module. To prove this assertion, one employes an Euler characteristic formula to prove that $H^1(\mathbb{Q}_p, T/pT)$ is a rank two $\mathbb{F}_p$-vector space, and then deforms by replacing T/pT by T/p^nT and $\mathbb{Q}_p$ by $k_{n,m}$ to obtain the result.

Definition 3.39. We now choose a Λ_K-basis (v_1, v_2) of $H^1(K_{\mathfrak{q}}, \mathcal{T})$.

Definition 3.40. Choose $\xi \in \{\alpha, \beta\}$. We fix integral (v_1, v_2)-coordinates of the $\mathfrak{q}$-localized Beilinson–Flach element $(\Delta_\xi)_{\mathfrak{q}} = \mathrm{loc}_{\mathfrak{q}}(\Delta_\xi)$ denoted $\delta_{\xi i}$ (for $i \in \{1, 2\}$) satisfying

$$((\Delta_\alpha)_{\mathfrak{q}}, (\Delta_\beta)_{\mathfrak{q}}) = (v_1, v_2) \begin{pmatrix} \delta_{\alpha 1} & \delta_{\beta 1} \\ \delta_{\alpha 2} & \delta_{\beta 2} \end{pmatrix}, \text{ where}$$

$$\delta_{\xi i} \in D_K^{\frac{1}{2},0}.$$

Proof of Proposition 3.36. We follow the strategy of [74, Lemma 3.8]. From Theorem 3.8 and Proposition 3.10, we know that

$$\mathcal{L}og(Y)^T \begin{pmatrix} L^{\sharp\sharp} & L^{\flat\sharp} \\ L^{\sharp\flat} & L^{\flat\flat} \end{pmatrix} \mathcal{L}og(X) = \begin{pmatrix} L_{\alpha\alpha} & L_{\beta\alpha} \\ L_{\alpha\beta} & L_{\beta\beta} \end{pmatrix} = \begin{pmatrix} \mathcal{L}_\alpha \\ \mathcal{L}_\beta \end{pmatrix} \circ (\Delta_\alpha, \Delta_\beta)_{\mathfrak{q}}$$

$$= \begin{pmatrix} \mathcal{L}_\alpha \\ \mathcal{L}_\beta \end{pmatrix} \circ (v_1, v_2) \begin{pmatrix} \delta_{\alpha 1} & \delta_{\beta 1} \\ \delta_{\alpha 2} & \delta_{\beta 2} \end{pmatrix} = \begin{pmatrix} \mathcal{L}_\alpha(v_1) & \mathcal{L}_\alpha(v_2) \\ \mathcal{L}_\beta(v_1) & \mathcal{L}_\beta(v_2) \end{pmatrix} \begin{pmatrix} \delta_{\alpha 1} & \delta_{\beta 1} \\ \delta_{\alpha 2} & \delta_{\beta 2} \end{pmatrix}.$$

By [41, Proposition 4.9],

$$\begin{pmatrix} \mathcal{L}_\alpha(v_1) & \mathcal{L}_\alpha(v_2) \\ \mathcal{L}_\beta(v_1) & \mathcal{L}_\beta(v_2) \end{pmatrix} \in M_2\left(D_K^{0,\frac{1}{2}}\right),$$

so that we can choose $h \in \Lambda_K$ so that the entries of $h \times \begin{pmatrix} \delta_{\alpha 1} & \delta_{\beta 1} \\ \delta_{\alpha 2} & \delta_{\beta 2} \end{pmatrix} \mathcal{L}og(X)^{ad}$ are multiples of $\log_p(X)$ and elements of $\mathbb{Q}_p \otimes (\Lambda_K)$, where $\mathcal{L}og(X)^{ad}$ denotes the adjugate of $\mathcal{L}og(X)$.

Thus, the coordinates of the Beilinson-Flach elements are divisible by $\mathcal{L}og(X)$ after correcting by h, i.e.

$$h \begin{pmatrix} \delta_{\alpha 1} & \delta_{\beta 1} \\ \delta_{\alpha 2} & \delta_{\beta 2} \end{pmatrix} = \begin{pmatrix} \delta_{\sharp 1} & \delta_{\flat 1} \\ \delta_{\sharp 2} & \delta_{\flat 2} \end{pmatrix} \mathcal{L}og(X)$$

for some $\delta_{*i} \in \Lambda_K \otimes \mathbb{Q}$ for $* \in \{\sharp, \flat\}$ and $i \in \{1, 2\}$. □

Corollary 3.41. *Assume Conjecture 3.33. Then the elements* $(\Delta_\sharp, \Delta_\flat) := h(\Delta_\alpha, \Delta_\beta)\mathcal{L}og(X)^{-1}$ *are well-defined as elements of* $\frac{1}{\nu} H^1\left(K^S, \mathcal{T}\right)$.

Proof. This follows from Proposition 3.36. □

The algebraic side. The objects here are the "$\sharp/\flat$ at $\mathfrak{p}$ but fine at $\mathfrak{q}$" Selmer groups:

Definition 3.42. For $\diamond \in \{\sharp, \flat\}$, put

$$\mathrm{Sel}^{\diamond 0} := \ker\left(H^1(K, \mathcal{W}) \to \prod_{v \nmid p} H^1(I_v, \mathcal{W}) \times \frac{H^1_{\mathfrak{p}}(K_{\mathfrak{p}}, \mathcal{W})}{E^\diamond} \times H^1_{\mathfrak{q}}(K_{\mathfrak{q}}, \mathcal{W}) \right).$$

We then put

$$\mathcal{X}^{\diamond 0} := \mathrm{Hom}(\mathrm{Sel}^{\diamond 0}, \mathbb{Q}_p/\mathbb{Z}_p).$$

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 "dual $\sharp/\flat$ at $\mathfrak{p}$ but coarse at $\mathfrak{q}$" Selmer groups.

Definition 3.43. Let K be so that we can choose $\bullet \in \{\sharp, \flat\}$ as in Choice 3.12. Put

$$\mathcal{X}^{\hat{\bullet}\forall} := \ker\left(H^1\left(K^S, \mathcal{T}\right) \to \prod_{v \nmid p} H^1(I_v, \mathcal{T}) \times \frac{H^1(K_\mathfrak{p}, \mathcal{T})}{\ker(\mathrm{Col}^\bullet_\mathfrak{p})} \right).$$

Proposition 3.44. *Assume Corollary 3.41. Then with the above choice, $\mathcal{X}^{\hat{\bullet}\forall}$ is a free rank one Λ_K-module.*

Proof. For the freeness, we argue as in [22, Lemma 2.2.9]: From [52, beginning of Section 1.3.3], it suffices to see that $E(K_\infty)[p] = 0$. This is proved in [64, Lemma 2.3].

For the rank being one, we first show that the Λ_K-rank of $\mathcal{X}^{\hat{\bullet}\forall}$ is at most one. We know from the construction of Coleman maps that

$$\mathrm{rk}_{\Lambda_K} \frac{H^1(K_\mathfrak{q}, \mathcal{T})}{\ker(\mathrm{Col}^\bullet_\mathfrak{q})} = 1.$$

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

$$\mathcal{N} := \ker\left(\mathcal{X}^{\hat{\bullet}\forall} \to \frac{H^1(K_\mathfrak{q}, \mathcal{T})}{\ker(\mathrm{Col}^\bullet_\mathfrak{q})} \right)$$

to the $\mathbb{Q}$-cyclotomic line has rank zero, by equation (3) in [64, Proof of Theorem 7.14]. Now if $\mathcal{N}$ as a Λ_K-module were not torsion, then the specialization to the cyclotomic line of $\mathcal{N}$ would also be non-torsion, which contradicts the previous sentence. Thus $\mathcal{N}$ itself must be of rank zero, whence $\mathcal{X}^{\hat{\bullet}\forall}$ has rank at most one.

To see that the rank is at least one, consider the composed map

$$\mathcal{X}^{\hat{\bullet}\forall} \longrightarrow \frac{H^1(K_\mathfrak{q}, \mathcal{T})}{\ker(\mathrm{Col}^\bullet_\mathfrak{q})} \xrightarrow{\mathrm{Col}^\bullet_\mathfrak{q}} \Lambda_K$$

and note that we have chosen $\bullet$ so that $\mathrm{Col}^\bullet_\mathfrak{q}(\nu\Delta_\bullet) \neq 0$. □

We will see in the next section that $\nu\Delta_\bullet \in \mathcal{X}^{\hat{\bullet}\forall}$ (see the proof of Proposition 4.15 and the discussion before that) and that $\mathcal{X}^{\bullet 0}$ is a finitely generated torsion Λ_K-module if one chooses $\bullet \in \{\sharp, \flat\}$ as in Choice 3.12. Assuming this for now, we can formulate the main conjecture of this subsection:

Conjecture 3.45. *(The ♯/♭ Beilinson-Flach element main conjecture) Assume Corollary 3.41. Choose* $\bullet \in \{\sharp, \flat\}$ *so that* $\mathcal{X}^{\bullet 0}$ *and* $\mathcal{X}^{\hat{\bullet}\forall}/\nu\Delta_\bullet\Lambda_K$ *are finitely generated torsion as* Λ_K*-modules. We then have*

$$\mathrm{Char}(\mathcal{X}^{\hat{\bullet}\forall}/\nu\Delta_\bullet\Lambda_K) = (\nu)\,\mathrm{Char}(\mathcal{X}^{\bullet 0}).$$

4. Connecting the main conjectures together

4.1. The ♯/♭-Beilinson-Flach conjectures and the Greenberg-type conjecture

The aim of this subsection is to prove equivalence of slightly modified main conjectures, where instead of ideals in the ring Λ_K, we instead work with fractional Λ_K-ideals for which we have controllable denominators. We do this by constructing maps $\mathscr{L}^\sharp$ and $\mathscr{L}^\flat$ which generalize Wan's map LOG^+. Put

$$\mathcal{H}_n(X) =: \begin{pmatrix} \omega_n^\sharp & \Phi_{p^n}\omega_{n-1}^\sharp \\ \omega_n^\flat & \Phi_{p^n}\omega_{n-1}^\flat \end{pmatrix}.$$

We can describe $\ker(h_{n,m})$, defined in Definition 3.16, explicitly by $\ker(h_{n,m}) = (\Lambda_{n,m} \oplus \Lambda_{n,m})\mathcal{H}_n^\perp$, where

$$\mathcal{H}_n^\perp = X \begin{pmatrix} \omega_n^\flat & -\omega_n^\sharp \\ \Phi_{p^n}\omega_{n-1}^\flat & -\Phi_{p^n}\omega_{n-1}^\sharp \end{pmatrix}.$$

(See [64, Lemma 5.8] for the Λ_n-module case. The same arguments apply to the $\Lambda_{n,m}$-module case as well.)

Remark 4.1. Similarly, the kernel of multiplying by $\mathcal{H}_n^\perp$ is $(\Lambda_{n,m} \oplus \Lambda_{n,m})\mathcal{H}_n$.

Lemma 4.2. *We have* $(c_{n,m}, c_{n-1,m})\mathcal{H}_n^\perp = (0,0)$.

Proof. This follows from $\Lambda_{n,m}$-bilinearity of the pair of pairings $(P_{n,m,c_{n,m}}, P_{n,m,c_{n-1,m}})$. □

Proposition 4.3. *We can choose* $(b_{n,m}^\sharp, b_{n,m}^\flat) \in H^1(k_{n,m}, T)^{\oplus 2}$ *so that*

$$(i) \quad (b_{n,m}^\sharp, b_{n,m}^\flat)\mathcal{H}_n = (c_{n,m}, c_{n-1,m}), \text{ and}$$

$$(ii) \quad \mathrm{tr}_{k_{n,m}/k_{n-1,m}}\, b_{n,m}^{\sharp/\flat} = b_{n-1,m}^{\sharp/\flat}, \text{ and } \mathrm{tr}_{k_{n,m}/k_{n,m-1}}\, b_{n,m}^{\sharp/\flat} = b_{n,m-1}^{\sharp/\flat}.$$

Proof. The existence of such $(b_{n,m}^\sharp, b_{n,m}^\flat)$ satisfying (i) follows from Lemma 4.2 and Remark 4.1. 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

$$\mathrm{tr}_{n/n-1}\left((b^\sharp_{n,m}, b^\flat_{n,m})\mathcal{H}_n\right) = \left(\mathrm{tr}_{n/n-1}\, b^\sharp_{n,m}, \mathrm{tr}_{n/n-1}\, b^\flat_{n,m}\right)\mathcal{H}_{n-1}\left(\begin{smallmatrix} a_p & p \\ -1 & 0\end{smallmatrix}\right),$$
$$\text{while } \mathrm{tr}_{n/n-1}\,(c_{n,m}, c_{n-1,m}) = (c_{n-1,m}, c_{n-2,m})\left(\begin{smallmatrix} a_p & p \\ -1 & 0\end{smallmatrix}\right). \quad \square$$

Definition 4.4. 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 $b^\sharp_{n,m}$, and define $H^1_\flat(k_{n,m}, T)$ analogously.

Note that the definition of $H^1_\sharp(k_{n,m}, T)$ and $H^1_\flat(k_{n,m}, T)$ depends on the choice of $b^\sharp_{n,m}$ and $b^\flat_{n,m}$. The next proposition shows that this dependence goes away in the limit.

Proposition 4.5. *We have* $H^1_{\sharp/\flat} := \varprojlim_{n,m} H^1_{\sharp/\flat}(k_{n,m}, T) = \ker \mathrm{Col}^{\sharp/\flat}$.

Proof. For $(b^\sharp_{n,m}, b^\flat_{n,m}) \in H^1(k_{n,m}, T)^2$, we have $\mathrm{Col}_{n,m}(b^\sharp_{n,m}, b^\flat_{n,m}) = 0$ in $\frac{\Lambda_{n,m}\oplus\Lambda_{n,m}}{\ker \mathcal{H}_n}$ by construction. Thus, we have $H^1_\sharp \subset \ker \mathrm{Col}^\sharp$ and $H^1_\flat \subset \ker \mathrm{Col}^\flat$. To prove equality, we show that $\frac{\ker \mathrm{Col}^\sharp}{H^1_\sharp} = 0$. By Nakayama's lemma, it suffices to do this for the Coleman map at level 0: By [64, discussion before Definition 7.2], we have

$$\mathrm{Col}_{0,m} = (\mathrm{Col}^\sharp_{0,m}, \mathrm{Col}^\flat_{0,m}) = (-a_p P_{0,m,c_{0,m}} + P_{0,m,c_{0,m}}, -P_{c_{0,m}}) = \left(P_{0,m,b^\sharp_0}, P_{0,m,b^\flat_0}\right).$$

But $b^{\sharp/\flat}_0$ annihilate themselves under the cup product, so $\ker \mathrm{Col}^\sharp_{0,m}$ is generated by $b^\sharp_{0,m}$. The $\flat$ case is proved similarly. $\square$

Denote by t_{anti} the anticyclotomic variable. If we pick K and $\bullet \in \{\sharp, \flat\}$ as in our Choice 3.12, denote by $\mathcal{X}^\bullet_K$ the $\bullet$-Selmer group dual of the elliptic curve $E^{(K)}$.

Proposition 4.6. *For the above choice, we have* $\mathcal{X}^{\bullet\bullet} \otimes \Lambda_K/(t_{anti}) \cong \mathcal{X}^\bullet \oplus \mathcal{X}^\bullet_K$

Proof. Construct the dual $\mathcal{X}_{K_{cyc}/K}$ of the $\bullet$-Selmer group in the cyclotomic variable with base field K by restricting the construction of $\mathrm{Col}^\sharp$ and $\mathrm{Col}^\flat$ to $m = 0$, employing the compatibility in the ramified direction (Proposition 3.20): We put

$$(\mathrm{Col}^\sharp_{\mathrm{ram}}, \mathrm{Col}^\flat_{\mathrm{ram}}) := \varprojlim_n \mathrm{Col}_{n,0}$$

and denote the resulting local condition by $E^\sharp_{\mathrm{ram}}$ and $E^\flat_{\mathrm{ram}}$. (In other words, we repeat Definitions 3.22 and 3.23, setting $m = 0$.)

This results in a $\Lambda_K/(t_{anti})$-module, and in fact we claim that we have

$$\mathcal{X}^{\bullet\bullet} \otimes \Lambda_K/(t_{anti}) \cong \mathcal{X}^\bullet_{K_{cyc}/K}. \tag{4}$$

Assuming (4), the result follows by Shapiro's lemma.

To prove the claim (4), we prove the dual statement $(\mathrm{Sel}^{\bullet\bullet})^{t_{anti}=0} \cong \mathrm{Sel}^\bullet_{K_{cyc}/K}$, where $\mathrm{Sel}^\bullet_{K_{cyc}/K}$ is the Selmer group introduced at the beginning of the proof. This follows from applying the snake lemma to the following commutative diagram of exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Sel}^{\bullet}_{K_{cyc}/K} & \longrightarrow & \mathrm{Sel}(E/K_{cyc}) & \longrightarrow & \bigoplus_{v|\mathfrak{p}} \mathscr{H}_v^{\bullet}(\mathfrak{p}) \oplus \bigoplus_{v|\mathfrak{q}} \mathscr{H}_v^{\bullet}(\mathfrak{q}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & (\mathrm{Sel}^{\bullet\bullet})^{t_{anti}=0} & \longrightarrow & (\mathrm{Sel}(E/K_{\infty}))^{t_{anti}=0} & \longrightarrow & (\mathscr{H}^{\bullet\bullet}_{\mathrm{loc}})^{t_{anti}=0}, & & \end{array}$$

where

$$\mathscr{H}_v^{\bullet}(\mathfrak{p}) := \frac{\varinjlim_{m,n} H^1(k_{n,m}(\mathfrak{p}), V/T)}{E^{\bullet}_{\mathrm{ram}}}$$

and $\mathscr{H}_v^{\bullet}(\mathfrak{q})$ is defined similarly, and $\mathscr{H}^{\bullet\bullet}_{\mathrm{loc}}$ is the local condition appearing in Definition 3.24 with $\star = \circ = \bullet$. The middle map is an isomorphism by the inflation-restriction sequence applied to $H^1(K_{cyc}, V/T) \to H^1(K_{\infty}, V/T)$ and noting that the p-power torsion is trivial: $E(K_{\infty})_{p^{\infty}} = 0$, which can be proved as in [64, Lemma 2.3].

If we could prove that the lower right (horizontal) map injects into $\mathscr{H}^{\bullet\bullet}_{\mathrm{loc}}$, then a posteriori, the right map would be an injection. By Definition 3.23 and its restriction to $m = 0$, this would follow if $\mathrm{Hom}(\ker(\mathrm{Col}^{\bullet}_{\mathrm{ram}}), \mathbb{Q}_p/\mathbb{Z}_p)$ injects into $\mathrm{Hom}(\ker(\mathrm{Col}^{\bullet}), \mathbb{Q}_p/\mathbb{Z}_p)$, i.e. if $\ker \mathrm{Col}^{\bullet}$ surjects onto $\ker \mathrm{Col}^{\bullet}_{\mathrm{ram}}$.

Proposition 4.5 says that $\ker \mathrm{Col}^{\bullet}$ is the inverse limit of the rank one $\Lambda_{n,m}$-submodules of $H^1(k_{n,m}, T)$ generated by $b^{\bullet}_{n,m}$: $\ker \mathrm{Col}^{\bullet} = \varprojlim_{n,m} \Lambda_{n,m} b^{\bullet}_{n,m}$. We can restrict the arguments of Proposition 4.5 to $m = 0$ to obtain that $\ker \mathrm{Col}^{\bullet}_{\mathrm{ram}} = \varprojlim_n \Lambda_n b^{\bullet}_{n,0}$, where we have identified Λ_n with $\Lambda_{n,0}$. Proposition 4.3 (ii) and the Mittag-Leffler condition provide the desired surjectivity. □

Corollary 4.7. *For a choice of K and $\bullet \in \{\sharp, \flat\}$ as in Choice 3.12, the dual Selmer group $\mathcal{X}^{\bullet\bullet}$ is torsion as a Λ_K-module.*

Proof. This follows from Proposition 4.6, since the maximal Λ_K-torsion-free quotient of $\mathcal{X}^{\bullet\bullet}$ maps to the $\Lambda_K/(t_{anti})$-free part of $\mathcal{X}^{\bullet\bullet} \otimes \Lambda_K/(t_{anti})$, where t_{anti} is the anticyclotomic variable. □

Proposition 4.8. *Given K and $\bullet \in \{\sharp, \flat\}$ as in Choice 3.12, $\mathcal{X}^{\bullet 0}$ is a finitely generated torsion Λ_K-module.*

Proof. The inclusion $\mathrm{Sel}^{\bullet 0} \hookrightarrow \mathrm{Sel}^{\bullet\bullet}$ gives rise to a surjection

$$\mathcal{X}^{\bullet\bullet} \longrightarrow \mathcal{X}^{\bullet 0} \longrightarrow 0.$$

To prove that $\mathcal{X}^{\bullet 0}$ is finitely generated torsion, it suffices to prove that $\mathcal{X}^{\bullet\bullet}$ is, but this is exactly Corollary 4.7. □

Definition 4.9. The maps $\mathscr{L}^{\sharp/\flat}$ map elements of $H^1_{\sharp/\flat}$ to their coordinates, i.e. we put:

$$\mathscr{L}^{\sharp} : H^1_{\sharp} = \varprojlim_{n,m} H^1_{\sharp}(k_{n,m}, T) \to \Lambda_K, (f^{\sharp/\flat}_{n,m} \cdot b^{\sharp}_{n,m})_{n,m} \mapsto (f^{\sharp/\flat}_{n,m})_{n,m}$$

and define $\mathscr{L}^\flat$ similarly.

Definition 4.10. As in Definition 3.25, we let $\mathscr{L}_{\mathfrak{p}}^\sharp$ and $\mathscr{L}_{\mathfrak{p}}^\flat$ stand for their extensions to their sums over representatives $\{\gamma_v\}_{v|\mathfrak{p}}$ of $\mathrm{Gal}(K_\infty/K)/D_p$.

Proposition 4.11. *Recall we have chosen $\bullet \in \{\sharp, \flat\}$ so that $\Delta_\bullet \neq 0$. For such a choice,*

$$\mathscr{L}_{\mathfrak{p}}^\bullet\left((\nu\Delta_\bullet)_{\mathfrak{p}}\right) = L_p^{\forall 0} \times h \times H \times \nu,$$

where h is the constant chosen in the proof of Proposition 3.36 and $H \in \mathcal{R}$.

Lemma 4.12. *We have*

$$\tilde{\varphi}(c_{n,m}) = \tau(\varphi|_{\Gamma_{n,\mathfrak{q}}})\varphi(u) \times \sum_{v \in U_{m,\mathfrak{q}}} \varphi(v) d_m^v \text{ and}$$
$$\tilde{\varphi}(c_{n-1,m}) = 0.$$

(Remember that the d_m were defined in the proof of Lemma 3.13 after Definition 3.14.)

Proof. This is a calculation similar to [32, Prop 8.26]. Cf. also [74, Prop. 2.10]. □

Denote by $x_{n,m}^{\sharp/\flat}$ the image of $\nu\Delta_{\sharp/\flat}$ in $H^1_{\sharp/\flat}(k_{n,m}, T)$. By Assumption 3.33 ($*\exp_{\mathfrak{p}}$), the Beilinson-Flach elements $\Delta_\alpha, \Delta_\beta$ are geometric, so that

$$h \times \left(x_{n,m}^\sharp, x_{n,m}^\flat\right) \mathcal{H}_n = (c_{n,m}, c_{n-1,m}) \begin{pmatrix} g_{n,m}^\sharp & r_{n,m}^\sharp \\ g_{n,m}^\flat & r_{n,m}^\flat \end{pmatrix},$$

where the elements $g_{n,m}^{\sharp/\flat}$ and $r_{n,m}^{\sharp/\flat}$ of the matrix on the very right are in $\Lambda_{n,m}$.

The above lemma tells us the following:

Corollary 4.13. *We have $r_{n,m}^\sharp = 0$.*

Proof. By a direct calculation, we have that

$$\begin{pmatrix} g_{n-6,m}^\sharp & r_{n-6,m}^\sharp \\ g_{n-6,m}^\flat & r_{n-6,m}^\flat \end{pmatrix} = \mathrm{tr}_{k_{n,m}/k_{n-6,m}} \begin{pmatrix} g_{n,m}^\sharp & r_{n,m}^\sharp \\ g_{n,m}^\flat & r_{n,m}^\flat \end{pmatrix}.$$

By induction, $r_{n,m}^\sharp = \mathrm{tr}_{k_{n+6k,m}/k_{n,m}} r_{n+6k,m}^\sharp$. But by Lemma 4.12, $\Phi_{p^{n+6k}}$ divides $r_{n+6k,m}^\sharp$, contributing a factor of p to $r_{n,m}^\sharp$ after taking traces. Now $c_{n,m}$ are six-periodic with respect to trace. We refer to [64, Table after Definition 2.4] for a catalogue of these traces that relies on the Hasse-Weil bound $|a_p| \leqslant 2\sqrt{p}$ [60, Chapter 5]. Thus a factor of p^k divides $r_{n,m}^\sharp$, for any positive integer k, whence $r_{n,m}^\sharp = 0$.

Proof of Proposition 4.11. The above Corollary 4.13 tells us that $r^\sharp_{n,m} = 0$, for all n. Applying the trace $\mathrm{tr} = \mathrm{tr}_{k_{n,m}/k_{n-1,m}}$, we obtain that

$$h \times (x^\sharp_{n,m}, x^\flat_{n,m})\mathcal{H}_{n-1} \left(\begin{smallmatrix} a_p & p \\ -1 & 0 \end{smallmatrix}\right) = (c_{n,m}, c_{n-1,m}) \left(\begin{smallmatrix} a_p & p \\ -1 & 0 \end{smallmatrix}\right) \begin{pmatrix} \mathrm{tr}\, g^\sharp_{n,m} & 0 \\ \mathrm{tr}\, g^\flat_{n,m} & \mathrm{tr}\, r^\flat_{n,m} \end{pmatrix}.$$

But by definition,

$$h \times (x^\sharp_{n,m}, x^\flat_{n,m})\mathcal{H}_{n-1} = (c_{n,m}, c_{n-1,m}) \begin{pmatrix} g^\sharp_{n-1,m} & 0 \\ g^\flat_{n-1,m} & r^\flat_{n-1,m} \end{pmatrix}, \text{ so}$$

$$\begin{aligned} \begin{pmatrix} g^\sharp_{n-1,m} & 0 \\ g^\flat_{n-1,m} & r^\flat_{n-1,m} \end{pmatrix} &= \left(\begin{smallmatrix} a_p & p \\ -1 & 0 \end{smallmatrix}\right) \begin{pmatrix} \mathrm{tr}\, g^\sharp_{n,m} & 0 \\ \mathrm{tr}\, g^\flat_{n,m} & \mathrm{tr}\, r^\flat_{n,m} \end{pmatrix} \left(\begin{smallmatrix} a_p & p \\ -1 & 0 \end{smallmatrix}\right)^{-1} \\ &= \begin{pmatrix} \mathrm{tr}\, r^\flat_{n,m} & a_p\, \mathrm{tr}(r^\flat_{n,m} - g^\sharp_{n,m}) - p\, \mathrm{tr}\, g^\flat_{n,m} \\ 0 & \mathrm{tr}\, g^\sharp_{n,m} \end{pmatrix}. \end{aligned}$$

We thus conclude that $g^\flat_{n-1,m} = 0$ for all n, so in particular the coefficient matrix must be diagonal. Therefore, $a_p\, \mathrm{tr}(r^\flat_{n,m} - g^\sharp_{n,m}) = 0$.

In general, we thus have

$$h \times (x^\sharp_{n,m}, x^\flat_{n,m})\mathcal{H}_n = (c_{n,m}, c_{n-1,m}) \begin{pmatrix} g^\sharp_{n,m} & a_p\, \mathrm{tr}(r^\flat_{n,m} - g^\sharp_{n,m}) = 0 \\ 0 & r^\flat_{n,m} \end{pmatrix}.$$

Denote by $f^\sharp_{n,m}$ and $f^\flat_{n,m}$ the coordinates of $x^\sharp_{n,m}$ and $x^\flat_{n,m}$ (so that e.g. $x^\sharp_{n,m} = f^\sharp_{n,m} b^\sharp_{n,m}$).

By Lemma 4.14 below, we have $r^\flat_{n,m} = g^\sharp_{n,m}$ and give this element the name $f_{n,m}$. The reason for this name is simply that $f_{n,m} = f^\sharp_{n,m} = f^\flat_{n,m}$. We thus have

$$\tilde{\varphi}(c_{n,m}, c_{n-1,m})\varphi(f_{n,m})B = \tilde{\varphi}\left(h \times (x^\sharp_{n,m}, x^\flat_{n,m})\mathcal{H}_n\right) B$$

for any $B \in \mathrm{GL}_2(\mathbb{Q}_p(\alpha))$ and will now compare the first components of these two vectors more explicitly: Since

$$\mathcal{L}og_{a_p}(\varphi(\gamma)) = \mathcal{H}_n(\varphi(\gamma)) \left(\begin{smallmatrix} \alpha & \beta \\ -1 & -1 \end{smallmatrix}\right) \begin{pmatrix} \alpha^{-n} & 0 \\ 0 & \beta^{-n} \end{pmatrix},$$

we can let $B = \left(\begin{smallmatrix} \alpha & \beta \\ -1 & -1 \end{smallmatrix}\right) \begin{pmatrix} \alpha^{-n} & 0 \\ 0 & \beta^{-n} \end{pmatrix}$ and invoke[15] Assumption 3.33 $(*\log_{\mathfrak{q}})$ to compare the vectors. Thus, we conclude that the limit of the $f_{n,m}$'s agrees with $\nu L_p^{\forall 0}$ at finite characters φ up to the factors h and H, as desired. □

Lemma 4.14. *With the notation as in the previous proof, we have* $g^\sharp_{n,m} = r^\flat_{n,m}$.

[15] cf. also [74, Proposition 3.14].

Proof. If $a_p = 0$, $\mathcal{H}_n$ is diagonal for even n and antidiagonal for odd n. For even n, we can thus directly equate the diagonal coefficients and conclude that $f^{\sharp}_{n,m} = g^{\sharp}_{n,m}$ and $f^{\flat}_{n,m} = r^{\flat}_{n,m}$. The case of odd n is more interesting: Recall that an anti-diagonal matrix anti-commutes with a diagonal matrix. We thus have that $f^{\flat}_{n,m} = g^{\sharp}_{n,m}$ and $f^{\sharp}_{n,m} = r^{\flat}_{n,m}$. By trace-compatibility of the $f^{\sharp/\flat_{n,m}}$'s, we conclude that all four elements under discussion are equal to each other. When $a_p \neq 0$, then we know that $\mathrm{tr}_{n/n-1}(r^{\flat}_{n,m} - g^{\sharp}_{n,m}) = 0$ for all n which proves the assertion. □

The following proposition relates the Greenberg-type main conjecture (full equality in Theorem 3.29) – modified by the factor hH appearing in Proposition 4.11 – to the ♯/♭-Beilinson-Flach main Conjecture 3.45.

Proposition 4.15. *The equality of Λ_K-ideals*

$$\mathrm{Char}(\mathcal{X}^{\forall 0}) = (hHL_p^{\forall 0}) \lhd \frac{1}{\nu}\Lambda_K$$

is equivalent to the ♯/♭-Beilinson-Flach main conjecture Conjecture 3.45. The same can be said about any of the two halves (i.e. inclusion in one fixed direction between the algebraic and analytic sides) of the statements.

Proof. The localization at $\mathfrak{p}$ of $(\Delta_\sharp, \Delta_\flat)$ (defined in Corollary 3.41) lands in

$$H^1_\sharp(K_\mathfrak{p}, \mathcal{T}) \oplus H^1_\flat(K_\mathfrak{p}, \mathcal{T}) := \ker \mathrm{Col}^\sharp_\mathfrak{p} \oplus \ker \mathrm{Col}^\flat_\mathfrak{p},$$

since the image of $(\Delta_\alpha, \Delta_\beta) = (\Delta_\sharp, \Delta_\flat)\mathcal{L}og$ at any $\varphi \in \Gamma_{n,\mathfrak{p}} \times U_m$ is in the kernel of the pairing $\left(P_{n,m,c_{n,m}}, P_{n,m,c_{n-1,m}}\right)$ (cf. Proposition 3.18). From the Poitou-Tate exact sequence, we have the exact sequence

$$\mathcal{X}^{\hat{\bullet}\forall} \longrightarrow H^1_\bullet(K_\mathfrak{p}, \mathcal{T}) \longrightarrow \mathcal{X}^{\forall 0} \longrightarrow \mathcal{X}^{\bullet 0} \longrightarrow 0.$$

The first map $\mathcal{X}^{\hat{\bullet}\forall} \longrightarrow H^1_\bullet(K_\mathfrak{p}, \mathcal{T})$ is injective – this follows from the nontriviality of $\mathscr{L}^\bullet_\mathfrak{p}$ (cf. Proposition 4.11), using similar arguments as [32, Proof of Theorem 7.3.i)]: By our choice of $\bullet \in \{\sharp, \flat\}$, we have $\mathrm{Col}^\bullet(\nu\Delta_\bullet) \neq 0$, so that $H^1_\bullet \neq 0$ as well. From Proposition 3.44, $\mathcal{X}^{\hat{\bullet}\forall}$ is free of rank one, so the composed morphism

$$\mathcal{X}^{\hat{\bullet}\forall} \longrightarrow H^1_\bullet(K_\mathfrak{p}, \mathcal{T}) \longrightarrow \Lambda_K$$

is injective if and only if it is a non-zero map.

We then have an exact sequence

$$0 \longrightarrow \mathcal{X}^{\hat{\bullet}\forall}/\nu\Delta_\bullet \longrightarrow \Lambda_K/\mathscr{L}^\bullet_\mathfrak{p}(\nu\Delta_\bullet) \longrightarrow \mathcal{X}^{\forall 0} \longrightarrow \mathcal{X}^{\bullet 0} \longrightarrow 0.$$

The theorem follows from multiplicativity of characteristic ideals in exact sequences. □

Corollary 4.16. *Let $a \in \Lambda_K$. The inclusion of fractional Λ_K-ideals*

$$(a)\,\mathrm{Char}(\mathcal{X}^{\forall 0}) \subseteq (L_p^{\forall 0}) \triangleleft \frac{1}{\nu h H}\Lambda_K$$

is equivalent to the statement

$$(\nu)(a)\,\mathrm{Char}(\mathcal{X}^{\bullet 0}) \subseteq \frac{1}{hH}\,\mathrm{Char}(\mathcal{X}^{\hat{\bullet}\forall}/\nu\Delta_\bullet\Lambda_K) \triangleleft \Lambda_K \otimes \mathrm{Frac}\,\Lambda'$$

about fractional Λ_K-ideals (with $\bullet \in \{\sharp, \flat\}$ so that $\mathcal{X}^{\hat{\bullet}\forall}/\nu\Delta_\bullet\Lambda_K$ is a finitely generated torsion Λ_K-module).

Proof. We run the arguments of the above Proposition 4.15, but replace $\Delta_\bullet$ by $\frac{1}{ahH}\Delta_\bullet$. For this, we regard $\mathrm{Sel}^{\hat{\bullet}\forall}$ as a rank one Λ_K-submodule of $\mathrm{Frac}\,\Lambda_K$. Then we multiply back (a). □

4.2. The ♯/♭-Beilinson-Flach conjectures and the ♯/♭-♯/♭ conjectures

Proposition 4.17. *Assume Conjecture 3.33 $(*\exp_{\mathfrak{q}})$. Let $h \in \mathbb{Q}_p \otimes \mathbb{Z}_p[[X,U]]$ be the element from Proposition 3.36. Then*

$$\mathrm{Col}(\nu\Delta) := \begin{pmatrix} \mathrm{Col}_{\mathfrak{q}}^{\sharp}(\nu\Delta_\sharp) & \mathrm{Col}_{\mathfrak{q}}^{\sharp}(\nu\Delta_\flat) \\ \mathrm{Col}_{\mathfrak{q}}^{\flat}(\nu\Delta_\sharp) & \mathrm{Col}_{\mathfrak{q}}^{\flat}(\nu\Delta_\flat) \end{pmatrix} = h \cdot \nu \begin{pmatrix} L_{\sharp\sharp} & L_{\flat\sharp} \\ L_{\sharp\flat} & L_{\flat\flat} \end{pmatrix}.$$

Proof. It suffices to show that

$$\mathcal{L}og(Y)^T\,\mathrm{Col}(\nu\Delta)\mathcal{L}og(X) = \mathcal{L}og(Y)^T h \cdot \nu \begin{pmatrix} L^{\sharp\sharp} & L^{\flat\sharp} \\ L^{\sharp\flat} & L^{\flat\flat} \end{pmatrix} \mathcal{L}og(X) = h \cdot \nu \begin{pmatrix} L_{\alpha\alpha} & L_{\beta\alpha} \\ L_{\alpha\beta} & L_{\beta\beta} \end{pmatrix}.$$

Since the entries of $\mathcal{L}og(\_)$ are $\mathcal{O}(\log^{\frac{1}{2}}(\_))$, we need to prove that the above holds at all cyclotomic points in the variables X and Y, i.e. at $X = \zeta_{p^n} - 1$ and $Y = \zeta_{p^{n'}} - 1$.

We can relate $\mathcal{L}og(\zeta_{p^{n'}} - 1)^T\ \mathrm{Col}(\nu\Delta)|_{Y=\zeta_{p^{n'}}-1}$ to the pairing $P_n^{(1\text{ or }0)}(\Delta_{\sharp/\flat})$ for evaluation at $Y = \zeta_{p^{n'}} - 1$, by the proof of [64, Proposition 6.5]. Using the relation

$$h(\Delta_\alpha, \Delta_\beta) = (\Delta_\sharp, \Delta_\flat)\mathcal{L}og(X),$$

the claim then follows from Proposition 3.18, the identity

$$P_{n,m,x}(z) = \left(\sum_{\sigma \in \Gamma_n \times U_m} \log_{\mathfrak{q}}(x^\sigma)\sigma\right)\left(\sum_{\sigma \in \Gamma_n \times U_m} \exp_{\mathfrak{q}}^*(z^\sigma)\sigma^{-1}\right),$$

the commutative diagram in ([40, Theorem 7.1.4]) that compares $\exp_{\mathfrak{q}}$ and $\mathcal{L}$, and Conjecture 3.33 $(*\exp_{\mathfrak{q}})$. □

Proposition 4.18. *Choose $\bullet, \diamond \in \{\sharp, \flat\}$ so that $\mathcal{X}^{\bullet\diamond}$ is finitely generated Λ_K-torsion and $L_{\bullet\diamond} \neq 0$. Then the $\bullet\diamond$-main conjecture modified by the factor h from Proposition 4.17, i.e. the statement*

$$\mathrm{Char}(\mathcal{X}^{\bullet\diamond}) = (hL_{\bullet\diamond}) \triangleleft \Lambda_K \otimes \mathbb{Q}_p$$

is equivalent to the $\bullet$-Beilinson–Flach main conjecture, Conjecture 3.45.

Corollary 4.7 guarantees that such a choice exists. The idea of the proof of this theorem is the same as the one for Proposition 4.15.

Proof. From the Poitou–Tate sequence, we have

$$\mathcal{X}^{\hat{\bullet}\forall} \longrightarrow \frac{H^1(K_\mathfrak{q}, \mathcal{T})}{H^1_\diamond(K_\mathfrak{q}, \mathcal{T})} \longrightarrow \mathcal{X}^{\bullet\diamond} \longrightarrow \mathcal{X}^{\bullet 0} \longrightarrow 0,$$

where $H^1_\diamond(K_\mathfrak{q}, \mathcal{T}) := \ker \mathrm{Col}_\diamond$. Since $L_{\bullet\diamond} \neq 0$, neither $\mathrm{Col}^\diamond$ nor $\Delta_\bullet$ are zero. Thus $\mathcal{X}^{\hat{\bullet}\forall}$ is free of rank 1 (cf. Proposition 3.44), so the first map in the above exact sequence being injective as a Λ_K-module is equivalent to its non-triviality.

Taking quotients by the $\sharp/\flat$ Beilinson–Flach elements resp. their images, we have the exact sequence

$$0 \longrightarrow \mathcal{X}^{\hat{\bullet}\forall}/\nu\Delta_\bullet \longrightarrow \Lambda_K/\,\mathrm{Col}^\diamond(\nu\Delta_\bullet) \longrightarrow \mathcal{X}^{\bullet\diamond} \longrightarrow \mathcal{X}^{\bullet 0} \longrightarrow 0.$$

The equivalence of main conjectures follows from multiplicativity of characteristic ideals. □

Corollary 4.19. *Choose $\bullet, \diamond \in \{\sharp, \flat\}$ so that $\mathcal{X}^{\bullet\diamond}$ and $\mathcal{X}^{\hat{\bullet}\forall}/\nu\Delta_\bullet\Lambda_K$ are finitely generated Λ_K-torsion and $L_{\bullet\diamond} \neq 0$. Then for $a \in \Lambda_K$, the inclusion of Λ_K-fractional ideals*

$$(a)\,\mathrm{Char}(\mathcal{X}^{\bullet\diamond}) \subseteq \left(\frac{1}{H} L_{\bullet\diamond}\right) \triangleleft \Lambda_K \otimes \mathrm{Frac}\,\Lambda'$$

is equivalent to the inclusion

$$(\nu)(a)\,\mathrm{Char}(\mathcal{X}^{\bullet 0}) \subseteq \frac{1}{hH}\,\mathrm{Char}(\mathcal{X}^{\hat{\bullet}\forall}/\nu\Delta_\bullet\Lambda_K) \triangleleft \Lambda_K \otimes \mathrm{Frac}\,\Lambda'.$$

(By construction, Choice 3.12 furnishes us with such a choice.)

Proof. We can use similar arguments as in Corollary 4.16 but applied to the above Proposition 4.18. The direct analogue would be to multiply $\Delta_\bullet$ by $\frac{1}{ah}$, which would give us that

$$(a)\,\mathrm{Char}(\mathcal{X}^{\bullet\diamond}) \subseteq (L_{\bullet\diamond}) \triangleleft \Lambda_K$$

is equivalent to the statement

$$(\nu)(a)\,\mathrm{Char}(\mathcal{X}^{\bullet 0}) \subseteq \frac{1}{h}\,\mathrm{Char}(\mathcal{X}^{\hat{\bullet}\forall}/\nu\Delta_\bullet\Lambda_K) \lhd \Lambda_K \otimes \mathbb{Q}_p.$$

Instead, we multiply $\Delta_\bullet$ by $\frac{1}{ah} \times \frac{1}{H}$ and obtain the desired equivalence of statements. □

4.3. Almost completing the argument

We now bring all the arguments together to deduce an inclusion of two-variable power series, before deriving an inclusion of one-variable power series.

Proposition 4.20. *Choose K and $\bullet \in \{\sharp, \flat\}$ as in Choice 3.12. Let E have square-free conductor N that has at least one prime divisor $l|N$ not split in K, and suppose that $E[p]|_{G_K}$ is absolutely irreducible. Then we have*

$$(a)\,\mathrm{Char}(\mathcal{X}^{\bullet\bullet}) \subseteq \left(\frac{1}{H}L_{\bullet\bullet}\right).$$

Here, $H \in \mathrm{Frac}\,\Lambda'$ and $a \in \Lambda_K$ are chosen as in Propositions 4.17, 4.11, and Theorem 3.29.

Proof. Corolllary 4.7 guarantees that $\mathcal{X}^{\bullet\bullet}$ is torsion. The proposition then follows from combining Theorem 3.29 with Corollaries 4.16 and 4.19. □

The idea of the proof is to now project down to the one-variable Iwasawa algebra by collapsing along the anticyclotomic line. To do this, we need to deal with the denominators that could occur when collapsing the right-hand side of the inclusion in the above proposition.

We let K_{anti} be the anticyclotomic $\mathbb{Z}_p$-extension of K.

Proposition 4.21. *($\mathfrak{Q}$-coprimality of $L^{\bullet\bullet}$) Let K and $\bullet \in \{\sharp, \flat\}$ be as in Choice 3.12 so that $L^{\bullet\bullet} \neq 0$. Furthermore, assume that N is a product of distinct unramified primes in K, an odd number of which are inert. Also assume that for any such inert prime $q|N$, the representation $E[p]|_{G_{\mathbb{Q}_q}}$ is ramified. Then for any height one prime $\mathfrak{Q}$ of Λ_K which is the pullback of a height one prime of $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K_{anti})]]$, we have*

$$\mathrm{ord}_{\mathfrak{Q}}\, L^{\bullet\bullet} = 0.$$

Lemma 4.22. *Let $\mathfrak{Q}$ be as in the above Proposition 4.21. If a power series $\mathcal{P} \in \Lambda_K$ satisfies $\mathrm{ord}_{\mathfrak{Q}}\,\mathcal{P} > 0$, then its specialization to the anticyclotomic line $\mathcal{P}_{t_{anti}}$ satisfies $\mathrm{ord}_p(\mathcal{P}_{t_{anti}}) > 0$.*

Proof. We can evaluate $\mathfrak{Q}$ by setting the cyclotomic variable to be equal to 0, and obtain a (nonzero) positive power of p by the Weierstrass preparation theorem. □

Proof of Proposition 4.21. By the above Lemma 4.22, this follows from the vanishing of the μ-invariants for the specialization of $L^{\bullet\bullet}$ to the anticyclotomic line.[16] (The assumptions on the divisors of N are used to establish that $L^{\bullet\bullet}$ does not identically vanish there, cf. [69].) The assumptions of [55] are not necessary in our case, cf. [74, the discussion in Proposition 4.8] and [29, Theorem 1.13]. In the case $a_p = 0$, the vanishing of this μ-invariant follows from [55, Theorem 2.5]. Here, the anticyclotomic p-adic L-functions $L^{\pm}_{anti}$ were constructed by combining sequences $\{L_n\}_{n\geqslant 1}$ (satisfying certain three-term relations) with Kobayashi's construction of the $\pm$-Coleman maps [32, 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 $\bullet$-Coleman maps in [64, Section 5] to arrive at an anticyclotomic p-adic L-function $L^{\bullet}_{anti}$. The arguments in [55, Proof of Theorem 2.5] then show that $\mu(L_n) = 0$ for $n \gg 0$. But [53, discussion at the end of page 165] shows that the $\mu_\bullet$-invariant of Perrin-Riou is then 0. By [66, Corollary 8.9], we conclude that the μ-invariant of $L^{\bullet}_{anti}$ is zero. □

Recall from Choice 3.12 that $L^{\bullet}_K$ is the $\bullet$ p-adic L-function for the elliptic curve $E^{(K)}$.

Lemma 4.23. *We have* $L^{\bullet\bullet}|_{t_{anti}=0} = L^{\bullet}L^{\bullet}_K$.

Proof. For ease of notation in the proof, we write restrictions of two-variable p-adic L-functions to the cyclotomic line as evaluated at the cyclotomic variable Z, so e.g. $L^{\bullet\bullet}(Z)$ instead of $L^{\bullet\bullet}|_{t_{anti}=0}$. From [2, Theorem C and the discussion at the end of the introduction], we have

$$L_{\alpha\alpha}(Z) = L_\alpha(Z)L^{(K)}_\alpha(Z) \text{ and } L_{\beta\beta}(Z) = L_\beta(Z)L^{(K)}_\beta(Z),$$

where $L^{(K)}_*$ is the L-function of the quadratic twist of E by K. Following [64, Definition 6.8], we let

$$\begin{pmatrix} \log^\sharp_\alpha(1+Z) & \log^\sharp_\beta(1+Z) \\ \log^\flat_\alpha(1+Z) & \log^\flat_\beta(1+Z) \end{pmatrix} := \mathcal{L}og(Z).$$

We know that

$$\begin{pmatrix} L_\alpha \\ L_\beta \end{pmatrix} = \mathcal{L}og^T \begin{pmatrix} L^\sharp \\ L^\flat \end{pmatrix}$$

and

$$\left(L^{(K)}_\alpha, L^{(K)}_\beta\right) = (L^\sharp_K, L^\flat_K)\mathcal{L}og,$$

so that

[16] For the case $a_p = 0$, see [74, Prop. 4.8].

$$\begin{aligned} L_\alpha L_\alpha^{(K)} &= (\log_\alpha^\sharp L^\sharp + \log_\alpha^\flat L^\flat)(\log_\alpha^\sharp L_K^\sharp + \log_\alpha^\flat L_K^\flat) \\ &= (\log_\alpha^\sharp)^2 L^\sharp L_K^\sharp + \log_\alpha^\sharp \log_\alpha^\flat (L^\sharp L_K^\flat + L^\flat L_K^\sharp) + (\log_\alpha^\flat)^2 L^\flat L_K^\flat. \end{aligned}$$

But restricting $\begin{pmatrix} L_{\alpha\alpha} & L_{\beta\alpha} \\ L_{\alpha\beta} & L_{\beta\beta} \end{pmatrix} = \mathcal{L}og(Y)^T \begin{pmatrix} L^{\sharp\sharp} & L^{\flat\sharp} \\ L^{\sharp\flat} & L^{\flat\flat} \end{pmatrix} \mathcal{L}og(X)$ to the cyclotomic line yields

$$\begin{aligned} L_{\alpha\alpha}(Z) = (\log_\alpha^\sharp(1+Z))^2 L^{\sharp\sharp}(Z) + \log_\alpha^\sharp(1+Z)\log_\alpha^\flat(1+Z)\left(L^{\sharp\flat}(Z) + L^{\flat\sharp}(Z)\right) \\ + (\log_\alpha^\flat(1+Z))^2 L^{\flat\flat}(Z). \end{aligned}$$

If we knew that $(\log_\alpha^\sharp(1+Z))^2, \log_\alpha^\sharp(1+Z)\log_\alpha^\flat(1+Z)$, and $(\log_\alpha^\flat(1+Z))^2$ are $\mathbb{Z}_p[[Z]]$-linearly independent, the claim would follow.

Note first that $\log_\alpha^\sharp(1+Z)$ and $\log_\alpha^\flat(1+Z)$ have at most finitely many common zeros: A common zero ζ satisfies $\det \mathcal{L}og(\zeta) = 0$, so ζ would be a p-power cyclotomic zero by [66, Remark 4.4]. But $L_\alpha(Z) = \log_\alpha^\sharp(1+Z)L^\sharp(Z) + \log_\alpha^\flat(1+Z)L^\flat(Z)$ has only finitely many p-power cyclotomic zeros by [58, page 1].

Since $(\log_\alpha^\sharp(1+Z))$ and $(\log_\alpha^\flat(1+Z))$ have infinitely many zeros, we conclude that any $\mathbb{Z}_p[[Z]]$-multiple of $(\log_\alpha^\sharp(1+Z))^2$ is $\mathbb{Z}_p[[Z]]$-linearly independent from $\log_\alpha^\sharp(1+Z)\log_\alpha^\flat(1+Z)$ and $(\log_\alpha^\flat(1+Z))^2$, and can make the analogous claim for $(\log_\alpha^\flat(1+Z))^2$. To see that any $\mathbb{Z}_p[[Z]]$-multiple of $\log_\alpha^\sharp(1+Z)\log_\alpha^\flat(1+Z)$ is independent from the other two, note that no $\mathbb{Z}_p[[Z]]$-linear combination of $(\log_\alpha^\sharp(1+Z))^2$ and $(\log_\alpha^\flat(1+Z))^2$ can vanish at all the infinitely many zeros of $\log_\alpha^\sharp(1+Z)\log_\alpha^\flat(1+Z)$. □

Remark 4.24. A. Lei announced a different proof of Lemma 4.23 in [36].

Proposition 4.25. *Under the assumptions of Propositions 4.20 and 4.21, we have*

$$\mathrm{Char}(\mathcal{X}^\bullet)\,\mathrm{Char}(\mathcal{X}_K^\bullet) \subseteq (L^\bullet L_K^\bullet).$$

Proof. The left hand side is the Λ-characteristic ideal of $\mathcal{X}^{\bullet\bullet}/(t_{anti})$ by Proposition 4.6.

Correspondingly for the right hand-side, we have $L^{\bullet\bullet}|_{t_{anti}=0} = L^\bullet L_K^\bullet$ by the above Lemma 4.23. We prove the inequality prime by prime.

For primes $\mathfrak{L}$ in Λ_K coprime to a or H, Proposition 4.20 tells us that

$$\mathrm{ord}_\mathfrak{L}\,\mathrm{Char}(\mathcal{X}^{\bullet\bullet}) \geqslant \mathrm{ord}_\mathfrak{L}(L^{\bullet\bullet}).$$

For prime factors $\mathfrak{L} \neq (p)$ of a, we have

$$\mathrm{ord}_\mathfrak{L}\,\mathrm{Char}(\mathcal{X}^{\bullet\bullet}) \geqslant 0 = \mathrm{ord}_\mathfrak{L}(L^{\bullet\bullet})$$

by integrality of $\mathrm{Char}(\mathcal{X}^{\bullet\bullet})$ and Proposition 4.21. For prime factors $\mathfrak{L} \neq (p)$ of H, we have similarly

$$\operatorname{ord}_{\mathfrak{L}} \operatorname{Char}(\mathcal{X}^{\bullet\bullet}) \geqslant \operatorname{ord}_{\mathfrak{L}}(L^{\bullet\bullet}) + \operatorname{ord}_{\mathfrak{L}}\left(\frac{1}{H}\right) \geqslant \operatorname{ord}_{\mathfrak{L}}(L^{\bullet\bullet}).$$

By the choice of $\bullet$, only the above $\mathfrak{L}$ contribute to prime factors different from p upon restricting to $t_{anti} = 0$, so all that is left to prove is the p-part of the proposition.

First note that since $\operatorname{Char}(\mathcal{X}^{\bullet\bullet})$ is an integral Λ_K-ideal, $\operatorname{ord}_p \operatorname{Char}(\mathcal{X}^{\bullet\bullet}) \geqslant 0$. We also know from Proposition 4.20 that $\operatorname{ord}_p \operatorname{Char}(\mathcal{X}^{\bullet\bullet}) \geqslant \operatorname{ord}_p(\frac{1}{aH}) + \operatorname{ord}_p(L^{\bullet\bullet})$. Putting these and Proposition 4.21 together yields

$$\operatorname{ord}_p \operatorname{Char}(\mathcal{X}^{\bullet\bullet}) \geqslant \max\left(0, \operatorname{ord}_p \frac{1}{aH}\right). \tag{a}$$

Until the end of the proof, we let all sums be over the height one prime ideals $\mathfrak{P}$ in Λ_K for which $v_{\mathfrak{P}} := \operatorname{ord}_p(\mathfrak{P}|_{t_{anti}=0}) > \operatorname{ord}_p(\mathfrak{P})$. From Proposition 4.20, we know

$$\sum_{\mathfrak{P}} v_{\mathfrak{P}} \cdot \operatorname{ord}_{\mathfrak{P}} \operatorname{Char}(\mathcal{X}^{\bullet\bullet}) \geqslant \sum_{\mathfrak{P}} v_{\mathfrak{P}} \cdot \operatorname{ord}_{\mathfrak{P}} L^{\bullet\bullet}. \tag{b}$$

From Proposition 4.21,

$$\operatorname{ord}_p(L^{\bullet} L_K^{\bullet}) = \operatorname{ord}_p L^{\bullet\bullet} + \sum_{\mathfrak{P}} v_{\mathfrak{P}} \cdot \operatorname{ord}_{\mathfrak{P}} L^{\bullet\bullet} = \sum_{\mathfrak{P}} v_{\mathfrak{P}} \cdot \operatorname{ord}_{\mathfrak{P}} L^{\bullet\bullet}. \tag{c}$$

Putting the above (a), (b), and (c) together, we obtain

$$\begin{aligned} \operatorname{ord}_p \operatorname{Char}(\mathcal{X}^{\bullet}) \operatorname{Char}(\mathcal{X}_K^{\bullet}) &= \operatorname{ord}_p \operatorname{Char}(\mathcal{X}^{\bullet\bullet}) + \sum_{\mathfrak{P}} v_{\mathfrak{P}} \cdot \operatorname{ord}_{\mathfrak{P}} \operatorname{Char}(\mathcal{X}^{\bullet\bullet}) \\ &\geqslant \max(0, \operatorname{ord}_p \frac{1}{aH}) + \sum_{\mathfrak{P}} v_{\mathfrak{P}} \cdot \operatorname{ord}_{\mathfrak{P}} L^{\bullet\bullet} \\ &\geqslant \operatorname{ord}_p(L^{\bullet} L_K^{\bullet}). \quad \square \end{aligned}$$

5. Conclusion

We have now assembled all the ingredients to prove our main theorem.

Theorem 5.1. *Let $E/\mathbb{Q}$ be an elliptic curve and $p > 2$ a prime of supersingular reduction. Assume that E has square-free conductor and also that Conjecture 3.33 holds. Choose $\bullet \in \{\sharp, \flat\}$ so that $L^{\bullet} \neq 0$. Then $L^{\bullet}$ is a characteristic power series of the Iwasawa module $\operatorname{Hom}(\operatorname{Sel}^{\bullet}(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$.*

Proof. From [64, Theorem 7.16], we know that $\operatorname{Char}(\mathcal{X}^{\bullet}) \supseteq (L^{\bullet})$ if $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ surjects onto $\operatorname{Aut} E[p]$. But this surjectivity assumption can be replaced by the pair of assumption that $E[p]$ be irreducible and ramified at a prime $q||N$ different from p, as explained in [62, discussion after Theorem 2.5.2].

This pair of assumptions is indeed satisfied: The irreducibility was originally proved by Fontaine. (For a statement of the theorem, see [14, Theorem 2.6], and for the proof, see [14, Section 6.8].) Since N is square-free, Ribet's level-lowering theorem [57, Theorem 8.2] implies that $E[p]$ ramifies at some prime $q|N$.

We now choose our K so that similarly $E^{(K)}[p]$ ramifies at q, so that $\mathrm{Char}(\mathcal{X}_K^\bullet) \supseteq (L_K^\bullet)$. We can further choose our auxiliary K so that it satisfies Choice 3.12 and the assumptions for Proposition 4.21.[17] All this only inflicts congruence conditions on the choice of K, so that we can choose K so that Proposition 4.25 holds. With such a choice, we can combine the pair of inclusions $\mathrm{Char}(\mathcal{X}^\bullet) \supseteq (L^\bullet)$ and $\mathrm{Char}(\mathcal{X}_K^\bullet) \supseteq (L_K^\bullet)$ with the conclusion of Proposition 4.25 that $\mathrm{Char}(\mathcal{X}^\bullet)\,\mathrm{Char}(\mathcal{X}_K^\bullet) = (L^\bullet)(L_K^\bullet)$ to conclude $\mathrm{Char}(\mathcal{X}^\bullet) = (L^\bullet)$. □

5.1. Proof of the Birch and Swinnerton-Dyer formula at p in the rank 1 case

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

Theorem 5.2. *(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 $\mathrm{ord}_{s=1} L(E,s) = 1$ and assume Conjecture 3.33 holds. Then

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

Proof. The Iwasawa main conjecture is the only missing ingredient in the discussion of [33, Proof of Corollary 1.3]. □

Theorem 5.3. *(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 $L(E,1) \neq 0$ and assume also Conjecture 3.33 holds. Then

$$\left|\frac{L(E,1)}{\Omega}\right|_p = \left|Ш(E/\mathbb{Q})\prod_l c_l\right|_p,$$

Here, $Ш(E/\mathbb{Q})$ is the Tate–Shafarevich group of $E/\mathbb{Q}$, c_l are the Tamagawa numbers, and Ω 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 [63, Theorem 3.35], this gives the leading term formula up to powers of 2 and bad primes.

[17] e.g. so that p and all prime divisors of N different from q split while q is inert.

5.2. Proof of the Birch and Swinnerton-Dyer formula at p in the rank 0 case

We now prove Theorem 5.3. Recall that the main assumptions are that $L(E,1) \neq 0$ and that Conjecture 3.33 holds. In view of the first assumption, the $\sharp$ and $\flat$ Selmer groups from [64, Definition 7.11] are both finitely generated cotorsion $\mathbb{Z}_p[[X]]$-modules, cf. [64, Theorem 7.14]. We thus are not confined to a particular choice (for which we previously reserved the symbol $\bullet$) and let $\star$ denote either $\sharp$ or $\flat$ in this final subsection. We now define $\mathrm{Col}_p^\sharp$ and $\mathrm{Col}_p^\flat$ to be the component of the trivial tame character of the maps appearing in [64, Definition 7.1], i.e. in the notation of [64], these would be $\varepsilon_\eta \mathrm{Col}^\sharp$ and $\varepsilon_\eta \mathrm{Col}^\flat$ for η the trivial character. (We add the subscript p to distinguish them from the maps appearing in Proposition 4.5). These are the Coleman maps in the one-variable $\mathbb{Q}$-cyclotomic case which can also be obtained by proceeding as in Definition 3.22 by ignoring the unramified tower indexed by m. We denote by $E^\sharp_{\infty,p}$ (resp. $E_{\infty,p}$) the exact annihilator of $\ker \mathrm{Col}_p^\sharp$ (resp. $\ker \mathrm{Col}_p^\flat$) under the local Tate pairing, cf. [64, Definition 7.9]. Similarly, we let $E^\sharp_{0,p}$ (resp. $E^\flat_{0,p}$) be the exact annihilator of $\ker \mathrm{Col}^\sharp_{p,0}$ resp. $\ker \mathrm{Col}^\flat_{p,0}$. See [64, Definition 7.2].[18] Note that $E^\sharp_{0,p} = E^\flat_{0,p} = E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. This is because the pair of maps $(\mathrm{Col}_p^\sharp, \mathrm{Col}_p^\flat)$ (thought of as a vector) is constructed as an inverse limit of *one* map at every finite layer of the cyclotomic tower. However, this map splits at level infinity and at level $n = 0$, cf. [64, Proposition 5.7] and [64, Definition 7.2 and the preceding discussion]. Thus our description follows from [65, Proposition 4.7].

We let

$$\mathcal{G}^\star(\mathbb{Q}_n) = \mathrm{Im}\left(H^1(\mathbb{Q}_n, E[p^\infty]) \longrightarrow \frac{H^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E^\star_{n,p}} \times \prod_{v \neq p} \frac{H^1(\mathbb{Q}_{n,v}, E[p^\infty])}{E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

for $n = 0$ or $n = \infty$ and $\star \in \{\sharp, \flat\}$. We denote $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ by Γ.

Remark 5.4. Since the analytic rank is 0, we have that $L^\sharp(0) \neq 0 \neq L^\flat(0)$, and $\mathcal{X}^\sharp$ and $\mathcal{X}^\flat$ are both Λ-torsion, by [64, Theorem 7.14]

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

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

For convenience, we let

$$\mathcal{P}_E(\mathbb{Q}_n) := \frac{H^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E^\star_{n,p}} \times \prod_{v \neq p} \frac{H^1(\mathbb{Q}_{n,v}, E[p^\infty])}{E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \text{ for } n = 0 \text{ or } n = \infty.$$

[18] The maps $\mathrm{Col}_{p,0}$ are denoted simply by Col_0 in [64].

We denote the map $\mathcal{P}_E(\mathbb{Q}_0) \longrightarrow \mathcal{P}_E(\mathbb{Q}_\infty)$ by r.

Lemma 5.5. *Denote by $E(\mathbb{Q})_p$ the p-primary torsion points of $E(\mathbb{Q})$. Also denote by $c_l^{(p)}$ the p-component of the Tamagawa number c_l for a prime l at which E has bad reduction. That is, we put $c_l := [E(\mathbb{Q}_l) : E_0(\mathbb{Q}_l)]$, where $E_0(\mathbb{Q}_l)$ denotes the subgroup of points of nonsingular reduction modulo the bad prime l, and $c_l^{(p)}$ is the highest power of p dividing c_l. Assume $(\mathrm{Sel}^\star(E,\mathbb{Q}_\infty))_{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}$ is finite. We then have*

$$\frac{1}{\left|(\mathrm{Sel}^\star(E,\mathbb{Q}_\infty))_{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}\right|} = \frac{\prod_{l \ bad} c_l^{(p)}}{\#E(\mathbb{Q})_p} \times \frac{1}{|\ker g|}.$$

Proof. The lemma with the Tamagawa factors "$\prod_{l \text{ bad}} c_l^{(p)}$" replaced with "$|\ker(r)|$" follows from the proof of [18, 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 [18, Proof of Lemma 3.3].

If $v = l$ is a bad reduction prime, [18, discussion after 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 [18, Lemma 3.4] do not apply since ordinarity is a key assumption there.) We want to show that the map

$$\frac{H^1(\mathbb{Q}_p, E[p^\infty])}{E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \xrightarrow{r_p} \frac{H^1(\mathbb{Q}_{p,\infty}, E[p^\infty])}{E^\sharp_{\infty,p}}$$

is injective.

As in [32, Proof of Proposition 9.2], we consider the following commutative diagram with exact sequences, were X is the cyclotomic variable:

$$\begin{array}{ccccccc} & & \frac{\ker \mathrm{Col}_p^\star}{X} & \longrightarrow & \frac{\mathbb{H}^1_{\mathrm{Iw}}}{X} & \longrightarrow & \frac{\left(\mathbb{H}^1_{\mathrm{Iw}}/\ker \mathrm{Col}_p^\star\right)}{X} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \ker \mathrm{Col}^\star_{p,0} & \longrightarrow & H^1(k_0,T) & \longrightarrow & \frac{H^1(k_0,T)}{\ker \mathrm{Col}^\star_{p,0}}, \end{array}$$

where $\mathbb{H}^1_{\mathrm{Iw}} = \varprojlim_n H^1(\mathbb{Q}_{p,n}, T)$.

By construction, the right vertical map is an isomorphism. The middle vertical map is a surjection by [64, 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. □

We let $\mathcal{X}_0^\star = \mathrm{Hom}(\mathrm{Sel}^\star(E,\mathbb{Q}),\mathbb{Q}_p/\mathbb{Z}_p)$. Note that by the discussions at the beginning of the subsection, we have $E_{0,p}^\sharp = E_{0,p}^\flat = E(\mathbb{Q}_p)\otimes\mathbb{Q}_p/\mathbb{Z}_p$. Let

$$\mathcal{X}_0 := \mathrm{Hom}(\mathrm{Sel}(E,\mathbb{Q}),\mathbb{Q}_p/\mathbb{Z}_p).$$

Then $\mathcal{X}_0^\star = \mathcal{X}_0$.

Lemma 5.6. *(Small Control Theorem) The natural morphism $\mathcal{X}^\star/X\mathcal{X}^\star \longrightarrow \mathcal{X}_0^\star/X\mathcal{X}_0^\star = \mathcal{X}_0$ is surjective and has finite kernel.*

Proof. The proof of [32, Theorem 9.3] with $n=0$ with the adjustment that r_p is injective (cf. Lemma 5.5) works. (Note that in [32, 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 $\prod_v \mathscr{H}^+(K_{n,v})$.) □

Lemma 5.7. $\mathrm{Sel}^\star(E,\mathbb{Q}_\infty)^{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}$ *is finite if $L(E,1)\neq 0$.*

Proof. It suffices to prove that $\mathcal{X}^\star/X\mathcal{X}^\star$ is finite. This follows from the small control theorem (i.e. Lemma 5.6) above, which implies that $\mathcal{X}^\star/X\mathcal{X}^\star$ is finite if and only if $\mathcal{X}_0^\star/X\mathcal{X}_0^\star$ is. $\mathcal{X}_0^\star/X\mathcal{X}_0^\star = \mathcal{X}_0$ being finite is automatic by our assumption. One can also show that $\mathcal{X}^\star/X\mathcal{X}^\star$ is finite directly by observing that $L(E,1)\neq 0$ implies that $f^\star(0)\neq 0$ using [64, table before Proposition 6.14]. □

Lemma 5.8. *We have*

$$\left|\mathrm{Sel}^\star(E,\mathbb{Q}_\infty)^{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}\right| = \frac{|\mathrm{Sel}(E,\mathbb{Q})|}{\#E(\mathbb{Q})_p}\times|\ker g|\,.$$

Proof. The proof of [17, Lemma 4.3] with "Sel" replaced by "Sel*" works, taking into account Lemma 5.7. □

Lemma 5.9. *Let $f^\star$ be a generator of the characteristic ideal of $\mathcal{X}^\star$ and assume that $\mathrm{Sel}^\star(E,\mathbb{Q}_\infty)^{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}$ is finite. Then*

$$|f(0)|_p = \frac{\left|\mathrm{Sel}^\star(E,\mathbb{Q}_\infty)^{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}\right|}{\left|(\mathrm{Sel}^\star(E,\mathbb{Q}_\infty))_{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}\right|}.$$

Proof. This is a general fact about finitely generated Λ-modules, using the assumption that $\mathrm{Sel}^\star(E,\mathbb{Q}_\infty)^{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}$ is finite, which Lemma 5.7 guarantees. See [18, Lemma 4.2], which implies that $(\mathrm{Sel}^\star(E,\mathbb{Q}_\infty))_{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})}$ is finite in this case. □

Proof of Theorem 5.3. The theorem now follows using Lemma 5.9 and multiplying the terms in Lemma 5.8 and Lemma 5.5, 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 Ш then follows from [34, Sledstvie 2]. □

Acknowledgments

We are very grateful to Xin Wan for explicitly making several very pessimistic comments about the feasibility of the $a_p \neq 0$ case after a seminar run by Shouwu Zhang, for patiently answering questions during the preparation of our manuscript, and for asking numerous questions once an earlier version was up on the arxiv. We would also like to thank referee#1, who made numerous helpful suggestions and corrections that greatly improved the paper. (More acknowledgments to be added later.) Our thanks also go to Masataka Chida, Dorian Goldfeld, Jeff Hoffstein, Alex Kontorovich, Antonio Lei, Masato Kurihara, Yuichi Hirano, Tadashi Ochiai, Joseph Silverman, and Wei Zhang for their comments on an earlier version and answering some questions. We thank Shuai Zhai for generously providing us with the examples found in the appendix. We thank M for a helpful SAGE code. We also thank Richard Taylor who suggested doing a small seminar on this topic. We thank John Coates (1945–2022) for a remark that led us to study a work by Zhihuan Wang (688–742), inspiring the main idea of this paper. Finally, we thank all the referees for their time and their valuable suggestions for improvements, and anybody else who deserves to be thanked.

Appendix A. Numerical examples and infinite families of elliptic curves satisfying the full Birch and Swinnerton-Dyer conjecture

A corollary to our main theorem and its corollaries are:

Corollary A.1. *(Assume Conjecture 3.33 holds.) The elliptic curve $y^2+y = x^3-x$ studied by Mordell[19] in [48] satisfies the full BSD conjecture.*

Proof. The analytic rank is one (cf. [37, label 37.a1]), and the BSD formula is already known computationally (see e.g. [46,19] for computer-assisted verification for all curves of conductor less than 1000, and for 16714 of the 16725 such curves of conductor less than 5000). Theoretically, it is only outstanding at the supersingular primes $p = 2$ and $p = 3$, since $a_2 = -2$ and $a_3 = -3$. Corollary 1.3 removes the assumption at $p = 3$, (and we expect the techniques in this paper can be generalized to handle $a_2 = -2$ as well). Thus, the BSD formula stands *up to powers of the single prime* 2. It is enough to confirm that

$$\frac{1}{2} < \frac{L'(E,1)\#E(\mathbb{Q})^2_{\mathrm{tor}}}{\mathrm{Reg}(E/\mathbb{Q})\Omega\#Ш(E/\mathbb{Q})\prod_l c_l} < 2,$$

for which the computations only have to be accurate to the first leading digit.[20] □

[19] How many products of two consecutive numbers are products of three consecutive numbers?

[20] The approximations $L'(E,1) = 0.305999773834, \mathrm{Reg}(E/\mathbb{Q}) = 0.05111140824, \Omega = 5.98691729246$ from [37] also suffice.

An example of an elliptic curve with $a_3 = 3$ which is outside the scope of computation of [46,19] for which the Birch and Swinnerton-Dyer formula has non-trivial 3-valuation is the curve given by $y^2 = x^3 - 21904x - 810448$.

There are only finitely many elliptic curves with $a_3 = \pm 3$ for which the full BSD conjecture is known to hold [46,19]. By contrast for $a_3 = \pm 2, \pm 1$ or 0, there exist infinitely many: Li, Liu and Tian in [39] have found infinite families of CM elliptic curves satisfying full BSD (building on their breakthroughs on the 2-part.) Note that when E has CM, we can't have $a_3 = \pm 3$ [61, Exercise 2.30]. Wan has found infinitely many non-CM elliptic curves in [74] (still assuming $a_3 \in \{\pm 2, \pm 1, 0\}$) building on work of Cai, Li, and Zhai who exhibit an infinite number of quadratic twists at which the 2-part of BSD holds.

We generalize Wan's theorem to give a criterion for the existence of infinite families of elliptic curves (with $a_3 = \pm 3$ allowed) which satisfy full BSD.

Corollary A.2. *(Assume Conjecture 3.33 holds.) Let E be a semistable elliptic curve over $\mathbb{Q}$. Assume that for $l \neq 2$, $E[l]$ is absolutely irreducible as an $\mathbb{F}_l$-representation of $G_{\mathbb{Q}}$ and ramified at some prime $q \neq l$ of multiplicative reduction, and q is not the only multiplicative prime.*

Let M be a product of distinct good ordinary primes. Then if

(**) the 2-part of BSD holds for the Mth quadratic twist $E^{(M)}$ of E and $L(E^{(M)}, 1) \neq 0$,

the full BSD formula holds for $E^{(M)}$.

The condition (**) can be verified thanks to the recent work of Cai, Li, and Zhai for a(n infinite) number of elliptic curves. We are grateful to Shuai Zhai for providing us with explicit examples of such elliptic curves with $a_3 = \pm 3$ that satisfy the full Birch and Swinnerton-Dyer conjecture. Here is one of them:

Example A.3. (Quadratic twists of 170E1)

The curve E given by $y^2 + xy = x^3 - x^2 - 10x - 10$ has $a_3 = 3$ and satisfies the conditions for Corollary A.2. The Cai-Li-Zhai condition (**) is satisfied for $M = q_1 q_2 \cdots q_r$ for products of r distinct primes q_i in the infinite set $\mathcal{S}$ below so that the bad primes of E — 2, 5, and 17 — all split in $\mathbb{Q}(\sqrt{M})$ and $M \equiv 1 \mod 4$.

$\mathcal{S} = \{$ primes $q \neq 3$ so that a_q is odd, E has good reduction at q, and q is inert[21] in $\mathbb{Q}(\theta)\}$

$= \{13, 19, 29, 31, 47, 53, 59, 61, 71, 73, 89, 97, 109, 113, 127, 199, 223, 227, 233, 263, \dots\}$

There are infinitely many such M, of which the first few possibilities are 89, 281, 409, 569, 689 $= 13 \cdot 53$, 769, 1121 $= 19 \cdot 59$, 1249, 1361, 1481, 1721, 1769 $= 29 \cdot 61$, 1801, 1889, 2089, 2129, 2161, 2609, 3001. The smallest M which is a product of three primes is $11609 = 13 \cdot 19 \cdot 47$.

[21] θ is a root of a 2-division polynomial of E.

We can now prove the following theorem:

Theorem A.4. *(Assume Conjecture 3.33 holds.) Let E be a semistable elliptic curve over $\mathbb{Q}$. Assume that for $l \neq 2$, $E[l]$ is absolutely irreducible as an $\mathbb{F}_l$-representation of $G_{\mathbb{Q}}$ and ramified at some prime $q \neq l$ of multiplicative reduction, and q is not the only multiplicative prime.*

Let M be a product of distinct good ordinary primes. Then if

(**) the 2-part of BSD holds for $E^{(M)}$ of E and $L(E^{(M)}, 1) \neq 0$,
the full BSD formula holds for $E^{(M)}$, where $E^{(M)}$ is the Mth quadratic twist.

Proof. This follows from [74, Theorem 5.3] and the main theorem of this paper, which removes the condition $a_3 \neq \pm 3$.

We are grateful to Shuai Zhai for finding all elliptic curves with conductor less than 604 for which one can construct infinite families of quadratic twists of elliptic curves with $a_3 = \pm 3$ satisfying full BSD analogously to the example above involving $170E1$.

Example A.5. Infinitely many quadratic twists of the following elliptic curves with $a_3 = \pm 3$ satisfy the full Birch and Swinnerton-Dyer conjecture: 170E1, 182D1, 182E1, 323A1, 434E1, 602C1, 142E1, 574E1.

References

[1] Y. Amice, J. Vélu, Distributions p-adiques associées aux séries de Hecke, in: Journées Arithmétiques de Bordeaux, Bordeaux, 1974, in: Astérisque, vol. 24–25, Société Mathématique de France, Montrogue, 1975, pp. 119–131.
[2] D. Barrera Salazar, C. Williams, Families of Bianchi modular symbols: critical base-change p-adic L-functions and p-adic Artin formalism, Sel. Math. 27 (82) (2021) 1–45 (with an appendix by C. Wang-Erickson).
[3] L. Berger, H. Li, H.J. Zhu, Construction of some families of 2-dimensional crystalline representations, Math. Ann. 329 (2) (2004) 365–377.
[4] D. Bump, S. Friedberg, J. Hoffstein, Nonvanishing theorems for L-functions of modular forms and their derivatives, Invent. Math. 102 (3) (1990) 543–618.
[5] K. Büyükboduk, A. Lei, Iwasawa theory of elliptic modular forms over imaginary quadratic fields at non-ordinary primes, Int. Math. Res. Not. 2021 (14) (2021) 10654–10730, https://doi.org/10.1093/imrn/rnz117, arXiv:1605.05310.
[6] K. Büyükboduk, A. Lei, G. Venkat, Iwasawa theory for symmetric squares of p-non-ordinary eigenforms, Doc. Math. 26 (2021) 1–63, https://arxiv.org/pdf/1807.11517.pdf.
[7] K. Büyükboduk, A. Lei, D. Loeffler, G. Venkat, Iwasawa theory for Rankin-Selberg Products of p-non-ordinary eigenforms, Algebra Number Theory 13 (4) (2019) 901–941, arXiv:1802.04419.
[8] M. Bhargava, A. Shankar, Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0, Ann. Math. 181 (2) (2015) 587–621.
[9] 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.
[10] L. Cai, C. Li, S. Zhai, On the 2-part of the Birch and Swinnerton-Dyer Conjecture for quadratic twists of elliptic curves, J. Lond. Math. Soc. 101 (2) (2020) 714–734, https://doi.org/10.1112/jlms.12284, https://arxiv.org/pdf/1712.01271.pdf.
[11] F. Castella, Z. Liu, X. Wan, Iwasawa–Greenberg Main Conjectures for non-ordinary modular forms and Eisenstein congruences on $GU(3,1)$, Forum Math. Sigma 10 (2022) e110.

[12] F. Castella, M. Ciperiani, S. Skinner, F. Sprung, Iwasawa main conjectures for modular forms of weight two, on arxiv.
[13] G. Chinta, S. Friedberg, J. Hoffstein, Dirichlet Series and Automorphic Forms, Proc. Sympos. Pure Math., vol. 75, Amer. Math. Soc., Providence, RI, 2006, pp. 3–41.
[14] B. Edixhoven, The weight in Serre's conjectures on modular forms, Invent. Math. 109 (1) (1992) 563–594.
[15] E. Eischen, X. Wan, p-adic Eisenstein series and L-functions of certain cusp forms on definite unitary goups, J. Inst. Math. Jussieu 15 (3) (2016) 471–510, https://doi.org/10.1017/S1474748014000395.
[16] J-M. Fontaine, Le corps des périodes p-adiques, in: Périodes p-adiques, Bures-sur-Yvette, 1988, Astérisque 223 (1994) 59–111.
[17] R. Greenberg, Iwasawa theory for elliptic curves, in: C. Viola (Ed.), Arithmetic Theory of Elliptic Curves. Lectures from the 3rd C.I.M.E. Session Held in Cetraro, July 12–19, 1997, in: Lecture Notes in Mathematics, vol. 1716, Springer-Verlag/Centro Internazionale Matematico Estivo (C.I.M.E.), Berlin/Florence, 1999, pp. 51–144.
[18] R. Greenberg, Iwasawa theory and p-adic deformations of motives, in: Motives, Seattle, WA, 1991, in: Proc. Sympos. Pure Math., vol. 55, Part 2, Amer. Math. Soc., Providence, RI, 1994, pp. 19–223.
[19] G. Grigorov, A. Jorza, S. Patrikis, W.A. Stein, C. Tarnita, Computational verification of the Birch and Swinnerton-Dyer Conjecture for individual ellioptic curves, Math. Comput. 78 (268) (October 2009) 2397–2425.
[20] S. Haran, p-adic L-functions for modular forms, Compos. Math. 62 (1) (1987) 31–46.
[21] H. Hida, J. Tilouine, Anti-cyclotomic Katz p-adic L-functions and congruence modules, Ann. Sci. Éc. Norm. Supér. (4) 26 (2) (1993) 189–259.
[22] B. Howard, The Heegner point Kolyvagin system, Compos. Math. 141 (6) (2004) 1439–1472.
[23] H. Iwaniec, On the order of vanishing of modular L-functions at the critical point, Sém. Théor. Nombres Bordeaux (2) 2 (2) (1990) 365–376.
[24] D. Jetchev, C. Skinner, X. Wan, The Birch-Swinnerton-Dyer formula for elliptic curves of analytic rank one, Camb. J. Math. 5 (3) (2017) 369–434.
[25] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, Astérisque 295 (2004) 117–290.
[26] N. Katz, p-adic L-functions for CM fields, Invent. Math. 49 (1978) 199–297.
[27] B.D. Kim, The parity conjecture for elliptic curves at supersingular reduction primes, Compos. Math. 143 (2007) 47–72.
[28] B.D. Kim, $\pm/\pm$ Selmer groups over the maximal $\mathbb{Z}_p^2$-extension of an imaginary quadratic field, Can. J. Math. 66 (4) (2014) 826–843.
[29] C.H. Kim, Anticyclotomic Iwasawa invariants and congruences of modular forms, Asian J. Math. 21 (3) (June 2017) 499–530.
[30] G. Kings, D. Loeffler, S.L. Zerbes, Rankin-Eisenstein classes and explicit reciprocity laws, Camb. J. Math. 5 (1) (2017) 1–122, http://arxiv.org/abs/1501.03289.
[31] G. Kings, D. Loeffler, S.L. Zerbes, Rankin–Eisenstein classes for modular forms, Am. J. Math. 142 (1) (2020) 79–138.
[32] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, Invent. Math. 152 (1) (2003) 1–36.
[33] S. Kobayashi, The p-adic Gross-Zagier formula at supersingular primes, Invent. Math. 191 (3) (2013) 527–629.
[34] V. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and Ш$(E, \mathbb{Q})$ for a subclass of Weil curves, Izv. Akad. Nauk SSSR, Ser. Mat. 52 (3) (1989) 522–540, 670–671.
[35] A. Lei, Factorisation of two-variable p-adic L-functions, Can. Math. Bull. 57 (4) (2014) 845–852.
[36] A. Lei, Artin formalism for p-adic L-functions of modular forms at non-ordinary primes, available at https://arxiv.org/pdf/2404.01835.
[37] The L-functions and modular forms database, http://www.lmfdb.org/EllipticCurve/Q/.
[38] A. Lei, D. Loeffler, S. Zerbes, Euler systems for Rankin–Selberg convolutions of modular forms, Ann. Math. 180 (2) (2014) 653–771.
[39] Y. Li, Y. Liu, Y. Tian, The Birch and Swinnerton-Dyer Conjecture for CM Elliptic Curves over $\mathbb{Q}$, preprint, 2017.
[40] D. Loeffler, S. Zerbes, Rankin–Eisenstein classes in Coleman families, Res. Math. Sci. 3 (2016) 26, http://arxiv.org/abs/1506.06703.
[41] D. Loeffler, S. Zerbes, Iwasawa theory and p-adic L-functions over $\mathbb{Z}_p^2$-extensions, Int. J. Number Theory 10 (8) (2014) 2045–2095.

[42] D. Loeffler, p-adic integration on ray class groups and non-ordinary p-adic L-functions, in: Iwasawa Theory 2012, in: Contributions in Mathematical and Computational Sciences, vol. 7, 2014, pp. 357–378.
[43] Ju. Manin, Periods of Parabolic Forms and p-adic Hecke series, Sbornik 21 (3) (1973).
[44] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Invent. Math. 18 (1972) 183–266.
[45] B. Mazur, J. Tate, J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math. 84 (1986) 1–48.
[46] R. Miller, Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one, LMS J. Comput. Math. 14 (November 2011) 327–350.
[47] B. Mazur, P. Swinnerton-Dyer, Arithmetic of Weil curves, Invent. Math. 25 (1974) 1–61.
[48] L. Mordell, On the integer solutions of $y(y+1) = x(x+1)(x+2)$, Pac. J. Math. 13 (1963) 1347–1351.
[49] M.R. Murty, V. Kumar Murty, Mean values of derivatives of modular L-series, Ann. Math. (2) 133 (3) (1991) 447–475.
[50] R. Pollack, The p-adic L-function of a modular form at a supersingular prime, Duke Math. J. 118 (3) (2003) 523–558.
[51] B. Perrin-Riou, Théorie d'Iwasawa p-adique loale te globale, Invent. Math. 99 (1990) 247–292.
[52] B. Perrin-Riou, Fonctions L p-adiques des représentations p-adiques, Astérisque 229 (1995).
[53] B. Perrin-Riou, Arithmétique des courbes elliptiques à réduction supersingulière, Exp. Math. 12 (2003) 155–186.
[54] R. Pollack, K. Rubin, The main conjecture for CM elliptic curves at supersingular primes, Ann. Math. 159 (1) (2004) 447–464.
[55] R. Pollack, T. Weston, On anticyclotomic μ-invariants of modular forms, Compos. Math. 147 (5) (2011) 1353–1381.
[56] J. Pottharst, Analytic families of finite-slope Selmer groups, Algebra Number Theory 7 (7) (2013) 1571–1612.
[57] K. Ribet, On modular representations of Gal $\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ arising from modular forms, Invent. Math. 100 (2) (1990) 431–476.
[58] D. Rohrlich, On L-functions of elliptic curves and cyclotomic towers, Invent. Math. 75 (1984) 409–423.
[59] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Invent. Math. 103 (1991) 25–68.
[60] J. Silverman, The Arithmetic of Elliptic Curves, second edition, Graduate Texts in Mathematics, vol. 106, Springer, New York, 2009.
[61] J. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 151, Springer, New York, 1991.
[62] C. Skinner, Multiplicative reduction and the cyclotomic main conjecture for GL_2, Pac. J. Math. 283 (1) (2016) 171–200.
[63] C. Skinner, E. Urban, The Iwasawa main conjectures for GL_2, Invent. Math. 195 (1) (2014) 1–277.
[64] F. Sprung, Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures, J. Number Theory 132 (7) (2012).
[65] F. Sprung, The Šafarevič-Tate group in cyclotomic $\mathbb{Z}_p$-extensions at supersingular prime, J. Reine Angew. Math. 681 (2013) 199–218.
[66] F. Sprung, On pairs of p-adic L-functions of modular forms of weight two, Algebra Number Theory 11 (4) (2017) 885–928.
[67] F. Sprung, The Iwasawa Main Conjecture for elliptic curves at odd supersingular primes, arXiv: 1610.10017.
[68] E. Urban, Nearly overconvergent modular forms, in: Iwasawa Theory 2012, in: Contributions in Mathematical and Computational Sciences, vol. 7, 2014, pp. 401–441.
[69] V. Vatsal, Uniform distribution of Heegner points, Invent. Math. 148 (2002) 1.
[70] M.M. Višik, Nonarchimedean measures associated with Dirichlet series, Mat. Sb. 99(141) (2) (1976) 248–260, 296.
[71] J.-L. Waldspurger, Correspondances de Shimura, in: Proceedings of the International Congress of Mathematicians, Vol. 1, 2, Warsaw, 1983, pp. 525–531.
[72] J.-L. Waldspurger, Quelques propriétés arithmétiques de certaines formes automorphes sur GL(2), Compos. Math. 54 (2) (1985) 121–171.
[73] X. Wan, Iwasawa main conjecture for Rankin–Selbergp-adic L-functions, Algebra Number Theory 14 (2) (2020) 383–483, https://doi.org/10.2140/ant.2020.14.383.

[74] X. Wan, Iwasawa main conjecture for supersingular elliptic curves, https://arxiv.org/pdf/1411.6352v8.pdf.
[75] A. Wiles, The Birch and Swinnerton-Dyer Conjecture, in: The Millenium Prize Problems, in: Clay Mathematical Institute/American Mathematical Society, available at: http://www.claymath.org/library/monographs/MPPc.pdf.