CODIMENSION TWO CYCLES IN IWASAWA THEORY AND ELLIPTIC CURVES WITH SUPERSINGULAR REDUCTION

ANTONIO LEI [1] and BHARATHWAJ PALVANNAN[2]

[1] Département de mathématiques et de statistique, Université Laval, Pavillon Alexandre-Vachon, 1045 avenue de la Médecine, Québec, Canada, G1V 0A6;
email: antonio.lei@mat.ulaval.ca

[2] Department of Mathematics, University of Pennsylvania, 4W1 DRL, 209 South 33rd Street, Philadelphia, 19104-6395, USA;
email: pbharath@math.upenn.edu

Abstract

A result of Bleher, Chinburg, Greenberg, Kakde, Pappas, Sharifi and Taylor has initiated the topic of higher codimension Iwasawa theory. As a generalization of the classical Iwasawa main conjecture, they prove a relationship between analytic objects (a pair of Katz's 2-variable p-adic L-functions) and algebraic objects (two 'everywhere unramified' Iwasawa modules) involving codimension two cycles in a 2-variable Iwasawa algebra. We prove a result by considering the restriction to an imaginary quadratic field K (where an odd prime p splits) of an elliptic curve E, defined over $\mathbb{Q}$, with good supersingular reduction at p. On the analytic side, we consider eight pairs of 2-variable p-adic L-functions in this setup (four of the 2-variable p-adic L-functions have been constructed by Loeffler and a fifth 2-variable p-adic L-function is due to Hida). On the algebraic side, we consider modifications of fine Selmer groups over the $\mathbb{Z}_p^2$-extension of K. We also provide numerical evidence, using algorithms of Pollack, towards a pseudonullity conjecture of Coates–Sujatha.

2010 Mathematics Subject Classification: 11R23 (primary); 11G05, 11G07, 11R34, 11S25 (secondary)

1. Introduction

Fix an odd prime p. Let $\mathcal{R}$ denote a Noetherian, complete, integrally closed, local domain of characteristic zero with Krull dimension $n + 1$ and whose residue field

has characteristic p. To a continuous Galois representation

$$\rho_{d,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_d(\mathcal{R}),$$

satisfying the 'Panchishkin condition', which is a type of 'ordinariness' assumption for Galois deformations introduced in [**14**, Section 4], Greenberg [**14**] has formulated a main conjecture in Iwasawa theory. The Iwasawa main conjecture provides a relation involving codimension one cycles in the divisor group of the ring $\mathcal{R}$, relating a p-adic L-function, satisfying suitable interpolation properties, to a Selmer group. The divisor group, denoted by $Z^1(\mathcal{R})$, is the free abelian group on the set of height 1 prime ideals of the ring $\mathcal{R}$.

One could consider $Z^2(\mathcal{R})$, the free abelian group on the set of height 2 prime ideals of the ring $\mathcal{R}$. Many standard conjectures in Iwasawa theory predict that pseudonull modules are ubiquitous. For example, see Conjecture 3.5 in Greenberg's article [**15**] and Conjecture B in the work of Coates and Sujatha [**10**]. These pseudonull $\mathcal{R}$-modules are supported in codimension at least two. One desirable extension of the Iwasawa main conjecture is an answer to the following question:

QUESTION 1.1. Can we use codimension two cycles from $Z^2(\mathcal{R})$ to associate analytic invariants to pseudonull modules in Iwasawa theory?

The crucial insight in the seven-author paper [**3**], to obtain such an association, is to study a situation when the Galois representation $\rho_{d,n}$ satisfies two distinct Panchishkin conditions. We will use this insight and obtain a result by considering the restriction to an imaginary quadratic field, where an odd prime p splits, of an elliptic curve defined over $\mathbb{Q}$ with good supersingular reduction at p.

Let K denote an imaginary quadratic field where the prime p splits. Let $\mathfrak{p}$ and $\mathfrak{q}$ denote the two prime ideals in K containing p. We fix an isomorphism $i : \overline{\mathbb{Q}}_p \cong \mathbb{C}$ along with embeddings $K \hookrightarrow \overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p \overset{i}{\cong} \mathbb{C}$. The embedding $i_{\mathfrak{p}} : K \hookrightarrow \overline{\mathbb{Q}}_p$ fixes a prime ideal, say $\mathfrak{p}$, in K lying above p. Let $G_{\mathbb{Q}}$ and G_K denote the absolute Galois groups of $\mathbb{Q}$ and K respectively. Let $\widetilde{K}_{\infty}$ denote the compositum of all the $\mathbb{Z}_p$-extensions of K. Let $\mathbb{Q}_{\mathrm{cyc}}$ and K_{cyc} denote the cyclotomic $\mathbb{Z}_p$-extensions of $\mathbb{Q}$ and K respectively. Let $K(\mathfrak{p}^{\infty})_{\mathbb{Z}_p}$ denote the unique $\mathbb{Z}_p$-extension of K that is unramified outside $\mathfrak{p}$. Let $\widetilde{\Gamma}$, Γ_{cyc} and $\Gamma_{\mathfrak{p}}$ denote the Galois groups $\mathrm{Gal}(\widetilde{K}_{\infty}/K)$, $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$ and $\mathrm{Gal}(K(\mathfrak{p}^{\infty})_{\mathbb{Z}_p}/K)$ respectively. To summarize, we have the following isomorphisms of topological groups:

$$\widetilde{\Gamma} = \mathrm{Gal}(\widetilde{K}_{\infty}/K) \cong \mathbb{Z}_p^2, \quad \Gamma_{\mathrm{cyc}} \cong \mathrm{Gal}(K_{\mathrm{cyc}}/K) \cong \mathbb{Z}_p,$$
$$\Gamma_{\mathfrak{p}} = \mathrm{Gal}(K(\mathfrak{p}^{\infty})_{\mathbb{Z}_p}/K) \cong \mathbb{Z}_p.$$

The natural restriction maps $\widetilde{\Gamma} \twoheadrightarrow \Gamma_{\text{cyc}}$ and $\widetilde{\Gamma} \twoheadrightarrow \Gamma_{\mathfrak{p}}$ provide us the following isomorphism of topological groups:

$$\widetilde{\Gamma} \cong \Gamma_{\text{cyc}} \times \Gamma_{\mathfrak{p}}.$$

We shall consider the Iwasawa algebras $\mathbb{Z}_p[[\widetilde{\Gamma}]]$, $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$ and $\mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]]$. Note that we have the following topological ring isomorphisms involving power series rings over $\mathbb{Z}_p$:

$$\mathbb{Z}_p[[\widetilde{\Gamma}]] \cong \mathbb{Z}_p[[x_1, x_2]], \quad \mathbb{Z}_p[[\Gamma_{\text{cyc}}]] \cong \mathbb{Z}_p[[x_{\text{cyc}}]], \quad \mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]] \cong \mathbb{Z}_p[[x_{\mathfrak{p}}]].$$

We shall also consider the following tautological characters:

$$\widetilde{\kappa} : G_K \twoheadrightarrow \widetilde{\Gamma} \hookrightarrow \text{GL}_1(\mathbb{Z}_p[[\widetilde{\Gamma}]]), \quad \kappa_{\text{cyc}} : G_{\mathbb{Q}} \twoheadrightarrow \Gamma_{\text{cyc}} \hookrightarrow \text{GL}_1(\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]),$$
$$\kappa_{\mathfrak{p}} : G_K \twoheadrightarrow \Gamma_{\mathfrak{p}} \hookrightarrow \text{GL}_1(\mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]]).$$

Let E denote an elliptic curve defined over $\mathbb{Q}$ with good supersingular reduction at p with $a_p(E) = 0$. Let f_E denote the weight two cuspidal newform associated to the elliptic curve E. The p-adic Tate module, denoted by $T_p(E)$, has a natural action of the Galois group $G_{\mathbb{Q}}$. We let $\text{Res}_{G_K} T_p(E)$ denote the restriction of $T_p(E)$ to the Galois group G_K. We have a four-dimensional Galois representation:

$$\rho_{4,2} : G_{\mathbb{Q}} \to \text{GL}_4(\mathbb{Z}_p[[\widetilde{\Gamma}]])$$

given by the action of $G_{\mathbb{Q}}$ on the following free $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module of rank four:

$$T_{\rho_{4,2}} := T_p(E) \widehat{\otimes}_{\mathbb{Z}_p} \text{Ind}_{G_K}^{G_{\mathbb{Q}}}(\mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]](\kappa_{\mathfrak{p}}^{-1})) \widehat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p[[\Gamma_{\text{cyc}}]](\kappa_{\text{cyc}}^{-1}).$$

Here, $\widehat{\otimes}_{\mathbb{Z}_p}$ denotes the completed tensor product over $\mathbb{Z}_p$. We will also consider the following discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module:

$$D_{\rho_{4,2}} := T_{\rho_{4,2}} \otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} \text{Hom}_{\text{cont}}\left(\mathbb{Z}_p[[\widetilde{\Gamma}]], \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right).$$

Let ρ_K denote the two-dimensional Galois representation, defined over the ring $\mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]]$, given by the action of $G_{\mathbb{Q}}$ on $\text{Ind}_{G_K}^{G_{\mathbb{Q}}}(\mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]](\kappa_{\mathfrak{p}}^{-1}))$.

The Galois representation $\rho_{4,2}$ satisfies Greenberg's Panchishkin condition. Following Greenberg's approach in [14], it is possible to define a discrete Selmer group, denoted by $\text{Sel}^{\text{Gr}}(\mathbb{Q}, D_{\rho_{4,2}})$, attached to the Galois representation $\rho_{4,2}$. The Pontryagin dual of $\text{Sel}^{\text{Gr}}(\mathbb{Q}, D_{\rho_{4,2}})$, denoted by $\text{Sel}^{\text{Gr}}(\mathbb{Q}, D_{\rho_{4,2}})^{\vee}$, is a finitely generated $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module.

Corresponding to the tensor product of the Galois representation associated to the newform f_E and ρ_K, Hida has constructed a two-variable Rankin–Selberg

p-adic L-function, denoted by $\theta_{4,2}^{\mathrm{Gr}}$, in the fraction field of the Iwasawa algebra $\mathbb{Z}_p[[\widetilde{\Gamma}]]$. For the p-adic L-function $\theta_{4,2}^{\mathrm{Gr}}$, one can vary the weight variable and the cyclotomic variable. See Hida's works in [21, 22]. One can consider the Iwasawa main conjecture for $\rho_{4,2}$ formulated by Greenberg.

CONJECTURE 1.2 [14, Conjecture 4.1]. *The $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\mathrm{Sel}^{\mathrm{Gr}}(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ is torsion. Furthermore, we have the following equality in $Z^1(\mathbb{Z}_p[[\widetilde{\Gamma}]])$:*

$$\mathrm{Div}(\mathrm{Sel}^{\mathrm{Gr}}(\mathbb{Q}, D_{\rho_{4,2}})^\vee) \stackrel{?}{=} \mathrm{Div}(\theta_{4,2}^{\mathrm{Gr}}).$$

Though the Galois representation $\rho_{4,2}$ satisfies the Panchishkin condition, it is also possible to consider Selmer groups and p-adic L-functions, that are truly artefacts of working in the supersingular case. On the analytic side, there are four '2-variable p-adic L-functions', which we denote $\theta_{4,2}^{++}, \theta_{4,2}^{+-}, \theta_{4,2}^{-+}$ and $\theta_{4,2}^{--}$, that are elements of the fraction field of the ring $\mathbb{Z}_p[[\widetilde{\Gamma}]]$. The construction of these p-adic L-functions is essentially due to Loeffler [32]. On the algebraic side, Kim [26] has constructed four discrete Selmer groups $\mathrm{Sel}^{++}(\mathbb{Q}, D_{\rho_{4,2}})$, $\mathrm{Sel}^{+-}(\mathbb{Q}, D_{\rho_{4,2}})$, $\mathrm{Sel}^{-+}(\mathbb{Q}, D_{\rho_{4,2}})$ and $\mathrm{Sel}^{--}(\mathbb{Q}, D_{\rho_{4,2}})$. One can view Loeffler's construction of the p-adic L-functions $\theta_{4,2}^{\pm,\pm}$ (and Kim's construction of the Selmer groups $\mathrm{Sel}^{\pm\pm}(\mathbb{Q}, D_{\rho_{4,2}})$ respectively) as a generalization of the construction of the one-variable $\pm$ p-adic L-functions in [44] by Robert Pollack (and the Selmer groups in [27] by Shinichi Kobayashi respectively). We have the following conjecture of Wan, which is a modification of a conjecture of Kim [26, Conjecture 3.1]:

CONJECTURE 1.3 [62, Conjecture 6.7]. *Let $\bullet, \circ \in \{+, -\}$. The $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\mathrm{Sel}^{\bullet\circ}(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ is torsion. We have the following equality in $Z^1(\mathbb{Z}_p[[\widetilde{\Gamma}]])$:*

$$\mathrm{Div}(\mathrm{Sel}^{\bullet\circ}(\mathbb{Q}, D_{\rho_{4,2}})^\vee) \stackrel{?}{=} \mathrm{Div}(\theta_{4,2}^{\bullet\circ}).$$

Our main theorem is the following:

THEOREM 1. *Let $\{\theta_{\mathrm{I}}, \theta_{\mathrm{II}}\}$ denote one of the following unordered pairs:*

$$\{\theta_{4,2}^{++}, \theta_{4,2}^{+-}\}, \quad \{\theta_{4,2}^{++}, \theta_{4,2}^{-+}\}, \quad \{\theta_{4,2}^{--}, \theta_{4,2}^{+-}\}, \quad \{\theta_{4,2}^{--}, \theta_{4,2}^{-+}\},$$
$$\{\theta_{4,2}^{++}, \theta_{4,2}^{\mathrm{Gr}}\}, \quad \{\theta_{4,2}^{+-}, \theta_{4,2}^{\mathrm{Gr}}\}, \quad \{\theta_{4,2}^{-+}, \theta_{4,2}^{\mathrm{Gr}}\}, \quad \{\theta_{4,2}^{--}, \theta_{4,2}^{\mathrm{Gr}}\}.$$

Suppose that the following two conditions hold:

(1) *Conjectures 1.2 and 1.3 hold.*

(2) *The elements θ_{I} and θ_{II} of the unique factorization domain (UFD) $\mathbb{Z}_p[[\widetilde{\Gamma}]]$ have no common irreducible factor.*

Then, we have the following equality in $Z^2(\mathbb{Z}_p[[\widetilde{\Gamma}]])$:

$$c_2\left(\frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\theta_{\mathrm{I}}, \theta_{\mathrm{II}})}\right) = c_2(\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})) + c_2(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^\star}))$$
$$+ \sum_{l \in \Sigma \setminus \{p\}} c_2((H^0(\mathbb{Q}_l, D_{\rho_{4,2}})^\vee)_{\mathrm{P.N.}}).$$

Let us briefly review the notations used in Theorem 1. One can consider the Selmer groups $\mathrm{Sel}_{\mathrm{I}}(\mathbb{Q}, D_{\rho_{4,2}})$ and $\mathrm{Sel}_{\mathrm{II}}(\mathbb{Q}, D_{\rho_{4,2}})$ appearing in Conjectures 1.2 and 1.3 corresponding to the p-adic L-functions θ_{I} and θ_{II} respectively. Here, $\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})$ denotes the Pontryagin dual of the intersection

$$\mathrm{Sel}_{\mathrm{I}}(\mathbb{Q}, D_{\rho_{4,2}}) \cap \mathrm{Sel}_{\mathrm{II}}(\mathbb{Q}, D_{\rho_{4,2}})$$

inside the appropriate first discrete global Galois cohomology group. To make the notation for $\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})$ simpler, we have not included the indices I and II. One can also define modules $D_{\rho_{4,2}^\star}$ and $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^\star})$ for the Tate dual $\rho_{4,2}^\star$ of the Galois representation $\rho_{4,2}$. See Section 7.2 for the explicit description of $\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})$ and $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^\star})$ respectively. The invariant c_2 associates an element in $Z^2(\mathbb{Z}_p[[\widetilde{\Gamma}]])$ to a pseudonull $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module. See Section 2.1 for its definition. This invariant is the generalization of the 'characteristic divisor' appearing in the Iwasawa main conjecture formulated by Greenberg [**14**].

For each finite prime l in $\Sigma \setminus \{p\}$, the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $(H^0(\mathbb{Q}_l, D_{\rho_{4,2}})^\vee)_{\mathrm{P.N.}}$ denotes the maximal pseudonull submodule of $H^0(\mathbb{Q}_l, D_{\rho_{4,2}})^\vee$. See Section 7.3 for a discussion of these fudge factors $c_2((H^0(\mathbb{Q}_l, D_{\rho_{4,2}})^\vee)_{\mathrm{P.N.}})$ at primes $l \neq p$. The discussion is based on the criterion of Néron–Ogg–Shafarevich and the circle of ideas in Tate's algorithms [**58**].

Our main motivation in considering condition (2) of Theorem 1, which we later label 'Assumption GCD', is a conjecture of Coates and Sujatha involving the fine Selmer group. Let Σ denote a finite set of primes in $\mathbb{Q}$ containing p, ∞, the set of primes dividing the conductor of the elliptic curve E and the primes ramified in the extension $K/\mathbb{Q}$. Let $\mathbb{Q}_\Sigma$ denote the maximal extension of $\mathbb{Q}$ unramified outside Σ. Let G_Σ denote $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$. The fine Selmer group, denoted by $\mathrm{III}^1(\mathbb{Q}, D_{\rho_{4,2}})$, is defined below:

$$\mathrm{III}^1(\mathbb{Q}, D_{\rho_{4,2}}) := \ker(H^1(G_\Sigma, D_{\rho_{4,2}}) \to \bigoplus_{v \in \Sigma} H^1(\mathrm{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v), D_{\rho_{4,2}})).$$

We now state the conjecture of Coates and Sujatha.

CONJECTURE 1.4 [**10**, Conjecture B]. *The $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\mathrm{III}^1(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ is pseudonull.*

Recall that a finitely generated torsion module M over the UFD $\mathbb{Z}_p[[\widetilde{\Gamma}]]$ is said to be pseudonull if $\mathrm{Div}(M)$ equals zero. We have the following natural surjection of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$\mathrm{Sel}^{\pm,\pm}(\mathbb{Q}, D_{\rho_{4,2}})^\vee \twoheadrightarrow \mathrm{III}^1(\mathbb{Q}, D_{\rho_{4,2}})^\vee, \quad \mathrm{Sel}^{\mathrm{Gr}}(\mathbb{Q}, D_{\rho_{4,2}})^\vee \twoheadrightarrow \mathrm{III}^1(\mathbb{Q}, D_{\rho_{4,2}})^\vee.$$

Assume that Conjectures 1.2 and 1.3 are valid. Let $\mathrm{Supp}_{\mathrm{Ht}=1}(M)$ denote the set of height one prime ideals of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$ in the support of a finitely generated $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module M. Then, $\mathrm{Supp}_{\mathrm{Ht}=1}(\mathrm{III}^1(\mathbb{Q}, D_{\rho_{4,2}})^\vee)$ is a subset of

$$\mathrm{Supp}_{\mathrm{Ht}=1}\left(\frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\theta_{4,2}^{\mathrm{Gr}})}\right) \bigcap \mathrm{Supp}_{\mathrm{Ht}=1}\left(\frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\theta_{4,2}^{++})}\right) \bigcap \mathrm{Supp}_{\mathrm{Ht}=1}\left(\frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\theta_{4,2}^{+-})}\right)$$

$$\bigcap \mathrm{Supp}_{\mathrm{Ht}=1}\left(\frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\theta_{4,2}^{-+})}\right) \bigcap \mathrm{Supp}_{\mathrm{Ht}=1}\left(\frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\theta_{4,2}^{--})}\right).$$

To investigate Conjecture 1.4, it seems instructive to consider the setup when two of the above p-adic L-functions have no common irreducible factor in the UFD $\mathbb{Z}_p[[\widetilde{\Gamma}]]$. The motivation behind proving Theorem 1 is to provide a partial answer to Question 1.1 in this setup. See Section 8, where we produce numerical evidence towards the existence of elliptic curves E with good supersingular reduction at p, such that $\theta_{4,2}^{++}$ and $\theta_{4,2}^{+-}$ have no common irreducible factors in the UFD $\mathbb{Z}_p[[\widetilde{\Gamma}]]$. If $\theta_{4,2}^{++}$ and $\theta_{4,2}^{+-}$ have no common irreducible factor in $\mathbb{Z}_p[[\widetilde{\Gamma}]]$, then the pseudonullity conjecture of Coates–Sujatha is also valid, assuming the validity of the Iwasawa main conjectures. Hence, these example provide evidence towards Conjecture 1.4 as well.

The examples in Section 8 are based on computations of Robert Pollack, given on his website http://math.bu.edu/people/rpollack/Data/data.html. These computations and the examples in Section 8 are based on the theory of overconvergent modular symbols of Stevens [57], Pollack and Stevens [46] and related to Pollack's work with Kurihara [28].

REMARK 1.5. The pseudonullity conjecture of Coates and Sujatha [10, Conjecture B] is formulated in greater generality than the setting of Conjecture 1.4. They formulate their conjecture for the fine Selmer group of an elliptic curve over certain (admissible) p-adic Lie extensions whose Galois group is a p-adic Lie group with dimension $\geqslant 2$. We refer the reader to works of Ochi [39], Lim [31] and Shekhar [50] where there are other examples verifying the pseudonullity conjecture of Coates–Sujatha. The setups in their works and their approaches are completely different to ours.

Theorem 1 is a consequence of Theorem 4.3, which is applicable in a fairly general setting. To explain the method of the proof of Theorem 4.3 in the

introduction, we will consider the setup of Theorem 1. A key ingredient in proving our results is the construction of an auxiliary $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module, denoted by $\mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}})$. To make the notation simpler, we have not included the indices I and II. Assuming the validity of Conjectures 1.2 and 1.3, this $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module turns out to be torsion-free and to have rank one. This module also fits into the following surjection of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$\underbrace{H^1(G_\Sigma, D_{\rho_{4,2}})^\vee}_{\substack{\text{Conjecturally} \\ \text{has } \mathbb{Z}_p[[\widetilde{\Gamma}]]\text{-rank two}}} \twoheadrightarrow \underbrace{\mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}})}_{\substack{\text{Conjecturally} \\ \text{has } \mathbb{Z}_p[[\widetilde{\Gamma}]]\text{-rank one}}} \twoheadrightarrow \underbrace{\frac{\mathrm{Sel}_\mathrm{I}(\mathbb{Q}, D_{\rho_{4,2}})^\vee}{\mathrm{Sel}_\mathrm{II}(\mathbb{Q}, D_{\rho_{4,2}})^\vee}}_{\substack{\text{Conjecturally} \\ \mathbb{Z}_p[[\widetilde{\Gamma}]]\text{-torsion}}} \twoheadrightarrow \underbrace{\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})}_{\substack{\text{Pseudonull, assuming} \\ \text{the hypotheses in Theorem 1}}} \twoheadrightarrow \underbrace{\text{Ш}^1(\mathbb{Q}, D_{\rho_{4,2}})^\vee}_{\text{Conjecturally pseudonull}} .$$

To prove Theorem 1, we first show that for every height two prime ideal $\mathcal{Q}$ in the ring $\mathbb{Z}_p[[\widetilde{\Gamma}]]$, we have the following short exact sequence of $\mathbb{Z}_p[[\widetilde{\Gamma}]]_\mathcal{Q}$-modules:

$$0 \to \mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})_\mathcal{Q} \to \frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]_\mathcal{Q}}{(\theta_\mathrm{I}, \theta_\mathrm{II})} \to$$
$$\to \mathrm{coker}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}}) \to \mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}})^{**}) \otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} \mathbb{Z}_p[[\widetilde{\Gamma}]]_\mathcal{Q} \to 0. \quad (1.1)$$

Here, $\mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}})^{**}$ is the reflexive hull of the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}})$. The $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}})^{**}$ turns out to be free.

The $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\mathrm{coker}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}}) \to \mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}})^{**})$ is pseudonull. To study the invariant c_2 associated to this pseudonull $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module and thus complete the proof of Theorem 1, we use the duality theorems developed by Jan Nekovář in his work on Selmer complexes [37]. We show that we have the following equality in $Z^2(\mathbb{Z}_p[[\widetilde{\Gamma}]])$:

$$c_2(\mathrm{coker}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}}) \to \mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}})^{**}))$$
$$= c_2(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^\star})) + \sum_{l \in \Sigma \setminus \{p\}} c_2((H^0(\mathbb{Q}_l, D_{\rho_{4,2}})^\vee)_{\mathrm{P.N.}}). \quad (1.2)$$

A key idea in establishing (1.2) involves a careful study of Ext groups. This idea is based on the theory of Iwasawa adjoints, which was first conceived by Iwasawa [23] and later developed in greater generality in works of Jannsen [24, 25]. Combining equations (1.1) and (1.2) completes the proof of Theorem 1.

To apply our theorem in the general setup (Theorem 4.3) to the setting of Theorem 1, we use results of Kim [26] and Kobayashi [27]. These results of Kim and Kobayashi are in turn built on earlier works of Perrin-Riou [42] and Rubin [48].

REMARK 1.6. Since it is important to our methods to construct the rank-one $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}})$, we do not consider the case where $\{\theta_\mathrm{I}, \theta_\mathrm{II}\}$ equals $\{\theta_{4,2}^{++}, \theta_{4,2}^{--}\}$ or $\{\theta_{4,2}^{+-}, \theta_{4,2}^{-+}\}$. A similar construction of $\mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}})$ in these cases

would produce a $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module that has rank at least two (it is exactly two if the Pontryagin dual of any of the corresponding Selmer groups is torsion over $\mathbb{Z}_p[[\widetilde{\Gamma}]]$). Another interesting point to note is that when the root number of the elliptic curve E over K equals -1, it is known that $\ker(\pi_{\mathrm{ac}})$ belongs to the support of the divisors $\mathrm{Div}(\theta_{4,2}^{++})$ and $\mathrm{Div}(\theta_{4,2}^{--})$. The map

$$\pi_{\mathrm{ac}} : \mathbb{Z}_p[[\widetilde{\Gamma}]] \to \mathbb{Z}_p[[\Gamma_{\mathrm{ac}}]]$$

denotes the natural projection map (which one can view as the 'anticyclotomic specialization'). Here, Γ_{ac} denotes $\mathrm{Gal}(K_{\mathrm{ac}}/K)$, the Galois group of the anticyclotomic $\mathbb{Z}_p$-extension K_{ac} of K. See [**5**, **8**, **35**]. However, at present, we do not know when the root number of the elliptic curve E over K equals -1 whether $\ker(\pi_{\mathrm{ac}})$ belongs to the support of $\mathrm{Div}(\theta_{4,2}^{+-})$ or $\mathrm{Div}(\theta_{4,2}^{-+})$.

REMARK 1.7. As a referee had pointed out to us, the construction of Hida's Rankin–Selberg p-adic L-function is in fact contingent on a choice of a prime above p. On the algebraic side, this choice amounts to defining the filtration $\mathrm{Fil}_+ T_{\rho_{4,2}}$ for the Selmer group in Section 5.1 involving either the character $\kappa_{\mathfrak{p}}$ or $\kappa_{\mathfrak{q}}$. One can thus consider another Rankin–Selberg p-adic L-function. We do not consider the pair of Rankin–Selberg p-adic L-functions in Theorem 1 since, just as in Remark 1.6, the construction of $\mathfrak{X}(\mathbb{Q}, D_{\rho_{4,2}})$ does not yield a rank-one $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module. The discussion of Theorem 1 for the pair of p-adic L-functions involving this additional Rankin–Selberg p-adic L-function and one of the p-adic L-functions $\theta_{4,2}^{\pm,\pm}$ is completely analogous to the discussion of the pairs $\{\theta_{4,2}^{\pm,\pm}, \theta_{4,2}^{\mathrm{Gr}}\}$.

REMARK 1.8. Analogues of the $\pm\pm$ p-adic L-functions and Selmer groups have been constructed for cuspidal eigenforms with weight $\geqslant 2$ when p is a good nonordinary prime (see [**6**, **7**, **29**, **56**]). In the proof of Theorem 1, we rely on results of Kim [**26**] to verify that the local Selmer conditions at p satisfy certain freeness conditions (labelled Hypothesis LF in Section 3). At present, we are not sure to what extent these freeness results are available and whether they can be extended to the more general settings.

REMARK 1.9. The purpose of developing Theorem 4.3 in a general setting is to pursue applications to other arithmetic setups. In [**30**], we obtain one such application of Theorem 4.3 in the setting of cyclotomic twist deformations of Hida families. We refer the interested reader to [**30**] for the exact details. An added difficulty in this setting is that the (normalizations of) deformation rings, appearing in Hida theory, are not always known to be regular (see [**41**, Section 4] for examples when such rings are not even UFDs).

Section 2 involves establishing preliminaries in commutative and homological algebra. Section 3 describes the objects involved in the general setting of our main theorem. Section 4 involves the proof of our main theorem in the general setting.

Section 5 describes the Iwasawa main conjecture formulated by Greenberg in the setting of Theorem 1. Section 6 describes the $\pm\pm$ Iwasawa main conjectures for elliptic curves with supersingular reduction at p, formulated by Kim. Section 7 describes the proof of Theorem 1. Section 8 deals with providing evidence for Assumption GCD, and in turn the pseudonullity conjecture of Coates–Sujatha, in the setup of Theorem 1.

Here is a brief summary of some of the notations and conventions used in this paper.

- If $\mathcal{R}$ is a Noetherian, complete, integrally closed, local domain of characteristic zero with Krull dimension $n+1$ and whose residue field has characteristic p, we let $\mathcal{R}^\vee$ denote $\mathrm{Hom}_{\mathrm{cont}}(R, \mathbb{Q}_p/\mathbb{Z}_p)$. For a finitely generated module M over such a ring $\mathcal{R}$, we let $M^\vee$ denote the Pontryagin dual of M and M^* denote its reflexive dual $\mathrm{Hom}_{\mathcal{R}}(M, \mathcal{R})$. Similarly, if D is a discrete module over such a ring $\mathcal{R}$, we let $D^\vee$ denote the Pontryagin dual of D. If I is an ideal of $\mathcal{R}$, we write $D[I]$ for the $\mathcal{R}$-submodule of D annihilated by all elements of the ideal I.

- Suppose L is a field. If M is a discrete module with a continuous action of the absolute Galois group G_L, we will let $H^i(L, M)$ denote the continuous cohomology group $H^i(G_L, M)$, for each $i \geqslant 0$.

- If $\widehat{\mathcal{F}}$ is a formal group defined over the integral closure of $\mathbb{Z}_p$ in an algebraic extension L of $\mathbb{Q}_p$, we let $\widehat{\mathcal{F}}(L)$ denote the group of L-points on the corresponding formal group. That is, if $\mathfrak{m}_L$ denotes the maximal ideal in the integral closure of $\mathbb{Z}_p$ in L, then $\widehat{\mathcal{F}}(L)$ would equal $\widehat{\mathcal{F}}(\mathfrak{m}_L)$.

- Let L be an algebraic extension of $\mathbb{Q}_p$. Let Γ_1 be a topological group isomorphic to $\mathbb{Z}_p$. Let γ_1 be a topological generator of Γ_1 and fix an isomorphism $\mathbb{Z}_p[[\Gamma_1]] \cong \mathbb{Z}_p[[T]]$ of rings by sending γ_1 to $T+1$. To emphasize the choice of the topological generator, we may write $\mathbb{Z}_p[[\gamma_1 - 1]]$ and $L[[\gamma_1 - 1]]$ instead of the power series rings $\mathbb{Z}_p[[T]]$ and $L[[T]]$. If μ is an L-valued distribution on the topological group Γ_1, we have the Amice transform

$$\int_{x \in \Gamma_1} (1+T)^x \mu(x) \in L[[T]].$$

Suppose Γ_2 is another topological group isomorphic to $\mathbb{Z}_p$. Let γ_2 be a topological generator of Γ_2. Fix an isomorphism of the completed group ring $\mathbb{Z}_p[[\Gamma_1 \times \Gamma_2]]$ with $\mathbb{Z}_p[[S, T]]$ byidentifying $\gamma_1 - 1$ and $\gamma_2 - 1$ with S and T

respectively. Once again, to emphasize the choice of the topological generator, we may write $\mathbb{Z}_p[[\gamma_1 - 1, \gamma_2 - 1]]$ and $L[[\gamma_1 - 1, \gamma_2 - 1]]$ instead of the power series rings $\mathbb{Z}_p[[S, T]]$ and $L[[S, T]]$. Suppose μ is an L-valued distribution on $\Gamma_1 \times \Gamma_2$, its Amice transform is given by

$$\int_{x \in \Gamma_1, y \in \Gamma_2} (1 + S)^x (1 + T)^y \mu(x, y) \in L[[S, T]].$$

- The first subscript d of $\rho_{d,n}$ indicates the dimension of the Galois representation, while the second subscript n denotes a number one less than the Krull dimension of the ring $\mathcal{R}$. In the settings we are interested in, the number n would denote the number of variables in the corresponding p-adic L-functions.

- Under our (nonstandard) convention, the kernel of a homomorphism φ in $\mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]], \overline{\mathbb{Q}}_p) = \mathrm{Hom}_{\mathrm{cont}}(\Gamma_{\mathfrak{p}}, \overline{\mathbb{Q}}_p^{\times})$ corresponds to a weight k specialization if φ is the p-adic character associated to an algebraic Hecke character of K, with conductor equal to a power of $\mathfrak{p}$ and of infinity type $(1 - k)i \circ i_{\mathfrak{p}}$.

- As we explain in Remark 6.2, we have chosen to work with the normalizations of the plus and minus 2-variable p-adic L-functions adopted by Xin Wan instead of David Loeffler. The difference in normalizations is due to different choices of complex periods.

- Our choice of signs $+$ and $-$ in the definition of plus and minus Selmer groups is the same as Loeffler and Pollack. This choice is opposite to that of Kim and Kobayashi.

2. Some commutative and homological algebra

Let $\mathcal{R}$ denote a Noetherian local ring. Let $\mathcal{M}$ be a finitely generated $\mathcal{R}$-module. In Section 2, we will simply accumulate the general results in commutative and homological algebra needed for our purposes.

DEFINITION 1. The length of a finitely generated $\mathcal{R}$-module $\mathcal{M}$, denoted by $\mathrm{Len}_{\mathcal{R}} \mathcal{M}$, is the length of a(ny) composition series of $\mathcal{M}$ (if a composition series does not exist, we set the length to equal infinity).

We recall a few results on lengths of modules.

LEMMA 2.1 [2, Proposition 6.9]. *Suppose we have a short exact sequence*

$$0 \to \mathcal{M}' \to \mathcal{M} \to \mathcal{M}'' \to 0$$

of finitely generated $\mathcal{R}$-modules. Then, we have the following equality of lengths:

$$\mathrm{Len}_{\mathcal{R}}\mathcal{M} = \mathrm{Len}_{\mathcal{R}}\mathcal{M}' + \mathrm{Len}_{\mathcal{R}}\mathcal{M}''.$$

The following lemma follows from [**2**, Propositions 6.3 and 6.8].

LEMMA 2.2. *Suppose the local Noetherian ring $\mathcal{R}$ is also Artinian. For every finitely generated $\mathcal{R}$-module $\mathcal{M}$, we have $\mathrm{Len}_{\mathcal{R}}(\mathcal{M}) < \infty$.*

2.1. Pseudonull modules, Reflexive modules and Ext groups.

DEFINITION 2. A finitely generated $\mathcal{R}$-module $\mathcal{M}$ is said to be a pseudonull $\mathcal{R}$-module if

$$\mathcal{M}_{\mathfrak{p}} = 0, \ \text{for all prime ideals } \mathfrak{p} \text{ in } \mathcal{R} \text{ such that height}(\mathfrak{p}) \leqslant 1.$$

Let $\mathrm{Ann}_{\mathcal{R}}(\mathcal{M})$ denote the annihilator of the $\mathcal{R}$-module $\mathcal{M}$. If the $\mathcal{R}$-module $\mathcal{M}$ is pseudonull, then the height of the ideal $\mathrm{Ann}_{\mathcal{R}}(\mathcal{M})$ is greater than or equal to two.

LEMMA 2.3. *Suppose $\mathcal{Z}$ is a pseudonull $\mathcal{R}$-module. For every height two prime ideal $\mathcal{Q}$ in $\mathcal{R}$, we have $\mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}} \mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} < \infty$.*

Proof. There exist a positive integer m and a surjection

$$\left(\frac{\mathcal{R}_{\mathcal{Q}}}{\mathrm{Ann}_{\mathcal{R}}(\mathcal{Z})\mathcal{R}_{\mathcal{Q}}} \right)^m \twoheadrightarrow \mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}},$$

of $\mathcal{R}_{\mathcal{Q}}$-modules. Note that $\mathcal{R}_{\mathcal{Q}}$ is a Noetherian local ring with Krull dimension two. The $\mathcal{R}_{\mathcal{Q}}$-ideal $\mathrm{Ann}_{\mathcal{R}}(\mathcal{Z})\mathcal{R}_{\mathcal{Q}}$ has height two. As a result, the quotient ring $\mathcal{R}_{\mathcal{Q}}/(\mathrm{Ann}_{\mathcal{R}}(\mathcal{Z})\mathcal{R}_{\mathcal{Q}})$, being Noetherian and having Krull dimension zero, is Artinian. See Theorem 8.5 in Atiyah and Macdonald [**2**]. The proof of this lemma now follows from Lemma 2.2. $\qquad\square$

Lemma 2.3 allows us to associate, to a pseudonull $\mathcal{R}$-module, an element in $Z^2(\mathcal{R})$ (the free abelian group on the set of height two prime ideals of $\mathcal{R}$). If $\mathcal{M}$ is a pseudonull $\mathcal{R}$-module, we define an element $c_2(\mathcal{M})$ in $Z^2(\mathcal{R})$ as the following formal sum:

$$c_2(\mathcal{M}) := \sum_{\substack{\mathcal{Q} \subset \mathcal{R} \\ \text{height}(\mathcal{Q})=2}} (\mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}} \mathcal{M}_{\mathcal{Q}})\mathcal{Q}. \tag{2.1}$$

In the above formula, the summation is taken over all the height two prime ideals $\mathcal{Q}$ of $\mathcal{R}$. Since length is additive in exact sequences and since localization is exact, we have the following lemma:

LEMMA 2.4. *Suppose we have a short exact sequence*

$$0 \to \mathcal{M}' \to \mathcal{M} \to \mathcal{M}'' \to 0$$

of finitely generated pseudonull $\mathcal{R}$-modules. Then, we have the following equality in $Z^2(\mathcal{R})$:

$$c_2(\mathcal{M}) = c_2(\mathcal{M}') + c_2(\mathcal{M}'').$$

Theorem 4.4.8 in Weibel's book [63] and Lemma 2.3 (see also [63, Standard Facts 4.4.7]) automatically give us the following lemma:

LEMMA 2.5. *Let $\mathcal{Z}$ be a finitely generated pseudonull $\mathcal{R}$-module. Suppose $\mathcal{Q}$ is a height two prime ideal in $\mathcal{R}$ such that $\mathcal{Z} \otimes_\mathcal{R} \mathcal{R}_\mathcal{Q} \neq 0$. Then, we have $\mathrm{Depth}_{\mathcal{R}_\mathcal{Q}}(\mathcal{Z} \otimes_\mathcal{R} \mathcal{R}_\mathcal{Q}) = 0$.*

Let us recall a theorem of Serre.

LEMMA 2.6 [36, Theorem 23.8]. *Let $\mathcal{R}$ be a domain. The domain $\mathcal{R}$ is integrally closed if and only if both the following conditions hold:*

- *$\mathcal{R}_\mathfrak{p}$ is a discrete valuation ring (DVR), for every height one prime ideal $\mathfrak{p}$ of $\mathcal{R}$,*

- *$\mathrm{Depth}_{\mathcal{R}_\mathcal{Q}}(\mathcal{R}_\mathcal{Q}) = 2$, for all height two prime ideals $\mathcal{Q}$ of $\mathcal{R}$.*

For the rest of Section 2, we will let $\mathcal{R}$ be an integrally closed, local, Noetherian domain. Let $\mathfrak{X}$ be a finitely generated $\mathcal{R}$-module. The reflexive hull of $\mathfrak{X}$ (denoted by $\mathfrak{X}^{**}$) is defined below:

$$\mathfrak{X}^{**} := \mathrm{Hom}_\mathcal{R}(\mathrm{Hom}_\mathcal{R}(\mathfrak{X}, \mathcal{R}), \mathcal{R}).$$

One can define a natural map $i_\mathfrak{X} : \mathfrak{X} \to \mathfrak{X}^{**}$, as given below:

$$i_\mathfrak{X} : \mathfrak{X} \to \mathfrak{X}^{**}$$
$$x \to (\phi \to \phi(x)).$$

DEFINITION 3. The $\mathcal{R}$-module $\mathfrak{X}$ is said to be a *reflexive $\mathcal{R}$-module* if the map $i_\mathfrak{X}$ is an isomorphism.

The following lemma is proved in Section 1 of Ch. V in the book by Neukirch *et al.* [38].

LEMMA 2.7.

(1) *The $\mathcal{R}$-module $\ker(i_{\mathfrak{X}})$ equals $\mathfrak{X}_{\mathrm{tor}}$, the maximal $\mathcal{R}$-torsion submodule of $\mathfrak{X}$.*

(2) *The $\mathcal{R}$-module $\mathrm{coker}(i_{\mathfrak{X}})$ is a pseudonull $\mathcal{R}$-module.*

We also have the following useful result that follows from Propositions 1.2.12 and 1.4.1 in the book by Bruns and Herzog [**4**].

LEMMA 2.8. *Suppose $\mathcal{M}$ is a finitely generated nonzero reflexive $\mathcal{R}$-module. Let $\mathcal{Q}$ be a height two prime ideal of $\mathcal{R}$. Then, $\mathrm{Depth}_{\mathcal{R}_{\mathcal{Q}}} \mathcal{M}_{\mathcal{Q}}$ equals 2.*

LEMMA 2.9 (Proposition 3.3.10 in Weibel's book [**63**]). *Let $\mathfrak{p}$ be a prime ideal in $\mathcal{R}$. Let $\mathcal{M}$ be a finitely generated $\mathcal{R}$-module. Let $\mathcal{N}$ be an $\mathcal{R}$-module. We have the following natural isomorphism of $\mathcal{R}_{\mathfrak{p}}$-modules, for all $i \geqslant 0$:*

$$\mathrm{Ext}^i_{\mathcal{R}}(\mathcal{M}, \mathcal{N}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}} \cong \mathrm{Ext}^i_{\mathcal{R}_{\mathfrak{p}}}(\mathcal{M}_{\mathfrak{p}}, \mathcal{N}_{\mathfrak{p}}).$$

In particular, if $\mathcal{M}$ is a finitely generated reflexive $\mathcal{R}$-module, then $\mathcal{M}_{\mathfrak{p}}$ is a finitely generated reflexive $\mathcal{R}_{\mathfrak{p}}$-module for every prime ideal $\mathfrak{p}$ since

$$\begin{aligned} \mathcal{M}_{\mathfrak{p}} &\cong \mathrm{Hom}_{\mathcal{R}}(\mathrm{Hom}_{\mathcal{R}}(\mathcal{M}, \mathcal{R}), \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}} \\ &\cong \mathrm{Hom}_{\mathcal{R}_{\mathfrak{p}}}(\mathrm{Hom}_{\mathcal{R}_{\mathfrak{p}}}(\mathcal{M}_{\mathfrak{p}}, \mathcal{R}_{\mathfrak{p}}), \mathcal{R}_{\mathfrak{p}}). \end{aligned}$$

LEMMA 2.10. *Suppose $\mathcal{M}$ is a finitely generated reflexive $\mathcal{R}$-module. Suppose $\mathcal{Q}$ is a height two prime ideal in $\mathcal{R}$. If the projective dimension of the $\mathcal{R}_{\mathcal{Q}}$-module $\mathcal{M}_{\mathcal{Q}}$ is finite, then $\mathcal{M}_{\mathcal{Q}}$ is a free $\mathcal{R}_{\mathcal{Q}}$-module. Furthermore, we have*

$$\mathrm{Ext}^i_{\mathcal{R}}(\mathcal{M}, \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \cong \mathrm{Ext}^i_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{M}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}) = 0, \quad \forall i \geqslant 1. \qquad (2.2)$$

Proof. If $\mathcal{M}_{\mathcal{Q}}$ equals zero, the lemma follows automatically. Let us work with the case when $\mathcal{M}_{\mathcal{Q}}$ is not zero. Using the Auslander–Buchsbaum equality (see Theorem 4.4.15 in Weibel's book [**63**]) over the local ring $\mathcal{R}_{\mathcal{Q}}$ gives us the following equality:

$$\mathrm{pd}_{\mathcal{R}_{\mathcal{Q}}} \mathcal{M}_{\mathcal{Q}} = \mathrm{Depth}_{\mathcal{R}_{\mathcal{Q}}} \mathcal{R}_{\mathcal{Q}} - \mathrm{Depth}_{\mathcal{R}_{\mathcal{Q}}} \mathcal{M}_{\mathcal{Q}} = 2 - 2 = 0.$$

Here, $\mathrm{pd}_{\mathcal{R}_{\mathcal{Q}}}$ denotes the projective dimension over the ring $\mathcal{R}_{\mathcal{Q}}$. Finitely generated projective modules over commutative Noetherian local rings are free. Equation (2.2) then follows from Lemma 2 in Ch. 19 of Matsumura's book [**36**]. $\qquad \square$

Suppose $\mathcal{M}$ and $\mathcal{N}$ are two finitely generated $\mathcal{R}$-modules. Since $\mathcal{R}$ is a commutative Noetherian ring, $\mathrm{Ext}^i_{\mathcal{R}}(\mathcal{M}, \mathcal{N})$ is a finitely generated $\mathcal{R}$-module, for

every nonnegative integer i. See Lemma 3.3.6 in Weibel's book [63]. As indicated by Lemma 2.10, localization commutes with Ext for finitely generated modules over commutative rings. So, if $\mathcal{Z}$ is a finitely generated pseudonull $\mathcal{R}$-module, then $\mathrm{Ext}^i_{\mathcal{R}}(\mathcal{Z}, \mathcal{R})$ is also a finitely generated pseudonull $\mathcal{R}$-module, for every nonnegative integer i.

LEMMA 2.11. *Let $\mathcal{Z}$ be a finitely generated pseudonull $\mathcal{R}$-module. Let $\mathcal{Q}$ be a height two prime ideal in $\mathcal{R}$. We have*

$$\mathrm{Ext}^0_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}) = \mathrm{Ext}^1_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}) = 0. \qquad (2.3)$$

Proof. By Lemma 2.3, one can consider a composition series for $\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ of finite length. Suppose the following chain of $\mathcal{R}_{\mathcal{Q}}$-modules is such a composition series for $\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$:

$$\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} = \mathcal{M}_0 \supsetneq \mathcal{M}_1 \supsetneq \cdots \supsetneq \mathcal{M}_n = 0.$$

Each quotient $\mathcal{M}_i/\mathcal{M}_{i+1}$ in the composition series is isomorphic, as an $\mathcal{R}_{\mathcal{Q}}$-module, to $k_{\mathcal{Q}}$, the residue field of $\mathcal{R}_{\mathcal{Q}}$. One can then use a dévissage argument to reduce to the case when $\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ equals $k_{\mathcal{Q}}$. As Lemma 2.6 indicates, $\mathrm{Depth}_{\mathcal{R}_{\mathcal{Q}}} \mathcal{R}_{\mathcal{Q}}$ equals 2. So, in this case when $\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ equals $k_{\mathcal{Q}}$, equation (2.3) follows from Theorem 4.4.8 in Weibel's book [63]. $\qquad \square$

Let $\mathcal{Q}$ be a height two prime ideal in $\mathcal{R}$ such that the localization $\mathcal{R}_{\mathcal{Q}}$ is a Gorenstein local ring. In this case, the injective dimension of $\mathcal{R}_{\mathcal{Q}}$, as an $\mathcal{R}_{\mathcal{Q}}$-module, equals two. See Corollary 4.4.10 in Weibel's book [63]. As a result, we have

$$\mathrm{Ext}^3_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{M}, \mathcal{R}_{\mathcal{Q}}) = 0 \quad \text{for all } \mathcal{R}_{\mathcal{Q}}\text{-modules } \mathcal{M}.$$

See Lemma 2 in Ch. 19 of Matsumura's book [36]. These observations let us deduce the following corollary to Lemma 2.11.

COROLLARY 2.12. *Let $\mathcal{Q}$ be a height two prime ideal in $\mathcal{R}$ such that the localization $\mathcal{R}_{\mathcal{Q}}$ is a Gorenstein local ring. Suppose we have a short exact sequence $0 \to \mathcal{Z}' \to \mathcal{Z} \to \mathcal{Z}'' \to 0$ of finitely generated pseudonull $\mathcal{R}$-modules. Then, we have the following short exact sequence of finitely generated $\mathcal{R}_{\mathcal{Q}}$-modules:*

$$0 \to \mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{Z}'' \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}) \to \mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}) \to$$
$$\to \mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{Z}' \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}) \to 0.$$

REMARK 2.13. A regular local ring is Gorenstein. See Corollary 4.4.17 in Weibel's book [63].

2.2. Cokernels of maps defining reflexive hulls. The ring $\mathcal{R}$ is assumed to be an integrally closed, Noetherian, local domain in Section 2.2.

PROPOSITION 2.14. *Suppose the finitely generated $\mathcal{R}$-module $\mathfrak{X}$ is torsion-free. Suppose also that for every height two prime ideal $\mathcal{Q}$ of $\mathcal{R}$, the $\mathcal{R}_{\mathcal{Q}}$-modules $\mathfrak{X}_{\mathcal{Q}}$ and $\mathrm{coker}(i_{\mathfrak{X}})_{\mathcal{Q}}$ have finite projective dimension. Then, we have the following equality in $Z^2(\mathcal{R})$:*

$$c_2(\mathrm{coker}(i_{\mathfrak{X}})) = c_2(\mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}, \mathcal{R})).$$

Proof. We will divide the proof into two parts:

Part One: For every height two prime ideal $\mathcal{Q}$ in $\mathcal{R}$, we have the following isomorphism of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$\mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}, \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \cong \mathrm{Ext}^2_{\mathcal{R}}(\mathrm{coker}(i_{\mathfrak{X}}), \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}. \qquad (2.4)$$

Part Two: For every height two prime ideal $\mathcal{Q}$ in $\mathcal{R}$, we have the following equality of lengths of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$\mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}(\mathrm{Ext}^2_{\mathcal{R}}(\mathrm{coker}(i_{\mathfrak{X}}), \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}})$$
$$= \mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}(\mathrm{coker}(i_{\mathfrak{X}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}). \qquad (2.5)$$

The first part of the proof follows from Lemma 2.15. As Lemma 2.7 indicates, $\mathrm{coker}(i_{\mathfrak{X}})$ is a finitely generated pseudonull $\mathcal{R}$-module. The second part of the proof would then follow from Lemma 2.16. It is clear that the proposition would then follow from equations (2.4) and (2.5).

LEMMA 2.15. *Follow all the notations and hypotheses of Proposition 2.14. For every height two prime ideal $\mathcal{Q}$ in $\mathcal{R}$, we have the following isomorphism of $\mathcal{R}_{\mathcal{Q}}$-modules:*

$$\mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}, \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \cong \mathrm{Ext}^2_{\mathcal{R}}(\mathrm{coker}(i_{\mathfrak{X}}), \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}. \qquad (2.6)$$

Proof. Let $\mathcal{Q}$ be a height two prime ideal in $\mathcal{R}$. Note that since $\mathfrak{X}$ is a torsion-free $\mathcal{R}$-module, $\ker(i_{\mathfrak{X}})$ equals zero. Consider the localization of the short exact sequence $0 \to \mathfrak{X} \to \mathfrak{X}^{**} \to \mathrm{coker}(i_{\mathfrak{X}}) \to 0$ at the prime ideal $\mathcal{Q}$ of $\mathcal{R}$. We obtain the following short exact sequence of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$0 \to \mathfrak{X}_{\mathcal{Q}} \to \mathfrak{X}^{**} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to \mathrm{coker}(i_{\mathfrak{X}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to 0. \qquad (2.7)$$

The hypotheses of the lemma tell us that the $\mathcal{R}_{\mathcal{Q}}$-module $\mathfrak{X}^{**} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ has finite projective dimension and hence is free (by Lemma 2.10). We have the following equalities, for all $i \geqslant 1$:

$$\mathrm{Ext}^i_{\mathcal{R}_{\mathcal{Q}}}(\mathfrak{X}^{**} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}) = 0.$$

Applying the functor $\mathrm{Hom}_{\mathcal{R}_{\mathcal{Q}}}(-, \mathcal{R}_{\mathcal{Q}})$ to the short exact sequence (2.7) given above, we get the following isomorphism of $\mathcal{R}_{\mathcal{Q}}$-modules, for all $i \geqslant 1$:

$$\mathrm{Ext}^i_{\mathcal{R}}(\mathfrak{X}, \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \cong \mathrm{Ext}^{i+1}_{\mathcal{R}}(\mathrm{coker}(i_{\mathfrak{X}}), \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}. \tag{2.8}$$

In particular, we have the following isomorphism of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$\mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}, \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \cong \mathrm{Ext}^2_{\mathcal{R}}(\mathrm{coker}(i_{\mathfrak{X}}), \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}. \qquad \square$$

LEMMA 2.16. *Let $\mathcal{Z}$ be a finitely generated pseudonull $\mathcal{R}$-module. Let $\mathcal{Q}$ be a height two prime ideal in $\mathcal{R}$ such that $\mathcal{R}_{\mathcal{Q}}$ is Gorenstein. Then, we have the following equality of lengths of $\mathcal{R}_{\mathcal{Q}}$-modules:*

$$\mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}(\mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}})) = \mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}). \tag{2.9}$$

Proof. Without loss of generality, assume $\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ is not zero. As Lemma 2.3 indicates, we have

$$\mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}) < \infty, \quad \mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}(\mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}})) < \infty.$$

Suppose the following chain of $\mathcal{R}_{\mathcal{Q}}$-modules is a composition series for the $\mathcal{R}_{\mathcal{Q}}$-module $\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$:

$$\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} = \mathcal{M}_0 \supsetneq \mathcal{M}_1 \supsetneq \cdots \supsetneq \mathcal{M}_n = 0.$$

Consider the following short exact sequence of finitely generated pseudonull $\mathcal{R}_{\mathcal{Q}}$-modules:

$$0 \to \mathcal{M}_1 \to \mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to \frac{\mathcal{M}_0}{\mathcal{M}_1} \to 0. \tag{2.10}$$

By Corollary 2.12, we have the following short exact sequence of finitely generated pseudonull $\mathcal{R}_{\mathcal{Q}}$-modules:

$$0 \to \mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}\left(\frac{\mathcal{M}_0}{\mathcal{M}_1}, \mathcal{R}_{\mathcal{Q}}\right) \to \mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}) \to$$
$$\to \mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{M}_1, \mathcal{R}_{\mathcal{Q}}) \to 0. \tag{2.11}$$

If $\mathcal{M}_1$ equals zero, then the $\mathcal{R}_{\mathcal{Q}}$-module $\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ is isomorphic to $k_{\mathcal{Q}}$. Otherwise, note that

$$\mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{M}_1) < \mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}} \mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \quad \mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}\left(\frac{\mathcal{M}_0}{\mathcal{M}_1}\right) < \mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}} \mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}.$$

Suppose we could establish the following equality of lengths:

$$\mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{M}_1) \stackrel{?}{=} \mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}(\mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{M}_1, \mathcal{R}_{\mathcal{Q}})),$$

$$\mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}\left(\frac{\mathcal{M}_0}{\mathcal{M}_1}\right) \stackrel{?}{=} \mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}\left(\mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}\left(\frac{\mathcal{M}_0}{\mathcal{M}_1}, \mathcal{R}_{\mathcal{Q}}\right)\right). \tag{2.12}$$

As Lemma 2.1 indicates, length is additive in exact sequences. Equality in (2.12), along with the short exact sequences (2.10) and (2.11), would then let us obtain equation (2.9).

These observations let us use a dévissage argument to reduce to the case when $\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ equals $k_{\mathcal{Q}}$. The $\mathcal{R}_{\mathcal{Q}}$-module $\mathcal{R}_{\mathcal{Q}}$ is a canonical module (sometimes also called the dualizing module) for the Gorenstein local ring $\mathcal{R}_{\mathcal{Q}}$. See Theorem 3.3.7 in the book by Bruns and Herzog [**4**]. Consequently, we have the following isomorphism of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$\mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(k_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}) \cong k_{\mathcal{Q}}. \tag{2.13}$$

As a result, we have the following equality of lengths of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$\mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}(k_{\mathcal{Q}}) = \mathrm{Len}_{\mathcal{R}_{\mathcal{Q}}}(\mathrm{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(k_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}})) = 1.$$

This lets us deduce equation (2.9) when $\mathcal{Z} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ equals $k_{\mathcal{Q}}$. Hence, Lemma 2.16 follows.   □

Proposition 2.14 follows.

We would like to state one more application of Lemma 2.16. For each finitely generated $\mathcal{R}$-module $\mathcal{M}$, we let $\mathcal{M}_{\mathrm{P.N.}}$ denote the maximal pseudonull $\mathcal{R}$-submodule of $\mathcal{M}$.

LEMMA 2.17. *For every finitely generated $\mathcal{R}$-module $\mathcal{M}$, the $\mathcal{R}$-module $\mathrm{Ext}^2_{\mathcal{R}}(\mathcal{M}, \mathcal{R})$ is pseudonull. Furthermore, if we suppose that for every height two prime ideal $\mathcal{Q}$ in $\mathcal{R}$:*

- *$\mathcal{R}_{\mathcal{Q}}$ is a Gorenstein local ring, and*

- *the $\mathcal{R}_{\mathcal{Q}}$-module $\frac{\mathcal{M}}{\mathcal{M}_{\mathrm{P.N.}}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ has finite projective dimension.*

Then, we have the following equality in $Z^2(\mathcal{R})$:

$$c_2(\mathcal{M}_{\text{P.N.}}) = c_2(\text{Ext}^2_{\mathcal{R}}(\mathcal{M}, \mathcal{R})). \tag{2.14}$$

Proof. Let $\mathfrak{p}$ be a height one prime ideal in the ring $\mathcal{R}$. Since $\mathcal{R}$ is a Noetherian integrally closed local domain, the localization $\mathcal{R}_{\mathfrak{p}}$ is a DVR. As a result the localization $\text{Ext}^i_{\mathcal{R}}(\mathcal{M}, \mathcal{R}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}}$, which is isomorphic to the $\mathcal{R}_{\mathfrak{p}}$-module $\text{Ext}^i_{\mathcal{R}_{\mathfrak{p}}}(\mathcal{M}_{\mathfrak{p}}, \mathcal{R}_{\mathfrak{p}})$, vanishes for all $i \geqslant 2$. In particular, $\text{Ext}^2_{\mathcal{R}_{\mathfrak{p}}}(\mathcal{M}_{\mathfrak{p}}, \mathcal{R}_{\mathfrak{p}})$ vanishes. This lets us conclude that $\mathcal{R}$-module $\text{Ext}^2_{\mathcal{R}}(\mathcal{M}, \mathcal{R})$ is pseudonull.

Let $\mathcal{Q}$ be a height two prime ideal in $\mathcal{R}$. Since $\mathcal{R}_{\mathcal{Q}}$ is a Gorenstein ring, the injective dimension of the $\mathcal{R}_{\mathcal{Q}}$-module $\mathcal{R}_{\mathcal{Q}}$ must equal two. By Lemma 2 in Ch. 19 of Matsumura's book [**36**]

$$\text{Ext}^3_{\mathcal{R}_{\mathcal{Q}}}\left(\frac{\mathcal{M}}{\mathcal{M}_{\text{P.N.}}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}\right) = 0.$$

We will argue that $\text{pd}_{\mathcal{R}_{\mathcal{Q}}} \frac{\mathcal{M}}{\mathcal{M}_{\text{P.N.}}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \leqslant 1$. This is straightforward if $\frac{\mathcal{M}}{\mathcal{M}_{\text{P.N.}}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ equals zero. Let us consider the case when $\frac{\mathcal{M}}{\mathcal{M}_{\text{P.N.}}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ is not zero. Since $\mathcal{M}_{\text{P.N.}}$ is the maximal pseudonull $\mathcal{R}$-submodule of $\mathcal{M}$, the $\mathcal{R}$-module $\frac{\mathcal{M}}{\mathcal{M}_{\text{P.N.}}}$ has no nonzero pseudonull submodules. As a result the $\mathcal{R}_{\mathcal{Q}}$-module $\frac{\mathcal{M}}{\mathcal{M}_{\text{P.N.}}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ has no nonzero pseudonull submodules. Hence, we have $\text{Depth}_{\mathcal{R}_{\mathcal{Q}}} \frac{\mathcal{M}}{\mathcal{M}_{\text{P.N.}}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \geqslant 1$. The hypotheses of the lemma tell us that the $\mathcal{R}_{\mathcal{Q}}$-module $\frac{\mathcal{M}}{\mathcal{M}_{\text{P.N.}}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ has finite projective dimension. One can apply the Auslander–Buchsbaum equality over the two-dimensional local ring $\mathcal{R}_{\mathcal{Q}}$ to conclude that $\text{pd}_{\mathcal{R}_{\mathcal{Q}}} \frac{\mathcal{M}}{\mathcal{M}_{\text{P.N.}}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \leqslant 1$.

By Lemma 2 in Ch. 19 of Matsumura's book [**36**], we have

$$\text{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}\left(\frac{\mathcal{M}}{\mathcal{M}_{\text{P.N.}}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}\right) = 0.$$

Applying the functor $\text{Hom}_{\mathcal{R}_{\mathcal{Q}}}(-, \mathcal{R}_{\mathcal{Q}})$ to the short exact sequence

$$0 \to \mathcal{M}_{\text{P.N.}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to \mathcal{M} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to \frac{\mathcal{M}}{\mathcal{M}_{\text{P.N.}}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to 0$$

of $\mathcal{R}_{\mathcal{Q}}$-modules lets us obtain the following isomorphism of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$\text{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{M} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}) \cong \text{Ext}^2_{\mathcal{R}_{\mathcal{Q}}}(\mathcal{M}_{\text{P.N.}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{Q}}). \tag{2.15}$$

Using Lemma 2.16, we obtain the following equality in $Z^2(\mathcal{R})$:

$$c_2(M_{\text{P.N.}}) = c_2(\text{Ext}^2_{\mathcal{R}}(\mathcal{M}_{\text{P.N.}}, \mathcal{R})) = c_2(\text{Ext}^2_{\mathcal{R}}(\mathcal{M}, \mathcal{R})).$$

This completes the proof of the Lemma. □

3. The general setup

We will obtain our results from a general perspective in Section 4. In this section, we will simply outline the various objects involved in describing the general results. Let $\mathcal{R}$ denote a Noetherian, complete, integrally closed, local domain, with Krull dimension $n + 1$, characteristic zero and whose residue field is finite with characteristic p. Cohen's structure theorems tell us that there exists a subring Λ_n of $\mathcal{R}$ that is isomorphic to the power series $\mathbb{Z}_p[[x_1, \ldots, x_n]]$. Let $\mathfrak{m}_{\mathcal{R}}$ denote the maximal ideal of $\mathcal{R}$. Let Σ denote a finite set of primes of $\mathbb{Q}$, containing p, ∞ and a finite prime $l_0 \neq p$. Let $\mathbb{Q}_\Sigma$ denote the maximal extension of $\mathbb{Q}$ unramified outside Σ. Let G_Σ denote the Galois group $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$.

Consider a continuous Galois representation

$$\rho_{d,n} : G_\Sigma \to \mathrm{GL}_d(\mathcal{R}).$$

Let $T_{\rho_{d,n}}$ denote the underlying free $\mathcal{R}$-module of rank n on which G_Σ-module acts to let us obtain $\rho_{d,n}$. We will let $d^+(\rho_{d,n})$ be the rank of $\mathcal{R}$-submodule of $T_{\rho_{d,n}}$ fixed by complex conjugation. We let $d^-(\rho_{d,n})$ equal $d - d^+(\rho_{d,n})$. Note that $\mathcal{R}^\vee$ denotes $\mathrm{Hom}_{\mathrm{cont}}(\mathcal{R}, \mathbb{Q}_p/\mathbb{Z}_p)$.

We shall also consider the Galois representation $\rho_{d,n}^\star : G_\Sigma \to \mathrm{GL}_d(\mathcal{R})$, given by the action of G_Σ on $T_{\rho_{d,n}^\star} := \mathrm{Hom}_{\mathcal{R}}(T_{\rho_{d,n}}, \mathcal{R}(\chi_p))$. Here, $\mathcal{R}(\chi_p)$ is the free $\mathcal{R}$-module of rank one on which G_Σ acts via the p-adic cyclotomic character

$$\chi_p : G_\Sigma \to \mathbb{Z}_p^\times.$$

To each of these Galois representation, one can attach the following discrete modules:

$$D_{\rho_{d,n}} := T_{\rho_{d,n}} \otimes_{\mathcal{R}} \mathcal{R}^\vee, \quad D_{\rho_{d,n}^\star} := T_{\rho_{d,n}^\star} \otimes_{\mathcal{R}} \mathcal{R}^\vee.$$

The various modules appearing in the general results are described in Section 3.1.1. To define these modules, we will need to consider various subgroups of the first discrete global Galois cohomology group $H^1(G_\Sigma, D_{\rho_{d,n}})$. In turn, to define the subgroups of the first global Galois cohomology group, we will need to consider local Selmer conditions, which are subgroups of the first discrete local cohomology group at the prime p. We will simply suppose that we have two discrete $\mathcal{R}$-submodules, $\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}})$ and $\mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})$, inside the first local Galois cohomology group $H^1(\mathbb{Q}_p, D_{\rho_{d,n}})$. That is, we have the following inclusions of $\mathcal{R}$-modules:

$$\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \subset H^1(\mathbb{Q}_p, D_{\rho_{d,n}}), \quad \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \subset H^1(\mathbb{Q}_p, D_{\rho_{d,n}}).$$

The properties, that these local factors at p need to satisfy, will be described in Section 3.1.2.

3.1. Various modules, assumptions and hypotheses.

3.1.1. Descriptions of the various modules. We let $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})$ denote the Pontryagin dual of

$$\ker\left(H^1(G_\Sigma, D_{\rho_{d,n}}) \xrightarrow{\phi_{\mathfrak{X}}} \frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_\mathrm{I}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_\mathrm{II}(\mathbb{Q}_p, D_{\rho_{d,n}})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}}) \right).$$

We let $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})_\mathrm{tor}$ denote the $\mathcal{R}$-torsion submodule of $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})$.

We shall define two discrete Selmer groups $\mathrm{Sel}_\mathrm{I}(\mathbb{Q}, D_{\rho_{d,n}})$ and $\mathrm{Sel}_\mathrm{II}(\mathbb{Q}, D_{\rho_{d,n}})$ as follows:

$$\mathrm{Sel}_\mathrm{I}(\mathbb{Q}, D_{\rho_{d,n}}) := \ker(H^1(G_\Sigma, D_{\rho_{d,n}}) \xrightarrow{\phi_\mathrm{I}} \frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_\mathrm{I}(\mathbb{Q}_p, D_{\rho_{d,n}})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}})),$$

$$\mathrm{Sel}_\mathrm{II}(\mathbb{Q}, D_{\rho_{d,n}}) := \ker(H^1(G_\Sigma, D_{\rho_{d,n}}) \xrightarrow{\phi_\mathrm{II}} \frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_\mathrm{II}(\mathbb{Q}_p, D_{\rho_{d,n}})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}})).$$

For each $i \in \{1, 2\}$, we will define the following discrete subgroup, labelled $\mathrm{III}^i(\mathbb{Q}, D_{\rho_{d,n}})$, of the global Galois cohomology group $H^i(G_\Sigma, D_{\rho_{d,n}})$:

$$\mathrm{III}^i(\mathbb{Q}, D_{\rho_{d,n}}) := \ker\left(H^i(G_\Sigma, D_{\rho_{d,n}}) \to \bigoplus_{l \in \Sigma} H^i(\mathbb{Q}_l, D_{\rho_{d,n}}) \right).$$

For each $i \in \{1, 2\}$, one can similarly define $\mathrm{III}^i(\mathbb{Q}, D_{\rho_{d,n}^\star})$ inside the global Galois cohomology group $H^i(G_\Sigma, D_{\rho_{d,n}^\star})$.

We let $\mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}})$ denote the Pontryagin dual of

$$\ker\left(H^1(G_\Sigma, D_{\rho_{d,n}}) \to \frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_\mathrm{I}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_\mathrm{II}(\mathbb{Q}_p, D_{\rho_{d,n}})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}}) \right).$$

(3.1)

It will be helpful to keep following surjections of $\mathcal{R}$-modules in mind:

$$H^1(G_\Sigma, D_{\rho_{d,n}})^\vee \twoheadrightarrow \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}) \twoheadrightarrow \frac{\mathrm{Sel}_\mathrm{I}(\mathbb{Q}, D_{\rho_{d,n}})^\vee}{\mathrm{Sel}_\mathrm{II}(\mathbb{Q}, D_{\rho_{d,n}})^\vee} \twoheadrightarrow \mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}}) \twoheadrightarrow \mathrm{III}^1(\mathbb{Q}, D_{\rho_{d,n}})^\vee.$$

(3.2)

REMARK 3.1. If one follows Greenberg's definition of Selmer groups in [**14**], one requires the global cocycles to be unramified at primes $l \in \Sigma \setminus \{p\}$. This point will not matter to us since for our applications, we will be considering Galois representations $\rho_{d,n}$ that are related to cyclotomic deformations (following the notations in [**14**, Section 3]). For such representations, the natural restriction map $H^1(\mathbb{Q}_l, D_{\rho_{d,n}}) \to H^1(I_l, D_{\rho_{d,n}})$ turns out to be injective, whenever $l \neq p$. Here, I_l is the inertia subgroup inside the decomposition group $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$.

3.1.2.   Statements of the various assumptions and hypotheses. We will deduce our results under various conditions. Some of these conditions will have the prefix 'Assumption'. Some of these conditions will have the prefix 'Hypothesis'. The conditions with the prefix 'Hypothesis' are those conditions which we will be able to establish in the setting of Theorem 1. In the setting of Theorem 1, the conditions labelled 'Assumptions' are currently not known to always hold unconditionally.

Assumption MC   We have the following equality of ranks

$$\mathrm{Rank}_{\mathcal{R}} \ \mathrm{Sel}_{\mathrm{I}}(\mathbb{Q}, D_{\rho_{d,n}})^{\vee} = 0, \quad \mathrm{Rank}_{\mathcal{R}} \ \mathrm{Sel}_{\mathrm{II}}(\mathbb{Q}, D_{\rho_{d,n}})^{\vee} = 0. \tag{3.3}$$

In addition, there exist two elements θ_{I} and θ_{II} in $\mathcal{R}$ such that we have the following equalities in $Z^1(\mathcal{R})$:

$$\mathrm{Div}(\mathrm{Sel}_{\mathrm{I}}(\mathbb{Q}, D_{\rho_{d,n}})^{\vee}) = \mathrm{Div}(\theta_{\mathrm{I}}),$$
$$\mathrm{Div}(\mathrm{Sel}_{\mathrm{II}}(\mathbb{Q}, D_{\rho_{d,n}})^{\vee}) = \mathrm{Div}(\theta_{\mathrm{II}}). \tag{3.4}$$

Assumption GCD   The height of the ideal $(\theta_{\mathrm{I}}, \theta_{\mathrm{II}})$ in $\mathcal{R}$ is greater than or equal to two.

In the statement of Assumption GCD, θ_{I} and θ_{II} are the elements appearing in the statement of Assumption MC.

Hypothesis Rank   We have the following equality of ranks:

$$\mathrm{Rank}_{\mathcal{R}} \ \mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}})^{\vee}$$
$$= \mathrm{Rank}_{\mathcal{R}} \ \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})^{\vee} = d^+,$$

$$\mathrm{Rank}_{\mathcal{R}} \ (\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}))^{\vee}$$
$$= d^+ + 1.$$

Hypothesis LF   The following $\mathcal{R}$-modules are free:

$$\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}})^{\vee}, \quad \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})^{\vee},$$
$$\left(\frac{\mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})} \right)^{\vee},$$
$$\left(\frac{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})} \right)^{\vee}.$$

Hypothesis $\mathrm{Loc}_p(0)$ The $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules $D_{\rho_{d,n}}[\mathfrak{m}_{\mathcal{R}}]$ and $D_{\rho_{d,n}^\star}[\mathfrak{m}_{\mathcal{R}}]$ have no quotient isomorphic to the trivial representation.

Hypothesis $\mathrm{Loc}(0)$ For every l in Σ, we have

$$\mathrm{Rank}_{\mathcal{R}}\, H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee = \mathrm{Rank}_{\mathcal{R}}\, H^0(\mathbb{Q}_l, D_{\rho_{d,n}^\star})^\vee = 0.$$

Hypothesis $\mathrm{Reg}(0)$ For every prime $l \in \Sigma \setminus \{p\}$ and every height two prime ideal $\mathcal{Q}$ in $\mathcal{R}$, the $\mathcal{R}_{\mathcal{Q}}$-module $H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ has finite projective dimension.

Hypothesis Gor $\mathcal{R}$ is a Gorenstein local ring.

REMARK 3.2. In the setup of Theorem 1, the ring $\mathcal{R}$ (which is isomorphic to the power series ring $\mathbb{Z}_p[[x_1, x_2]]$) is a regular local ring. Hypothesis Gor and Hypothesis Reg(0) are automatically valid.

REMARK 3.3. When the ring $\mathcal{R}$ is a UFD, Assumption GCD is equivalent to the statement that the elements θ_{I} and θ_{II} have no common irreducible factor.

REMARK 3.4. We would like to make a few remarks concerning Assumption MC. Since our approach towards proving Theorem 1 only involves studying the module theory of Galois cohomology groups, we have not defined p-adic L-functions in the general setup. One must view the statements in Assumption MC simply as abstract formulations of Iwasawa main conjectures (just as in Section 3 of the seven-author paper [3]). The content of equation (3.4) in Assumption MC is significant only when the ring $\mathcal{R}$ is not a UFD.

When the Galois representation $\rho_{d,n}$ satisfies the Panchishkin condition, the Iwasawa main conjecture (formulated in [14]) predicts an equality between the divisor associated to the p-adic L-function (say θ_{I}) and the divisor

$$\mathrm{Div}(\mathrm{Sel}_{\mathrm{I}}(\mathbb{Q}, D_{\rho_{d,n}})^\vee) - \mathrm{Div}(H^0(G_\Sigma, D_{\rho_{d,n}})^\vee) - \mathrm{Div}(H^0(G_\Sigma, D_{\rho_{d,n}^\star})^\vee)$$

in $Z^1(\mathcal{R})$. In our situation, Hypothesis $\mathrm{Loc}_p(0)$ lets us deduce that

$$H^0(G_\Sigma, D_{\rho_{d,n}}) = H^0(G_\Sigma, D_{\rho_{d,n}^\star}) = 0.$$

REMARK 3.5. While it seems reasonable to expect Assumption MC to always hold in the setup of Theorem 1, we do not know whether Assumption GCD always holds in this setup. However, we do produce some evidence towards the validity of Assumption GCD in the setup of Theorem 1 in Section 8.

3.2. Consequences of the various hypotheses and assumptions.

(a) Note that we have a natural isomorphism:

$$\left(\frac{\text{Loc}_\text{I}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \text{Loc}_\text{II}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\text{Loc}_\text{I}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^\vee$$
$$\cong \left(\frac{\text{Loc}_\text{II}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\text{Loc}_\text{I}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \text{Loc}_\text{II}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^\vee.$$

This observation, Hypothesis LF and the (split) short exact sequence

$$0 \to \left(\frac{\text{Loc}_\text{I}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \text{Loc}_\text{II}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\text{Loc}_\text{I}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^\vee \to$$
$$\to (\text{Loc}_\text{I}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \text{Loc}_\text{II}(\mathbb{Q}_p, D_{\rho_{d,n}}))^\vee \to \text{Loc}_\text{I}(\mathbb{Q}_p, D_{\rho_{d,n}})^\vee \to$$
$$\to 0,$$

let us conclude that the $\mathcal{R}$-module $(\text{Loc}_\text{I}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \text{Loc}_\text{II}(\mathbb{Q}_p, D_{\rho_{d,n}}))^\vee$ is free.

(b) As a result of local duality theorems (for example, see Section 0.3 in Nekovář's work on Selmer complexes [37]), Hypothesis Loc(0) and [16, Proposition 3.10], for all primes $l \in \Sigma$, we have

$$\begin{aligned} H^0_\text{ct}(\mathbb{Q}_l, T_{\rho_{d,n}^\star}) &= H^0_\text{ct}(\mathbb{Q}_l, T_{\rho_{d,n}}) = 0, \\ H^2(\mathbb{Q}_l, D_{\rho_{d,n}}) &= H^2(\mathbb{Q}_l, D_{\rho_{d,n}^\star}) = 0. \end{aligned} \tag{3.5}$$

As a result, for the zeroth global Galois cohomology groups, we also have

$$H^0_\text{ct}(G_\Sigma, T_{\rho_{d,n}}) = H^0_\text{ct}(G_\Sigma, T_{\rho_{d,n}^\star}) = 0. \tag{3.6}$$

(c) Hypothesis $\text{Loc}_\text{p}(0)$ lets us conclude that

$$\begin{aligned} H^0(\mathbb{Q}_p, D_{\rho_{d,n}}) &= H^0(\mathbb{Q}_p, D_{\rho_{d,n}^\star}) = 0, \\ H^2(\mathbb{Q}_p, D_{\rho_{d,n}}) &= H^2(\mathbb{Q}_p, D_{\rho_{d,n}^\star}) = 0. \end{aligned} \tag{3.7}$$

As a result, for the zeroth global Galois cohomology groups, we also have

$$H^0(G_\Sigma, D_{\rho_{d,n}}) = H^0(G_\Sigma, D_{\rho_{d,n}^\star}) = 0. \tag{3.8}$$

(d) By studying the local and global Euler Poincaré characteristics and using equation (3.3) and Hypothesis Rank, one can conclude that the Weak Leopoldt conjecture for $\rho_{d,n}$ holds. That is, the $\mathcal{R}$-module $\text{III}^2(\mathbb{Q}, D_{\rho_{d,n}})^\vee$ is torsion (in fact, equal to zero). See [40, Proposition 4.6]. In fact, in our situation, Proposition 6.1 in [16] lets us conclude that

$$H^2(G_\Sigma, D_{\rho_{d,n}}) = 0. \tag{3.9}$$

(e) The maps Φ_{I} and Φ_{II} are surjective. This follows by applying [**17**, Proposition 3.2.1] and using Hypothesis $\mathrm{Loc_p}(0)$.

(f) All the hypotheses in Proposition 4.1.1 listed in [**18**] can be verified to let us conclude that $\mathcal{R}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})$ has no nonzero pseudonull submodules. The fact, that the $\mathcal{R}$-module $(\mathrm{Loc_I}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc_{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}))^\vee$ is free, comes into play.

3.2.1. Various commutative diagrams. Let $J \in \{\mathrm{I}, \mathrm{II}\}$. To relate the various modules in this general setup, it will be helpful to keep the following commutative diagrams in mind:

$$
\begin{array}{ccc}
H^1(G_\Sigma, D_{\rho_{d,n}}) & \xrightarrow{\;\cong\;} & H^1(G_\Sigma, D_{\rho_{d,n}}) \\
\downarrow{\scriptstyle \phi_J} & & \downarrow{\scriptstyle \phi_{\mathfrak{X}}} \\
\frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_J(\mathbb{Q}_p, D_{\rho_{d,n}})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}}) & \longrightarrow & \frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc_I}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc_{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}})
\end{array}
$$

(Commutative diagram A)

$$
\begin{array}{ccc}
H^1(G_\Sigma, D_{\rho_{d,n}}) & \xrightarrow{\;\cong\;} & H^1(G_\Sigma, D_{\rho_{d,n}}) \\
\downarrow{\scriptstyle \phi_{\mathcal{Z}}} & & \downarrow{\scriptstyle \phi_{\mathfrak{X}}} \\
\frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc_I}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc_{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}}) & \longrightarrow & \frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc_I}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc_{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}})
\end{array}
$$

(Commutative diagram B)

$$
\begin{array}{ccc}
H^1(G_\Sigma, D_{\rho_{d,n}}) & \xrightarrow{\;\cong\;} & H^1(G_\Sigma, D_{\rho_{d,n}}) \\
\downarrow{\scriptstyle \phi_{\mathcal{Z}}} & & \downarrow{\scriptstyle \phi_J} \\
\frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc_I}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc_{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}}) & \longrightarrow & \frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_J(\mathbb{Q}_p, D_{\rho_{d,n}})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}})
\end{array}
$$

(Commutative diagram C)

LEMMA 3.6. *Suppose all the hypotheses and assumptions in Section 3.1.2 hold. Then, the map $\phi_{\mathfrak{X}}$ is surjective. We also have the following short exact sequences of $\mathcal{R}$-modules:*

$$
0 \to \left(\frac{\mathrm{Loc_{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc_I}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc_{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})} \right)^\vee \to \mathfrak{X}(D_{\rho_{d,n}}, \mathbb{Q}) \to \mathrm{Sel_I}(\mathbb{Q}, D_{\rho_{d,n}})^\vee \to 0, \quad (3.10)
$$

$$
0 \to \left(\frac{\mathrm{Loc_I}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc_I}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc_{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})} \right)^\vee \to \mathfrak{X}(D_{\rho_{d,n}}, \mathbb{Q}) \to \mathrm{Sel_{II}}(\mathbb{Q}, D_{\rho_{d,n}})^\vee \to 0, \quad (3.11)
$$

$$\left(\frac{\text{Loc}_{\text{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \text{Loc}_{\text{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\text{Loc}_{\text{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \text{Loc}_{\text{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^{\vee} \to \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}) \to \mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}}) \to 0, \quad (3.12)$$

$$\left(\frac{\text{Loc}_{\text{I}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\text{Loc}_{\text{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \text{Loc}_{\text{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^{\vee} \to \text{Sel}_{\text{I}}(\mathbb{Q}, D_{\rho_{d,n}})^{\vee} \to \mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}}) \to 0, \quad (3.13)$$

$$\left(\frac{\text{Loc}_{\text{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\text{Loc}_{\text{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \text{Loc}_{\text{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^{\vee} \to \text{Sel}_{\text{II}}(\mathbb{Q}, D_{\rho_{d,n}})^{\vee} \to \mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}}) \to 0. \quad (3.14)$$

Proof. The maps Φ_{I} and Φ_{II} are surjective. The lemma follows by applying the Snake Lemma to the commutative diagrams given above. $\square$

3.3. Consequences of duality theorems. Recall that the ring $\mathcal{R}$ is a Gorenstein local ring whose residue field is finite with characteristic p. The dualizing module, often denoted by $\omega_{\mathcal{R}}$, is isomorphic to $\mathcal{R}$.

Let $\mathcal{G}$ denote a profinite group satisfying the following conditions:

(F) $H^i(\mathcal{G}, M)$ is finite for all $i \geqslant 0$ and for every finite $\mathcal{R}$-module M (that is, the cardinality of M is finite) equipped with a continuous $\mathcal{R}$-linear action of the profinite group $\mathcal{G}$.

(CD) The p-cohomological dimension of $\mathcal{G}$ is less than or equal to 2.

REMARK 3.7. Note that conditions (F) and (CD) are both valid when the profinite group $\mathcal{G}$ equals the local decomposition $\text{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ for any prime $l \in \Sigma$, or the global Galois group G_Σ.

Let $\mathcal{T}$ denote a finitely generated $\mathcal{R}$-module with a continuous $\mathcal{R}$-linear $\mathcal{G}$-action. Let $\mathcal{D}$ denote the discrete $\mathcal{R}$-module $\mathcal{T} \otimes_{\mathcal{R}} \mathcal{R}^{\vee}$. Observe that $\mathcal{D}$ also has a natural continuous $\mathcal{R}$-linear action of $\mathcal{G}$.

Let $\mathbf{D}^+(\mathcal{R} - \text{mod})$ denote the subcategory of the derived category of finitely generated $\mathcal{R}$-modules, whose objects are chain complexes that are bounded from below. Proposition 4.2.5 in Nekovář's work on Selmer complexes [37] shows that we have

$$D(\mathbf{R}\boldsymbol{\Gamma}_{\text{cont}}(\mathcal{G}, \mathcal{D})) \in \mathbf{D}^+(\mathcal{R} - \text{mod}), \quad \mathbf{R}\boldsymbol{\Gamma}_{\text{cont}}(\mathcal{G}, \mathcal{T}) \in \mathbf{D}^+(\mathcal{R} - \text{mod}),$$

such that we have the following isomorphism of $\mathcal{R}$-modules, for all $j \geqslant 0$:

$$H^j(D(\mathbf{R}\boldsymbol{\Gamma}_{\text{cont}}(\mathcal{G}, \mathcal{D}))) \cong H^j(\mathcal{G}, \mathcal{D})^{\vee}, \quad H^j(\mathbf{R}\boldsymbol{\Gamma}_{\text{cont}}(\mathcal{G}, \mathcal{T})) \cong H^j_{\text{ct}}(\mathcal{G}, \mathcal{T}). \tag{3.15}$$

Here, $H^j(\mathcal{G}, \mathcal{D})$ (and $H^j_{\text{ct}}(\mathcal{G}, \mathcal{T})$ respectively) denote the discrete (and compact respectively) Galois cohomology groups for the continuous action of $\mathcal{G}$ on $\mathcal{D}$ (and $\mathcal{T}$ respectively).

To state Nekovář's results, one needs to use the notion of *hyperext* groups (denoted by $\mathbb{E}\mathrm{xt}(-,-)$) in the derived category $\mathbf{D}^+(\mathcal{R}-\mathrm{mod})$. See Section 6 in Ch. I of Hartshorne's book on Residues and Duality [20] for the definition of hyperext groups. Nekovář has deduced the following *hyper-cohomology* spectral sequence:

$$\mathbb{E}\mathrm{xt}^i(H^j(\mathcal{G},\mathcal{D})^\vee,\mathcal{R}) \implies H_{\mathrm{ct}}^{i+j}(\mathcal{G},\mathcal{T}). \tag{3.16}$$

See equation (4.3.1.2) in Section 4.3 of his work on Selmer complexes [37]. Using Corollary 6.1 in Ch. I of Hartshorne's book [20] (see also Corollary 10.7.5 in Weibel's book [63]), we have the following isomorphism of $\mathcal{R}$-modules:

$$\mathbb{E}\mathrm{xt}^i(H^j(\mathcal{G},\mathcal{D})^\vee,\mathcal{R}) \cong \mathrm{Ext}_{\mathcal{R}}^i(H^j(\mathcal{G},\mathcal{D})^\vee,\mathcal{R}). \tag{3.17}$$

We shall suppose the following conditions hold:

$$H^2(\mathcal{G},\mathcal{D})=0, \quad H_{\mathrm{ct}}^0(\mathcal{G},\mathcal{T})=0. \tag{3.18}$$

The spectral sequence (3.16) lets us obtain the exact sequences of $\mathcal{R}$-modules:

$$0 \to \mathrm{Ext}_{\mathcal{R}}^1(H^0(\mathcal{G},\mathcal{D})^\vee,\mathcal{R}) \to H_{\mathrm{ct}}^1(\mathcal{G},\mathcal{T}) \to$$
$$\to \mathrm{Ext}_{\mathcal{R}}^0(H^1(\mathcal{G},\mathcal{D})^\vee,\mathcal{R}) \to \mathrm{Ext}_{\mathcal{R}}^2(H^0(\mathcal{G},\mathcal{D})^\vee,\mathcal{R}), \tag{3.19}$$

and

$$\mathrm{Ext}_{\mathcal{R}}^0(H^1(\mathcal{G},\mathcal{D})^\vee,\mathcal{R}) \to \mathrm{Ext}_{\mathcal{R}}^2(H^0(\mathcal{G},\mathcal{D})^\vee,\mathcal{R}) \to H_{\mathrm{ct}}^2(\mathcal{G},\mathcal{T}) \to$$
$$\to \mathrm{Ext}_{\mathcal{R}}^1(H^1(\mathcal{G},\mathcal{D})^\vee,\mathcal{R}) \to \mathrm{Ext}_{\mathcal{R}}^3(H^0(\mathcal{G},\mathcal{D})^\vee,\mathcal{R}). \tag{3.20}$$

3.3.1. Consequences for local Galois cohomology groups, $l=p$. By equation (3.5), we have

$$H^2(\mathbb{Q}_p,D_{\rho_{d,n}})=0, \quad H_{\mathrm{ct}}^0(\mathbb{Q}_p,T_{\rho_{d,n}})^\vee=0.$$

Equation (3.7) lets us deduce that

$$H^0(\mathbb{Q}_p,D_{\rho_{d,n}})^\vee=0.$$

Hypothesis $\mathrm{Loc}_p(0)$ along with Proposition 5.10 (see also Remark 5.10.1) in Greenberg's work [16] lets us conclude that the $\mathcal{R}$-module $H^1(\mathbb{Q}_p,D_{\rho_{d,n}})^\vee$ is free. So, we have

$$\mathrm{Ext}_{\mathcal{R}}^i(H^1(\mathbb{Q}_p,D_{\rho_{d,n}})^\vee,\mathcal{R})=0, \quad \forall i \geqslant 1. \tag{3.21}$$

We have the following lemma:

LEMMA 3.8. *Suppose all the hypotheses and assumptions in Section* 3.1.2 *hold. Then, the $\mathcal{R}$-module $((H^1(\mathbb{Q}_p, D_{\rho_{d,n}}))/(\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})))^\vee$ is free. Consequently,*

$$\mathrm{Ext}^i_{\mathcal{R}}\left(\left(\frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^\vee, \mathcal{R}\right) = 0, \quad \forall i \geqslant 1.$$

Proof. The lemma follows directly using the following short exact sequence:

$$0 \to \left(\frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^\vee \to \underbrace{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})^\vee}_{\text{free over } \mathcal{R}} \to$$

$$\to \underbrace{(\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}))^\vee}_{\text{free over } \mathcal{R}} \to 0 \qquad \square$$

The observations in Section 3.2 along with equation (3.19) let us obtain the following isomorphisms of $\mathcal{R}$-modules:

$$\mathrm{Hom}_{\mathcal{R}}(H^1(\mathbb{Q}_p, D_{\rho_{d,n}})^\vee, \mathcal{R}) \cong H^1_{\mathrm{ct}}(\mathbb{Q}_p, T_{\rho_{d,n}}),$$
$$\cong H^1(\mathbb{Q}_p, D_{\rho^\star_{d,n}})^\vee, \quad \text{(local duality).} \quad (3.22)$$

The natural injection of $\mathcal{R}$-modules

$$\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \hookrightarrow H^1(\mathbb{Q}_p, \mathcal{D}_{\rho_{d,n}})$$

gives us the following natural surjections of $\mathcal{R}$-modules (by considering Pontryagin duals)

$$H^1(\mathbb{Q}_p, D_{\rho_{d,n}})^\vee \twoheadrightarrow (\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}))^\vee,$$

which in turn let us obtain the following natural injections of $\mathcal{R}$-modules (by considering reflexive duals and the isomorphism in equation (3.22)):

$$((\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}))^\vee)^* \hookrightarrow H^1_{\mathrm{ct}}(\mathbb{Q}_p, T_{\rho_{d,n}}).$$

Under the perfect pairing given by local duality

$$H^1(\mathbb{Q}_p, D_{\rho^\star_{d,n}}) \times H^1_{\mathrm{ct}}(\mathbb{Q}_p, T_{\rho_{d,n}}) \to \frac{\mathbb{Q}_p}{\mathbb{Z}_p},$$

we define

$$\mathrm{Loc}_{\mathrm{I},\mathrm{II}}(\mathbb{Q}_p, D_{\rho^\star_{d,n}}) \subset H^1(\mathbb{Q}_p, D_{\rho^\star_{d,n}}),$$

to be the orthogonal complement of $((\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}))^\vee)^*$ under the pairing given above.

We define $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^\star})$ to be the Pontryagin dual of

$$\ker\left(H^1(G_\Sigma, D_{\rho_{d,n}^\star}) \to \frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}^\star})}{\mathrm{Loc}_{\mathrm{I,II}}(\mathbb{Q}_p, D_{\rho_{d,n}^\star})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}^\star}) \right). \quad (3.23)$$

Note that we have the following natural surjection of $\mathcal{R}$-modules:

$$\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^\star}) \twoheadrightarrow \mathrm{III}^1(\mathbb{Q}, D_{\rho_{d,n}^\star})^\vee.$$

REMARK 3.9. This definition of $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^\star})$ in equation (3.23) does not match the description given in equation (3.1) for the Galois representation $\rho_{d,n}^\star$ and, in fact, it need not in general. See Section 7.2 for a description of $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^\star})$ in the setting of Theorem 1 and Remark 7.12 for when these descriptions do match.

LEMMA 3.10. *Suppose all the hypotheses and assumptions in Section* 3.1.2 *hold. We have the following natural isomorphism of $\mathcal{R}$-modules:*

$$\frac{(H^1(\mathbb{Q}_p, D_{\rho_{d,n}})^\vee)^*}{((\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}))^\vee)^*}$$
$$\cong \left(\left(\frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})} \right)^\vee \right)^*$$

Proof. The lemma follows directly using the observation 3.2 in Section 3.2 and the following short exact sequence of free $\mathcal{R}$-modules:

$$0 \to \left(\frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})} \right)^\vee \to$$
$$\to H^1(\mathbb{Q}_p, D_{\rho_{d,n}})^\vee \to (\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}, \mathbb{Q}_p) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}))^\vee \to$$
$$\to 0. \qquad \square$$

3.3.2. Consequences for local Galois cohomology groups, $l \neq p$. Note that Hypothesis Loc(0) lets us conclude that

$$\mathrm{Hom}_\mathcal{R}(H^1(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee, \mathcal{R}) = 0. \quad (3.24)$$

Let $\mathcal{Q}$ be a height two prime ideal in the ring $\mathcal{R}$. Since the ring $\mathcal{R}$ is Gorenstein, the localization $\mathcal{R}_\mathcal{Q}$ is also a Gorenstein ring with Krull dimension two. The injective dimension of the $\mathcal{R}_\mathcal{Q}$-module $\mathcal{R}_\mathcal{Q}$ equals two. By Lemma 2 in Ch. 19 of Matsumura's book [36], we have

$$\mathrm{Ext}^3_\mathcal{R}(H^0(\mathcal{G}, \mathcal{D})^\vee, \mathcal{R}) \otimes_\mathcal{R} \mathcal{R}_\mathcal{Q} \cong \mathrm{Ext}^3_{\mathcal{R}_\mathcal{Q}}(H^0(\mathcal{G}, \mathcal{D})^\vee \otimes_\mathcal{R} \mathcal{R}_\mathcal{Q}, \mathcal{R}_\mathcal{Q}) = 0.$$

Using equation (3.20), we have the following short exact sequence of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$0 \to \mathrm{Ext}^2_{\mathcal{R}}(H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee, \mathcal{R})_{\mathcal{Q}} \to H^2_{\mathrm{ct}}(\mathbb{Q}_l, T_{\rho_{d,n}})_{\mathcal{Q}} \to$$
$$\to \mathrm{Ext}^1_{\mathcal{R}}(H^1(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee, \mathcal{R})_{\mathcal{Q}} \to 0. \tag{3.25}$$

3.3.3. Consequences for global Galois cohomology groups. By equations (3.6) and (3.9), we have

$$H^2(G_\Sigma, D_{\rho_{d,n}}) = 0, \quad H^0_{\mathrm{ct}}(G_\Sigma, T_{\rho_{d,n}})^\vee = 0.$$

Equation (3.8) lets us deduce that

$$H^0(G_\Sigma, D_{\rho_{d,n}})^\vee = 0.$$

Using (3.19) and (3.20), we have the following isomorphisms of $\mathcal{R}$-modules:

$$H^1_{\mathrm{ct}}(G_\Sigma, T_{\rho_{d,n}}) \cong \mathrm{Hom}_{\mathcal{R}}(H^1(G_\Sigma, D_{\rho_{d,n}})^\vee, \mathcal{R}),$$
$$H^2_{\mathrm{ct}}(G_\Sigma, T_{\rho_{d,n}}) \cong \mathrm{Ext}^1_{\mathcal{R}}(H^1(G_\Sigma, D_{\rho_{d,n}})^\vee, \mathcal{R}). \tag{3.26}$$

3.3.4. Consequences for the module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})$.

PROPOSITION 3.11. *Suppose all the hypotheses and assumptions in Section 3.1.2 hold. Then, the $\mathcal{R}$-module $\mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}), \mathcal{R})$ is pseudonull if and only if $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho^\star_{d,n}})$ is pseudonull. Furthermore, if the $\mathcal{R}$-module $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho^\star_{d,n}})$ is pseudonull, then we have the following equality in $Z^2(\mathcal{R})$:*

$$c_2(\mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}), \mathcal{R})) = c_2(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho^\star_{d,n}}))$$
$$+ \sum_{l \in \Sigma \setminus \{p\}} c_2((H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee)_{\mathrm{P.N.}}).$$

Proof. To prove that an $\mathcal{R}$-module $\mathcal{M}$ is pseudonull, it suffices to show that the $\mathcal{R}_{\mathcal{Q}}$-module $\mathcal{M}_{\mathcal{Q}}$ is pseudonull for every height two prime ideal $\mathcal{Q}$ in $\mathcal{R}$.

By Lemma 3.6, the map $\Phi_{\mathfrak{X}}$ is surjective. So, we have the following short exact sequence of $\mathcal{R}$-modules:

$$0 \to \left(\frac{H^1(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^\vee \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee \to$$
$$\to H^1(G_\Sigma, D_{\rho_{d,n}})^\vee \to \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}) \to 0.$$

Apply the functor $\mathrm{Hom}_{\mathcal{R}}(-, \mathcal{R})$. Use Lemmas 3.8 and 3.10 along with the isomorphisms given in equations (3.24) and (3.26). We obtain the following long exact sequence of $\mathcal{R}$-modules:

$$H^1_{\mathrm{ct}}(G_{\Sigma}, T_{\rho_{d,n}}) \to \frac{H^1_{\mathrm{ct}}(\mathbb{Q}_p, T_{\rho_{d,n}})}{((\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}))^{\vee})^*} \to$$

$$\to \mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}), \mathcal{R}) \to$$

$$\to H^2_{\mathrm{ct}}(G_{\Sigma}, T_{\rho_{d,n}}) \to \bigoplus_{l \in \Sigma \setminus \{p\}} \mathrm{Ext}^1_{\mathcal{R}}(H^1(\mathbb{Q}_l, D_{\rho_{d,n}})^{\vee}, \mathcal{R}) \to$$

$$\to \mathrm{Ext}^2_{\mathcal{R}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}), \mathcal{R}).$$

The observations in Section 3.3.1 and Poitou–Tate duality along with the arguments in Section 3.1 of Greenberg's work on the surjectivity of the global-to-local map defining Selmer groups [17] let us deduce that the cokernel of the map

$$H^1_{\mathrm{ct}}(G_{\Sigma}, T_{\rho_{d,n}}) \to \frac{H^1_{\mathrm{ct}}(\mathbb{Q}_p, T_{\rho_{d,n}})}{((\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}}))^{\vee})^*}$$

is isomorphic, as an $\mathcal{R}$-module to $\ker(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho^{\star}_{d,n}}) \twoheadrightarrow \mathrm{III}^1(\mathbb{Q}, D_{\rho^{\star}_{d,n}})^{\vee})$. Thus, one obtains the following short exact sequence of $\mathcal{R}$-modules:

$$0 \to \ker(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho^{\star}_{d,n}}) \twoheadrightarrow \mathrm{III}^1(\mathbb{Q}, D_{\rho^{\star}_{d,n}})^{\vee}) \to \mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}), \mathcal{R}) \to$$

$$\to \ker\left(H^2_{\mathrm{ct}}(G_{\Sigma}, T_{\rho_{d,n}}) \to \bigoplus_{l \in \Sigma \setminus \{p\}} \mathrm{Ext}^1_{\mathcal{R}}(H^1(\mathbb{Q}_l, D_{\rho_{d,n}})^{\vee}, \mathcal{R}) \right) \to 0.$$

$$(3.27)$$

One can consider the following $\mathcal{R}$-module:

$$\mathrm{III}^2_{\mathrm{ct}}(\mathbb{Q}, T_{\rho_{d,n}})$$
$$:= \ker\left(H^2_{\mathrm{ct}}(G_{\Sigma}, T_{\rho_{d,n}}) \xrightarrow{\phi_{\mathrm{III}^2_{\mathrm{ct}}}} \underbrace{H^2_{\mathrm{ct}}(\mathbb{Q}_p, T_{\rho_{d,n}})}_{=0} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^2_{\mathrm{ct}}(\mathbb{Q}_l, T_{\rho_{d,n}}) \right).$$

Poitou–Tate duality provides us an isomorphism between the $\mathcal{R}$-modules $\mathrm{III}^1(\mathbb{Q}, D_{\rho^{\star}_{d,n}})^{\vee}$ and $\mathrm{III}^2_{\mathrm{ct}}(\mathbb{Q}, T_{\rho_{d,n}})$. Furthermore, Poitou–Tate duality also tells us that the cokernel of the map $\phi_{\mathrm{III}^2_{\mathrm{ct}}}$ is isomorphic to $H^0(G_{\Sigma}, D_{\rho^{\star}_{d,n}})^{\vee}$ and hence zero.

Let us fix a height two prime ideal, say $\mathcal{Q}$, in the ring $\mathcal{R}$. Using equation (3.25), we have the following commutative diagram of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$
\begin{array}{ccc}
H^2_{\mathrm{ct}}(G_\Sigma, T_{\rho_{d,n}})_{\mathcal{Q}} & \xrightarrow{\;\cong\;} & H^2_{\mathrm{ct}}(G_\Sigma, T_{\rho_{d,n}})_{\mathcal{Q}} \\
\downarrow & & \downarrow
\end{array}
$$

$$
0 \longrightarrow \bigoplus_{l \in \Sigma \setminus \{p\}} \mathrm{Ext}^2_{\mathcal{R}}(H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee, \mathcal{R})_{\mathcal{Q}} \longrightarrow \bigoplus_{l \in \Sigma \setminus \{p\}} H^2_{\mathrm{ct}}(\mathbb{Q}_l, T_{\rho_{d,n}})_{\mathcal{Q}} \longrightarrow \bigoplus_{l \in \Sigma \setminus \{p\}} \mathrm{Ext}^1_{\mathcal{R}}(H^1(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee, \mathcal{R})_{\mathcal{Q}} \longrightarrow 0.
$$

Applying the Snake Lemma, we obtain the following short exact sequence of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$
\begin{aligned}
0 &\to (\text{Ш}^1(\mathbb{Q}, D_{\rho^\star_{d,n}})^\vee)_{\mathcal{Q}} \to \\
&\to \ker\big(H^2_{\mathrm{ct}}(G_\Sigma, T_{\rho_{d,n}}) \to \mathrm{Ext}^1_{\mathcal{R}}(H^1(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee, \mathcal{R})\big)_{\mathcal{Q}} \to \\
&\to \bigoplus_{l \in \Sigma \setminus \{p\}} \mathrm{Ext}^2_{\mathcal{R}}(H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee, \mathcal{R})_{\mathcal{Q}} \to 0. \quad (3.28)
\end{aligned}
$$

By Lemma 2.17, for each $l \in \Sigma \setminus \{p\}$, the $\mathcal{R}$-module $\mathrm{Ext}^2_{\mathcal{R}}(H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee, \mathcal{R})$ is pseudonull. As a result, equation (3.28) lets us deduce that the $\mathcal{R}_{\mathcal{Q}}$-module

$$
\ker\big(H^2_{\mathrm{ct}}(G_\Sigma, T_{\rho_{d,n}}) \to \mathrm{Ext}^1_{\mathcal{R}}(H^1(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee, \mathcal{R})\big)_{\mathcal{Q}}
$$

is pseudonull if and only if the $\mathcal{R}_{\mathcal{Q}}$-module $(\text{Ш}^1(\mathbb{Q}, D_{\rho^\star_{d,n}})^\vee)_{\mathcal{Q}}$ is pseudonull. This observation along with equation (3.27) lets us deduce the following implications:

The $\mathcal{R}_{\mathcal{Q}}$-module $(\mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}), \mathcal{R})^\vee)_{\mathcal{Q}}$ is pseudonull

$\Longleftrightarrow$ The $\mathcal{R}_{\mathcal{Q}}$-modules $(\ker(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho^\star_{d,n}}) \twoheadrightarrow \text{Ш}^1(\mathbb{Q}, D_{\rho^\star_{d,n}}, \mathbb{Q})^\vee))_{\mathcal{Q}}$ and

$(\text{Ш}^1(\mathbb{Q}, D_{\rho^\star_{d,n}})^\vee)_{\mathcal{Q}}$ are pseudonull,

$\Longleftrightarrow$ The $\mathcal{R}_{\mathcal{Q}}$-module $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho^\star_{d,n}})_{\mathcal{Q}}$ is pseudonull.

This lets us conclude that the $\mathcal{R}$-module $\mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}), \mathcal{R})$ is pseudonull if and only if the $\mathcal{R}$-module $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho^\star_{d,n}})$ is pseudonull. Now, suppose the $\mathcal{R}$-module $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho^\star_{d,n}})$ is pseudonull. Equations (3.27) and (3.28) let us deduce the following equalities in $Z^2(\mathcal{R})$:

$$
\begin{aligned}
c_2&(\mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}), \mathcal{R})) \\
&= c_2(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho^\star_{d,n}})) - c_2(\text{Ш}^1(\mathbb{Q}, D_{\rho^\star_{d,n}})^\vee) + c_2(\text{Ш}^1(\mathbb{Q}, D_{\rho^\star_{d,n}})^\vee) \\
&\quad + \sum_{l \in \Sigma \setminus \{p\}} c_2(\mathrm{Ext}^2_{\mathcal{R}}(H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee, \mathcal{R})),
\end{aligned}
$$

$$= c_2(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^\star})) + \sum_{l \in \Sigma \setminus \{p\}} c_2(\mathrm{Ext}^2_{\mathcal{R}}(H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee, \mathcal{R})),$$

$$= c_2(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^\star})) + \sum_{l \in \Sigma \setminus \{p\}} c_2((H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee)_{\mathrm{P.N.}}),$$

using Hypothesis Reg(0) and by Lemma 2.17. This completes the proof of the proposition. $\qquad \square$

4. The main theorem in the general setup

4.1. Alternative characterizations of Assumption GCD.
Before proving the main theorem in the general setup, we would like to provide alternative characterizations of Assumption GCD.

PROPOSITION 4.1. *Suppose all the hypotheses and assumptions in Section* 3.1.2 *hold.*

Then, the following statements are equivalent:

(1) *The height of the ideal* (θ_I, θ_{II}) *in* $\mathcal{R}$ *is greater than or equal to two.*

(2) *The* $\mathcal{R}$-modules $\mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}})$ *and* $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})_{\mathrm{tor}}$ *are pseudonull.*

(3) *The* $\mathcal{R}$-modules $\mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}})$ *and* $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^\star})$ *are pseudonull.*

Proof. We will first show Condition (1) $\implies$ Condition (2).

Suppose Condition (1) holds. Let $\mathfrak{p}$ be a height one prime ideal in $\mathcal{R}$. Without loss of generality, assume $\theta_I \notin \mathfrak{p}$. By equation (3.4) in Assumption MC, we can conclude that the prime ideal $\mathfrak{p}$ does not belong to the support of the $\mathcal{R}$-module $\mathrm{Sel}_I(\mathbb{Q}, D_{\rho_{d,n}})^\vee$. As a result, $\mathrm{Sel}_I(\mathbb{Q}, D_{\rho_{d,n}})^\vee \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}}$ would equal zero. By (3.13), we have

$$\mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}} = 0.$$

By equation (3.10) and Hypothesis LF, we have the following isomorphism of free $\mathcal{R}_{\mathfrak{p}}$-modules of rank one:

$$\underbrace{\left(\frac{\mathrm{Loc}_{II}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_I(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{II}(\mathbb{Q}_p, D_{\rho_{d,n}})} \right)^\vee \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}}}_{\text{free } \mathcal{R}_{\mathfrak{p}}\text{-module of rank one}} \cong \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}}.$$

As a result, $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})_{\mathrm{tor}} \otimes_{\mathcal{R}} \mathcal{R}_p$ equals zero.

Second, we will show Condition (2) $\implies$ Condition (1).

Suppose Condition (2) holds. Let $\mathfrak{p}$ be a height one prime ideal in $\mathcal{R}$. It suffices to show that $\theta_{\mathrm{I}} \notin \mathfrak{p}$ or $\theta_{\mathrm{II}} \notin \mathfrak{p}$. We have

$$\mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}} = 0, \quad \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})_{\mathrm{tor}} \otimes_{\mathcal{R}} \mathcal{R}_p = 0.$$

By equation (3.12) and Hypothesis LF, we have the following surjection of free $\mathcal{R}_{\mathfrak{p}}$-modules:

$$\underbrace{\left(\frac{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^{\vee} \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}} \oplus \left(\frac{\mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^{\vee} \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}}}_{\text{free } \mathcal{R}_{\mathfrak{p}}\text{-module of rank one} \qquad \text{free } \mathcal{R}_{\mathfrak{p}}\text{-module of rank one}}$$

$$\twoheadrightarrow \underbrace{\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_p}_{\text{free } \mathcal{R}_{\mathfrak{p}}\text{-module of rank one}}.$$

As a result, at least one of the two maps

$$\left(\frac{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^{\vee} \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}} \to \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}},$$

$$\left(\frac{\mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^{\vee} \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}} \to \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}}.$$

must be an isomorphism of free $\mathcal{R}_{\mathfrak{p}}$-modules of rank one. Without loss of generality, assume that the first map is an isomorphism. By (3.10), we can conclude that $\mathrm{Sel}_{\mathrm{I}}(\mathbb{Q}, D_{\rho_{d,n}})^{\vee} \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}}$ equals zero. That is, $\mathfrak{p}$ does not belong to the support of the $\mathcal{R}$-module $\mathrm{Sel}_{\mathrm{I}}(\mathbb{Q}, D_{\rho_{d,n}})^{\vee}$. By equation (3.4) in Assumption MC, we have $\theta_{\mathrm{I}} \notin \mathfrak{p}$.

We will now show that Condition (2) is equivalent to Condition (3). To do so, we will need to show that the following statements are equivalent:

(i) The $\mathcal{R}$-module $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^{\star}})$ is pseudonull.

(ii) The $\mathcal{R}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})_{\mathrm{tor}}$ is pseudonull.

Let $\mathfrak{p}$ be a height one prime ideal in $\mathcal{R}$. Note that $\mathcal{R}_{\mathfrak{p}}$ is a DVR. Let $\pi_{\mathfrak{p}}$ denote a uniformizer in $\mathcal{R}_{\mathfrak{p}}$. Every finitely generated $\mathcal{R}_{\mathfrak{p}}$-module M is isomorphic to

$\mathcal{R}_{\mathfrak{p}}^r \bigoplus \oplus_i \frac{\mathcal{R}_{\mathfrak{p}}}{(\pi_{\mathfrak{p}}^{r_i})}$, for some nonnegative integers r, and r_i. In particular, M is a torsion-free $\mathcal{R}_{\mathfrak{p}}$-module if and only if M is a free $\mathcal{R}_{\mathfrak{p}}$-module. Also, the $\mathcal{R}_{\mathfrak{p}}$-module $\mathrm{Ext}^1_{\mathcal{R}_{\mathfrak{p}}}(\frac{\mathcal{R}_{\mathfrak{p}}}{(\pi_{\mathfrak{p}}^a)}, \mathcal{R}_{\mathfrak{p}})$ is noncanonically isomorphic to $\frac{\mathcal{R}_{\mathfrak{p}}}{(\pi_{\mathfrak{p}}^a)}$.

The fact that Conditions (i) and (ii) are equivalent follows from the above observations:

$$
\begin{aligned}
&\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^\star}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}} = 0, \\
&\iff \mathrm{Ext}^1_{\mathcal{R}_{\mathfrak{p}}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}}, \mathcal{R}_{\mathfrak{p}}) = 0, \quad \text{(by Proposition 3.11)} \\
&\iff \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})_{\mathrm{tor}} \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}} = 0. \qquad \qquad \square
\end{aligned}
$$

We have the following important corollary to Proposition 4.1.

COROLLARY 4.2. *Suppose all the hypotheses and assumptions in Section* 3.1.2 *hold. Then, the $\mathcal{R}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})_{\mathrm{tor}}$ equals zero.*

Proof. Proposition 4.1 tells us that $\mathcal{R}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})_{\mathrm{tor}}$ is pseudonull. We have already established that $\mathcal{R}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})$ has no nonzero pseudonull submodules (see Section 3.2). As a result, $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})_{\mathrm{tor}}$ equals zero. $\square$

We will need to consider the map

$$
i_{\mathfrak{X}} : \mathfrak{X}(D_{\rho_{d,n}}, \mathbb{Q}) \to \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^{**}.
$$

By Corollary 4.2, note that $\ker(i_{\mathfrak{X}})$ (which is equal to $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})_{\mathrm{tor}}$) equals zero.

4.2. Proof of the main theorem.

THEOREM 4.3. *Suppose that the following conditions hold:*

(1) *All the hypotheses and assumptions in Section* 3.1.2 *hold.*

(2) *For every height two prime ideal $\mathcal{Q}$ of $\mathcal{R}$, the $\mathcal{R}_{\mathcal{Q}}$-module*

$$
\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}
$$

has finite projective dimension.

Then, we have the following equality in $Z^2(\mathcal{R})$:

$$
c_2\left(\frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\theta_{\mathrm{I}}, \theta_{\mathrm{II}})}\right) = c_2(\mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}})) + c_2(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^\star}))
$$
$$
+ \sum_{l \in \Sigma \backslash \{p\}} c_2((H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee)_{\mathrm{P.N.}}).
$$

Proof. To prove the theorem, we proceed in three steps.

Step One: For every height two prime ideal $\mathcal{Q}$ in $\mathcal{R}$, the $\mathcal{R}_{\mathcal{Q}}$-module $\mathrm{coker}(i_{\mathfrak{x}})_{\mathcal{Q}}$ has finite projective dimension.

Step Two: For every height two prime ideal $\mathcal{Q}$ in $\mathcal{R}$, we have the following short exact sequence of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$0 \to \mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to \frac{\mathcal{R}_{\mathcal{Q}}}{(\theta_{\mathrm{I}}, \theta_{\mathrm{II}})} \to \mathrm{coker}(i_{\mathfrak{x}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to 0.$$

Step Three: We have the following equality in $Z^2(\mathcal{R})$:

$$\begin{aligned}
c_2(\mathrm{coker}(i_{\mathfrak{x}})) = {} & c_2(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^{\star}})) \\
& + \sum_{l \in \Sigma \setminus \{p\}} c_2((H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^{\vee})_{\mathrm{P.N.}}).
\end{aligned}$$

Step One follows from Corollary 4.2, Lemma 4.4 and condition (2). Step Two follows from Lemma 4.5. Step Three follows from Lemma 4.6. Theorem 4.3 would following from these lemmas. While proving these lemmas, we assume all the conditions stated in the theorem.

LEMMA 4.4. *The $\mathcal{R}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^{**}$ is free.*

Proof. It will be enough to show that the $\mathcal{R}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^*$ is free. By applying the functor $\mathrm{Hom}_{\mathcal{R}}(-, \mathcal{R})$ to the first short exact sequence in Lemma 3.6, we obtain the following exact sequence of R-modules:

$$\begin{aligned}
0 \to \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^* \to \mathcal{R} \to {} & \mathrm{Ext}^1_{\mathcal{R}}(\mathrm{Sel}_{\mathrm{I}}(\mathbb{Q}, D_{\rho_{d,n}})^{\vee}, \mathcal{R}) \to \\
& \to \mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}), \mathcal{R}).
\end{aligned} \tag{4.1}$$

To obtain equation (4.1), we have identified the free rank-one $\mathcal{R}$-module $\left(\frac{\mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})} \right)^{\vee}$ with $\mathcal{R}$. This allows us to identify $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^*$ with an ideal inside $\mathcal{R}$. This ideal must be reflexive over $\mathcal{R}$. The $\mathcal{R}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})$ is torsion-free. Since $\mathcal{R}$ is integrally closed, for every height one prime ideal $\mathfrak{p}$ in $\mathcal{R}$, the localization $\mathcal{R}_{\mathfrak{p}}$ must be a DVR and consequently the $\mathcal{R}_{\mathfrak{p}}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})_{\mathfrak{p}}$ must be free. Since localization commutes with Ext, the $\mathcal{R}$-module $\mathrm{Ext}^1_{\mathcal{R}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}), \mathcal{R})$ must be pseudonull. Using this trick of localizing at every height one prime ideal of $\mathcal{R}$, we have

$$\mathrm{Div}(\mathrm{Ext}^1_{\mathcal{R}}(\mathrm{Sel}_{\mathrm{I}}(\mathbb{Q}, D_{\rho_{d,n}})^{\vee}, \mathcal{R})) = \mathrm{Div}(\theta_{\mathrm{I}}),$$

an equality of divisors in $Z^1(\mathcal{R})$. Combining these observations, for every height one prime ideal $\mathfrak{p}$ in $\mathcal{R}$, we obtain the following short exact sequence of $\mathcal{R}_{\mathfrak{p}}$-modules:

$$0 \to \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^* \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}} \to \mathcal{R}_{\mathfrak{p}} \to \frac{\mathcal{R}_{\mathfrak{p}}}{(\theta_{\mathrm{I}})} \to 0. \tag{4.2}$$

Since $\mathcal{R}$ is integrally closed, equation (4.2) lets us deduce that under the inclusion $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^* \hookrightarrow \mathcal{R}$ given in equation (4.1), we have a natural inclusion map

$$\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^* \hookrightarrow (\theta_{\mathrm{I}}),$$

whose cokernel is pseudonull. Since the ideal $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^*$ is reflexive, this natural inclusion must be an equality. This shows that the $\mathcal{R}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^*$ is free. □

LEMMA 4.5. *For every height two prime ideal $\mathcal{Q}$ in $\mathcal{R}$, we have the following short exact sequence of $\mathcal{R}_{\mathcal{Q}}$-modules:*

$$0 \to \mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to \frac{\mathcal{R}_{\mathcal{Q}}}{(\theta_{\mathrm{I}}, \theta_{\mathrm{II}})} \to \mathrm{coker}(i_{\mathfrak{X}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to 0.$$

Proof of Lemma 4.5. Let $\mathcal{Q}$ be a height two prime ideal in $\mathcal{R}$. By Lemma 4.4, the $\mathcal{R}_{\mathcal{Q}}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^{**} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$ is free. By Lemma 3.6, we can conclude that the $\mathcal{R}_{\mathcal{Q}}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})$ has rank one.

Hypothesis LF lets us consider the following two maps of free $\mathcal{R}_{\mathcal{Q}}$-modules:

$$\underbrace{\left(\frac{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^{\vee} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}}_{\text{free } \mathcal{R}_{\mathcal{Q}}\text{-module of rank one}} \xrightarrow{A_{\mathrm{I}}} \underbrace{\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^{**} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}}_{\text{free } \mathcal{R}_{\mathcal{Q}}\text{-module of rank one}},$$
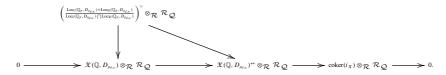
$$\underbrace{\left(\frac{\mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^{\vee} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}}_{\text{free } \mathcal{R}_{\mathcal{Q}}\text{-module of rank one}} \xrightarrow{A_{\mathrm{II}}} \underbrace{\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^{**} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}}_{\text{free } \mathcal{R}_{\mathcal{Q}}\text{-module of rank one}}.$$

Here, A_{I} and A_{II} are elements of $\mathcal{R}_{\mathcal{Q}}$. For every height one prime ideal $\mathfrak{p}$ in $\mathcal{R}$, the natural map

$$\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}} \xrightarrow{\cong} \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^{**} \otimes_{\mathcal{R}} \mathcal{R}_{\mathfrak{p}}$$

is an isomorphism. Equation (3.4) and the short exact sequences in (3.10) and (3.11) provide us the following equalities of divisors in $Z^1(\mathcal{R}_{\mathcal{Q}})$:

$$\mathrm{Div}(A_{\mathrm{I}}) = \mathrm{Div}(\theta_{\mathrm{I}}), \quad \mathrm{Div}(A_{\mathrm{II}}) = \mathrm{Div}(\theta_{\mathrm{II}}).$$

As a result, there exist two units u_{I} and u_{II} in the ring $\mathcal{R}_{\mathcal{Q}}$, such that we have the following equality of elements in the ring $\mathcal{R}_{\mathcal{Q}}$:

$$A_{\mathrm{I}} = u_{\mathrm{I}}\theta_{\mathrm{I}}, \quad A_{\mathrm{II}} = u_{\mathrm{II}}\theta_{\mathrm{II}}.$$

The cokernel of the map

$$\underbrace{\left(\frac{\operatorname{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \operatorname{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\operatorname{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \operatorname{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^{\vee} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}}_{\text{free } \mathcal{R}_{\mathcal{Q}}\text{-module of rank two}}$$

$$\xrightarrow{\ \left[A_{\mathrm{I}},\ A_{\mathrm{II}}\right]\ } \underbrace{\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})^{**} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}}_{\text{free } \mathcal{R}_{\mathcal{Q}}\text{-module of rank one}}$$

is, thus, isomorphic to $\frac{\mathcal{R}_{\mathcal{Q}}}{(\theta_{\mathrm{I}}, \theta_{\mathrm{II}})}$.

By (3.12), the cokernel of the map

$$\left(\frac{\operatorname{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) + \operatorname{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\operatorname{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \operatorname{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}\right)^{\vee} \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to \mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}}$$

is isomorphic to $\mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}})$.

Consider the following commutative diagram:

Now, applying the Snake lemma to the commutative diagram given above, we have the following short exact sequence of $\mathcal{R}_{\mathcal{Q}}$-modules:

$$0 \to \mathcal{Z}(\mathbb{Q}, D_{\rho_{d,n}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to \frac{\mathcal{R}_{\mathcal{Q}}}{(\theta_{\mathrm{I}}, \theta_{\mathrm{II}})} \to \operatorname{coker}(i_{\mathfrak{X}}) \otimes_{\mathcal{R}} \mathcal{R}_{\mathcal{Q}} \to 0. \qquad \square$$

LEMMA 4.6. *We have the following equality in* $Z^2(\mathbb{Z}_p[[\widetilde{\Gamma}]])$:

$$c_2(\operatorname{coker}(i_{\mathfrak{X}})) = c_2(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^{\star}})) + \sum_{l \in \Sigma \backslash \{p\}} c_2((H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^{\vee})_{\mathrm{P.N.}}).$$

Proof of Lemma 4.6. Note that Proposition 3.11 is applicable. By Corollary 4.2, the $\mathcal{R}$-module $\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}})$ is torsion-free. As a result of Step One and the hypotheses of the theorem, Proposition 2.14 is also applicable. The lemma follows from the following equalities in $Z^2(\mathbb{Z}_p[[\widetilde{\Gamma}]])$:

$$c_2(\operatorname{coker}(i_{\mathfrak{X}}))$$
$$= c_2(\operatorname{Ext}^1_{\mathcal{R}}(\mathfrak{X}(\mathbb{Q}, D_{\rho_{d,n}}), \mathcal{R})), \quad \text{(by Proposition 2.14)}$$

$$= c_2(\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{d,n}^\star}))$$
$$+ \sum_{l \in \Sigma \setminus \{p\}} c_2((H^0(\mathbb{Q}_l, D_{\rho_{d,n}})^\vee)_{\text{P.N.}}), \quad \text{(by Proposition 3.11).} \qquad \square$$

Theorem 4.3 follows. $\qquad \square$

5. The Iwasawa main conjecture and the Panchishkin condition

5.1. Greenberg's Selmer groups. We recall some of the notations from the introduction. We let $K(\mathfrak{p}^\infty)_{\mathbb{Z}_p}$ (and $K(\mathfrak{q}^\infty)_{\mathbb{Z}_p}$ respectively) denote the unique $\mathbb{Z}_p$-extension of K that is unramified outside $\mathfrak{p}$ (and $\mathfrak{q}$ respectively). Let $\Gamma_\mathfrak{p}$ and $\Gamma_\mathfrak{q}$ denote the Galois groups $\mathrm{Gal}(K(\mathfrak{p}^\infty)_{\mathbb{Z}_p}/K)$ and $\mathrm{Gal}(K(\mathfrak{q}^\infty)_{\mathbb{Z}_p}/K)$ respectively. We let $\kappa_\mathfrak{p} : G_K \twoheadrightarrow \Gamma_\mathfrak{p} \hookrightarrow \mathrm{GL}_1(\mathbb{Z}_p[[\Gamma_\mathfrak{p}]])$ and $\kappa_\mathfrak{q} : G_K \twoheadrightarrow \Gamma_\mathfrak{q} \hookrightarrow \mathrm{GL}_1(\mathbb{Z}_p[[\Gamma_\mathfrak{q}]])$ denote the associated tautological characters. Consider the two-dimensional Galois representation

$$\rho_\mathfrak{p} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}_p[[\Gamma_\mathfrak{p}]])$$

given by the action of $G_\mathbb{Q}$ on the following free $\mathbb{Z}_p[[\Gamma_\mathfrak{p}]]$-module of rank two:

$$T_\mathfrak{p} := \mathrm{Ind}_{G_K}^{G_\mathbb{Q}}(\mathbb{Z}_p[[\Gamma_\mathfrak{p}]](\kappa_\mathfrak{p}^{-1})).$$

Since the prime p splits in the imaginary quadratic field, we have the following decomposition of $\mathbb{Z}_p[[\Gamma_\mathfrak{p}]]$-modules which is $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-equivariant:

$$T_\mathfrak{p} \cong \mathbb{Z}_p[[\Gamma_\mathfrak{p}]](\kappa_\mathfrak{p}^{-1}) \oplus \mathbb{Z}_p[[\Gamma_\mathfrak{p}]](\kappa_\mathfrak{q}^{-1}). \tag{5.1}$$

Let $K_\mathfrak{p}$ denote the completion of the imaginary quadratic field K with respect to the prime ideal $\mathfrak{p}$. Since the prime p splits in the imaginary quadratic field, the embedding $K \hookrightarrow \overline{\mathbb{Q}}_p$ (fixed in our introduction) then gives us an isomorphism $\mathbb{Q}_p \xrightarrow{\cong} K_\mathfrak{p}$. This embedding then gives us the following isomorphism of Galois groups:

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\mathfrak{p}) \xrightarrow{\cong} \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p). \tag{5.2}$$

Throughout this paper, we will use this isomorphism to identify $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\mathfrak{p})$ with $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Recall from the introduction that E is an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at p with $a_p(E) = 0$. We refer the reader to the introduction for the precise details on the construction of the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module

$T_{\rho_{4,2}}$, which is free of rank four, that in turn gives rise to a $G_{\mathbb{Q}}$-representation $\rho_{4,2} : G_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{Z}_p[[\widetilde{\Gamma}]])$.

We can consider the following $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules that have a continuous action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$:

$$T_{\rho_{4,2}} = T_p(E) \,\widehat{\otimes}_{\mathbb{Z}_p}\, T_{\mathfrak{p}} \,\widehat{\otimes}_{\mathbb{Z}_p}\, \mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]](\kappa_{\mathrm{cyc}}^{-1}),$$

$$\mathrm{Fil}_+ T_{\rho_{4,2}} := T_p(E) \,\widehat{\otimes}_{\mathbb{Z}_p}\, \mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]](\kappa_{\mathfrak{p}}^{-1}) \,\widehat{\otimes}_{\mathbb{Z}_p}\, \mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]](\kappa_{\mathrm{cyc}}^{-1}).$$

One has the following discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$D_{\rho_{4,2}} = T_{\rho_{4,2}} \otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee, \quad \mathrm{Fil}_+ D_{\rho_{4,2}} = \mathrm{Fil}_+ T_{\rho_{4,2}} \otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee.$$

The decomposition given in (5.1) lets us deduce the following short exact sequences of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules that is $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\overline{\mathbb{Q}}_p)$-equivariant:

$$0 \to \mathrm{Fil}_+ T_{\rho_{4,2}} \to T_{\rho_{4,2}} \to \frac{T_{\rho_{4,2}}}{\mathrm{Fil}_+ T_{\rho_{4,2}}} \to 0,$$

$$0 \to \mathrm{Fil}_+ D_{\rho_{4,2}} \to D_{\rho_{4,2}} \to \frac{D_{\rho_{4,2}}}{\mathrm{Fil}_+ D_{\rho_{4,2}}} \to 0.$$

The local condition at p, denoted by $\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}})$, is given below.

$$\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}}) := \ker\left(H^1(\mathbb{Q}_p, D_{\rho_{4,2}}) \to H^1\left(I_p, \frac{D_{\rho_{4,2}}}{\mathrm{Fil}_+ D_{\rho_{4,2}}} \right) \right).$$

Here, I_p denotes the inertia subgroup inside the decomposition group $G_{\mathbb{Q}_p}$. The discrete Selmer group, following Greenberg's construction in [14], is defined below:

$$\mathrm{Sel}^{\mathrm{Gr}}(\mathbb{Q}, D_{\rho_{4,2}})$$
$$:= \ker\left(H^1(G_\Sigma, D_{\rho_{4,2}}) \to \frac{H^1(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}})} \oplus \bigoplus_{v \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_v, D_{\rho_{4,2}}) \right).$$

5.2. Hida's Rankin–Selberg p-adic L-function and the Iwasawa main conjecture.

The two-variable p-adic L-function $\theta_{4,2}^{\mathrm{Gr}}$ in this setup has been constructed by Hida. One must modify the p-adic L-function constructed in [21] by multiplying it with a one-variable p-adic L-function associated to the 3-dimensional adjoint representation $\mathrm{Ad}^0(\rho_F)$ (see [22, Conjecture 1.0.1]). A discussion surrounding the need to introduce this modification, which is related to the choice of a certain period (Néron period versus a period involving the Peterson

inner product), is carefully explained in [**22**]. See the introduction and Section 6 in Hida's article [**22**]. We avoid stating the precise interpolation property satisfied by $\theta_{4,2}^{\mathrm{Gr}}$. Instead, we refer the reader to Hida's works in [**21, 22**]. We will content ourselves with describing the critical set of specializations (following Greenberg's terminology in [**14**]). As mentioned in the introduction, the natural restriction maps $\widetilde{\Gamma} \twoheadrightarrow \Gamma_{\mathrm{cyc}}$ and $\widetilde{\Gamma} \twoheadrightarrow \Gamma_{\mathfrak{p}}$ provide us the following isomorphism of topological groups:

$$\widetilde{\Gamma} \cong \Gamma_{\mathrm{cyc}} \times \Gamma_{\mathfrak{p}}.$$

Note that $\mathbb{Z}_p[[\widetilde{\Gamma}]]$ is a coproduct in the category of complete semilocal Noetherian $\mathbb{Z}_p$-algebras (with respect to the maps $\mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]] \hookrightarrow \mathbb{Z}_p[[\widetilde{\Gamma}]]$ and $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]] \hookrightarrow \mathbb{Z}_p[[\widetilde{\Gamma}]]$). Note also that we have the following equalities of the group of continuous homomorphisms:

$$\mathrm{Hom}_{\mathrm{ring}}(\mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]], \overline{\mathbb{Q}}_p) = \mathrm{Hom}_{\mathrm{gp}}(\Gamma_{\mathfrak{p}}, \overline{\mathbb{Q}}_p^{\times}),$$
$$\mathrm{Hom}_{\mathrm{ring}}(\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]], \overline{\mathbb{Q}}_p) = \mathrm{Hom}_{\mathrm{gp}}(\Gamma_{\mathrm{cyc}}, \overline{\mathbb{Q}}_p^{\times}).$$

Taking this point of view, one can consider the set $C \subset \mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_p[[\widetilde{\Gamma}]], \overline{\mathbb{Q}}_p)$ obtained via the following continuous group homomorphisms:

$$\varphi_k : \Gamma_{\mathfrak{p}} \to \overline{\mathbb{Q}}_p^{\times}, \quad \varphi_{\mathrm{cyc}}\epsilon_p : \Gamma_{\mathrm{cyc}} \to \overline{\mathbb{Q}}_p^{\times},$$

- where we allow the group homomorphism $\phi_k : \Gamma_{\mathfrak{p}} \to \overline{\mathbb{Q}}_p^{\times}$ to vary over p-adic Galois characters, obtained via algebraic Hecke characters of K, with conductor equal to a power of $\mathfrak{p}$ and of infinity type $(1 - k)i \circ i_{\mathfrak{p}}$ subject to the following restriction on its weight k:

$$k \geqslant 3,$$

- and where we allow φ_{cyc} to vary over all the continuous group homomorphisms $\Gamma_{\mathrm{cyc}} \to \overline{\mathbb{Q}}_p^{\times}$ of finite order. (The character $\epsilon_p : \Gamma_{\mathrm{cyc}} \xrightarrow{\cong} 1 + p\mathbb{Z}_p$ is given by the product $\chi_p\omega^{-1}$, where $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^{\times}$ is the p-adic cyclotomic character and $\omega : G_{\mathbb{Q}} \to \mathbb{Z}_p^{\times}$ is the Teichmuller character giving the action of $G_{\mathbb{Q}}$ on the pth roots of unity.)

This set C is the critical set of specializations, corresponding to the fact that the Galois representation $\rho_{4,2}$ satisfies the Panchishkin condition.

We recall Conjecture 1.2 stated in the introduction.

CONJECTURE 1.2 [**14**, Conjecture 4.1]. *The $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\mathrm{Sel}^{\mathrm{Gr}}(\mathbb{Q}, D_{\rho_{4,2}})^{\vee}$ is torsion. Furthermore, we have the following equality in $Z^1(\mathbb{Z}_p[[\widetilde{\Gamma}]])$:*

$$\mathrm{Div}(\mathrm{Sel}^{\mathrm{Gr}}(\mathbb{Q}, D_{\rho_{4,2}})^{\vee}) \overset{?}{=} \mathrm{Div}(\theta_{4,2}^{\mathrm{Gr}}).$$

Progress towards establishing Conjecture 1.2 has been made by Xin Wan. See his works [**61**, **62**].

6. ±± Iwasawa main conjectures for elliptic curves with supersingular reduction at p

When the elliptic curve E has good supersingular reduction at p, the classical p-Selmer group of E defined over the field $\widetilde{K}_\infty$, is not well suited for the study of Iwasawa theory since its Pontryagin dual is not $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-torsion and will not satisfy a 'control theorem'. We shall recall the formulation of Kim's conjectures and the corresponding local conditions for the signed Selmer groups at p. Consider the following discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules that have a continuous action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$:

$$D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}} := (T_p(E)\widehat{\otimes}\mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]](\kappa_{\mathfrak{p}}^{-1})\widehat{\otimes}\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]](\kappa_{\mathrm{cyc}}^{-1})) \otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee,$$

$$D_{E,\kappa_{\mathfrak{q}}^{-1}\kappa_{\mathrm{cyc}}^{-1}} := (T_p(E)\widehat{\otimes}\mathbb{Z}_p[[\Gamma_{\mathfrak{p}}]](\kappa_{\mathfrak{q}}^{-1})\widehat{\otimes}\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]](\kappa_{\mathrm{cyc}}^{-1})) \otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee.$$

The decomposition in equation (5.1) gives us the following isomorphism of discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules that is $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-equivariant:

$$D_{\rho_{4,2}} \cong D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}} \oplus D_{E,\kappa_{\mathfrak{q}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}.$$

We obtain the following isomorphisms of discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$\begin{aligned}
H^1(\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p), D_{\rho_{4,2}}) &\cong H^1(\mathbb{Q}_p, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) \oplus H^1(\mathbb{Q}_p, D_{E,\kappa_{\mathfrak{q}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) \\
&\cong H^1(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) \oplus H^1(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{q}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}). \quad (6.1)
\end{aligned}$$

If we let δ denote the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$ and $\widetilde{\delta}$ some lift in G_Σ of δ, we have the following natural isomorphism inside $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$\widetilde{\delta}^{-1}\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_{\mathfrak{q}})\widetilde{\delta} \cong \mathrm{Gal}(\overline{\mathbb{Q}}_p/K_{\mathfrak{p}}).$$

This lets us obtain the following isomorphism of discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$H^1(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{q}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) \cong H^1(K_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}). \quad (6.2)$$

Shapiro's lemma (see the discussion in the introduction of Greenberg's work [**16**]) provides us the following isomorphism of discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$H^1(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) \cong \bigoplus_{\mathfrak{P}|\mathfrak{p}} H^1((\widetilde{K}_\infty)_{\mathfrak{P}}, E[p^\infty]), \quad (6.3)$$

$$H^1(K_{\mathfrak{q}}, D_{E, \kappa_{\mathfrak{p}}^{-1}\kappa_{\text{cyc}}^{-1}}) \cong \bigoplus_{\mathfrak{Q}|\mathfrak{q}} H^1((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty]). \tag{6.4}$$

Here, if we let $G_{\mathfrak{P}}$ denote the decomposition group for the prime $\mathfrak{P}$ inside $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, then $(\widetilde{K}_\infty)_{\mathfrak{P}}$ denotes the fixed field $\overline{\mathbb{Q}}_p^{G_{\mathfrak{P}}}$. Note that the isomorphism in equation (6.3) crucially relies on identifying $\widetilde{\Gamma}$ with $\Gamma_{\text{cyc}} \times \Gamma_{\mathfrak{p}}$. Note also that there are only finitely many primes $\mathfrak{P}$ (and $\mathfrak{Q}$ respectively) in the field $\widetilde{K}_\infty$ lying above the prime $\mathfrak{p}$ (and $\mathfrak{q}$ respectively) of the imaginary quadratic field K.

Combining equations (6.1), (6.2) and (6.3), we have the following isomorphism of discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$H^1(\mathbb{Q}_p, D_{\rho_{4,2}}) \cong \bigoplus_{\mathfrak{P}|\mathfrak{p}} H^1((\widetilde{K}_\infty)_{\mathfrak{P}}, E[p^\infty]) \oplus \bigoplus_{\mathfrak{Q}|\mathfrak{q}} H^1((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty]). \tag{6.5}$$

Keeping this isomorphism in mind, to define the local conditions inside the local cohomology group $H^1(\mathbb{Q}_p, D_{\rho_{4,2}})$, it will be sufficient to define local conditions inside $H^1((\widetilde{K}_\infty)_{\mathfrak{P}}, E[p^\infty])$ and $H^1((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty])$ for all the primes $\mathfrak{P}$ and $\mathfrak{Q}$ in $\widetilde{K}_\infty$ lying above the primes $\mathfrak{p}$ and $\mathfrak{q}$ in K respectively.

6.1. The ±± Selmer groups of Kim.

Let $\widehat{E}$ denote the formal group attached to the minimal Weierstrass model of the elliptic curve E over $\mathbb{Z}_p$. The height of the formal group $\widehat{E}$ equals two.

Given an ideal $\mathfrak{n}$ of the ring of integers of K, we write $K(\mathfrak{n})$ for the ray class field of K with modulus $\mathfrak{n}$. Let $\mathfrak{P}$ be a fixed prime of $K(p^\infty)$ lying above $\mathfrak{p}$. By an abuse of notation, we denote the prime $L \cap \mathfrak{P}$ again by $\mathfrak{P}$ whenever L is a subextension of $K(p^\infty)/K$. For nonnegative integers m and n, Kim [26] defined

$$E^+(K(\mathfrak{p}^m\mathfrak{q}^n)_{\mathfrak{P}})$$
$$= \{P \in \widehat{E}(K(\mathfrak{p}^m\mathfrak{q}^n)_{\mathfrak{P}}) : \text{Tr}_{m/l+1,n} P \in \widehat{E}(K(\mathfrak{p}^l\mathfrak{q}^n)_{\mathfrak{P}}), \text{ for odd } l < m\};$$
$$E^-(K(\mathfrak{p}^m\mathfrak{q}^n)_{\mathfrak{P}})$$
$$= \{P \in \widehat{E}(K(\mathfrak{p}^m\mathfrak{q}^n)_{\mathfrak{P}}) : \text{Tr}_{m/l+1,n} P \in \widehat{E}(K(\mathfrak{p}^l\mathfrak{q}^n)_{\mathfrak{P}}), \text{ for even } l < m\},$$

where $\text{Tr}_{m/l+1,n} : \widehat{E}(K(\mathfrak{p}^m\mathfrak{q}^n)_{\mathfrak{P}}) \to \widehat{E}(K(\mathfrak{p}^{l+1}\mathfrak{q}^n)_{\mathfrak{P}})$ denotes the trace map. We define $E^\pm(K(p^\infty)_{\mathfrak{P}})$ to be the union $\bigcup_{m,n \geqslant 0} E^\pm(K(\mathfrak{p}^m\mathfrak{q}^n)_{\mathfrak{P}})$. Let Δ be the finite Galois group $\text{Gal}(K(p^\infty)_{\mathfrak{P}}/(\widetilde{K}_\infty)_{\mathfrak{P}})$. Then, we may define the corresponding plus/minus subgroups by

$$E^\pm((\widetilde{K}_\infty)_{\mathfrak{P}}) := E^\pm(K(p^\infty)_{\mathfrak{P}})^\Delta \subset E((\widetilde{K}_\infty)_{\mathfrak{P}}).$$

Given a prime $\mathfrak{Q}$ of $K(p^\infty)$ lying above $\mathfrak{q}$, we may define $E^\pm((\widetilde{K}_\infty)_{\mathfrak{Q}})$ in a similar manner.

For each prime $\mathfrak{P}$ (and $\mathfrak{Q}$ respectively) in $\widetilde{K}_\infty$, lying above $\mathfrak{p}$ (and $\mathfrak{q}$ respectively), we consider:

$$
\begin{aligned}
&\mathrm{Loc}_\pm((\widetilde{K}_\infty)_{\mathfrak{P}}, E[p^\infty]) \\
&\quad := \mathrm{Image}(E^\pm((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \overset{\varkappa_{\mathfrak{P}}}{\hookrightarrow} H^1((\widetilde{K}_\infty)_{\mathfrak{P}}, E[p^\infty])), \\
&\mathrm{Loc}_\pm((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty]) \\
&\quad := \mathrm{Image}(E^\pm((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \overset{\varkappa_{\mathfrak{Q}}}{\hookrightarrow} H^1((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty])).
\end{aligned}
$$

Here, $\varkappa_{\mathfrak{P}}$ and $\varkappa_{\mathfrak{Q}}$ denote the usual Kummer map. Note that the restriction of the Kummer map to the groups $E^\pm((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and $E^\pm((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ are injections since the natural maps $E^\pm((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to E((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and $E^\pm((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to E((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ are injections. This fact follows from an argument similar to the one given in Lemma 8.17 of Kobayashi's work [27].

Let $\bullet, \circ \in \{+, -\}$. Via equation (6.5), we define the following local condition:

$$
\begin{aligned}
\mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}}) &:= \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Loc}_\bullet((\widetilde{K}_\infty)_{\mathfrak{P}}, E[p^\infty]) \oplus \bigoplus_{\mathfrak{Q}|\mathfrak{q}} \mathrm{Loc}_\circ((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty]) \\
&\subset H^1(\mathbb{Q}_p, D_{\rho_{4,2}}).
\end{aligned}
$$

This, in turn, lets us define the following discrete Selmer group:

$$
\begin{aligned}
&\mathrm{Sel}^{\bullet\circ}(\mathbb{Q}, D_{\rho_{4,2}}) \\
&= \ker\left(H^1(G_\Sigma, D_{\rho_{4,2}}) \to \frac{H^1(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})} \oplus \bigoplus_{v \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_v, D_{\rho_{4,2}}) \right).
\end{aligned}
$$

REMARK 6.1. Our choice of signs $+$ and $-$ is opposite to that of Kim since we would like to formulate the Iwasawa main conjecture using the convention for the signs $+$ and $-$ chosen by Loeffler in [32]. In particular, the Selmer groups $\mathrm{Sel}^{++}(\mathbb{Q}, D_{\rho_{4,2}})$, $\mathrm{Sel}^{+-}(\mathbb{Q}, D_{\rho_{4,2}})$, $\mathrm{Sel}^{-+}(\mathbb{Q}, D_{\rho_{4,2}})$ and $\mathrm{Sel}^{--}(\mathbb{Q}, D_{\rho_{4,2}})$ respectively correspond to the $--$, $-+$, $+-$ and $++$ Selmer groups respectively appearing in Kim's work [26].

6.2. Two-variable main conjectures and two-variable p-adic L-functions. Following Loeffler's work [32], we recall the construction of the four $\pm, \pm$ 2-variable p-adic L-functions attached to E. Suppose we are given a choice of $\lambda, \mu \in \{\pm\sqrt{-p}\}$. There exists an unbounded $\mathbb{Q}_p(\sqrt{-p})$-valued distribution $L_{\lambda,\mu}$ on $\widetilde{\Gamma}$, satisfying the following interpolation formula:

$$
L_{\lambda,\mu}(\psi) = \frac{p^{m+n}}{\lambda^m \mu^n \tau_K(\psi^{-1})} \times \frac{L(E/K, \psi^{-1}, 1)}{\Omega_{f_E}^+ \Omega_{f_E}^-}, \tag{6.6}
$$

for every finite Galois character $\psi : \mathrm{Gal}(\overline{K}/K) \to \overline{\mathbb{Q}}^{\times}$ with conductor $\mathfrak{p}^m \mathfrak{q}^n$ for some $m, n > 0$. Here $\tau_K(\psi^{-1})$ is the Gauss sum of ψ^{-1} (see, for example, the work of Skinner and Urban [**54**, Section 8.1.3]). The periods $\Omega_{f_E}^{\pm}$ are the real and imaginary periods associated to the newform f_E constructed by Shimura [**51**]. See also Theorem 3.5.4 in the work of Greenberg and Stevens [**19**]. These periods are well defined up to units in $\overline{\mathbb{Z}}_p^{\times}$.

REMARK 6.2. There are three choices of normalizations (depending on the choice of complex periods) available to us for the construction of these unbounded measures. These choices, denoted by $\Omega_{f_E}^{\mathrm{cong}}$, Ω_{Π} and $\Omega_{f_E}^{+} \Omega_{f_E}^{-}$ respectively, appear in works of Castella and Wan [**8**], Loeffler [**32**] and Wan [**62**] respectively. We refer the reader to these works for the precise definition of $\Omega_{f_E}^{\mathrm{cong}}$ and Ω_{Π}.

Lemma 9.5 in the work of Skinner and Zhang [**55**] asserts that the p-adic valuation of the ratio $\Omega_{f_E}^{\mathrm{cong}}/(\Omega_{f_E}^{+} \Omega_{f_E}^{-})$ is zero. Castella and Wan [**8**, Remark 2.4] assert that the ratio of the periods $\Omega_{\Pi}/(\Omega_{f_E}^{+} \Omega_{f_E}^{-})$ is an element of $\mathbb{Q}^{\times}$. However, it is not clear to us whether the ratio $\Omega_{\Pi}/(\Omega_{f_E}^{+} \Omega_{f_E}^{-})$ is a p-adic unit.

We have chosen to work with the complex period given in Wan's work [**62**] because, as we indicate in Remark 8.5, this choice makes it transparent how the cyclotomic specializations of the 2-variable $++$ and $--$ p-adic L-functions are related to certain one-variable p-adic L-functions of Rob Pollack. See Remark 8.5 for more details.

Fix a topological generator $\gamma_{\mathfrak{p}}$ of $\Gamma_{\mathfrak{p}}$. We choose $\gamma_{\mathfrak{q}}$ to be the image of $\gamma_{\mathfrak{p}}$ under the ring automorphism $\mathbb{Z}_p[[\widetilde{\Gamma}]] \to \mathbb{Z}_p[[\widetilde{\Gamma}]]$ induced by complex conjugation. We identify $L_{\lambda,\mu}$ with its Amice transform in $\mathbb{Q}_p(\sqrt{-p})[[\gamma_{\mathfrak{p}} - 1, \gamma_{\mathfrak{q}} - 1]]$. As power series, we may decompose these p-adic L-functions to obtain four bounded $\mathbb{Q}_p$-valued measures $\theta_{4,2}^{\bullet \circ}$ on $\widetilde{\Gamma}$, for $\bullet, \circ \in \{+, -\}$:

$$L_{\lambda,\mu} = \log_{\mathfrak{p}}^{+} \log_{\mathfrak{q}}^{+} \theta_{4,2}^{++} + \lambda \log_{\mathfrak{p}}^{+} \log_{\mathfrak{q}}^{-} \theta_{4,2}^{+-} + \mu \log_{\mathfrak{p}}^{-} \log_{\mathfrak{q}}^{+} \theta_{4,2}^{-+} + \lambda\mu \log_{\mathfrak{p}}^{-} \log_{\mathfrak{q}}^{-} \theta_{4,2}^{--},$$

$$(6.7)$$

where $\log_{\mathfrak{p}}^{\pm}$ and $\log_{\mathfrak{q}}^{\pm}$ are defined using Pollack's $\pm$ logarithms in [**44**]. As power series, we have

$$\log_{\mathfrak{r}}^{+} = \frac{1}{p} \prod_{i \geqslant 1} \frac{\Phi_{p^{2i}}(\gamma_{\mathfrak{r}})}{p}; \quad \log_{\mathfrak{r}}^{-} = \frac{1}{p} \prod_{i \geqslant 1} \frac{\Phi_{p^{2i-1}}(\gamma_{\mathfrak{r}})}{p},$$

where Φ_{p^m} denotes the p^mth cyclotomic polynomial. The corresponding distributions under Amice transform are described in [**12**].

If ψ is a finite Hecke character on $\widetilde{\Gamma}$ of conductor $\mathfrak{f}$ for $\mathfrak{r} \in \{\mathfrak{p}, \mathfrak{q}\}$, then $\log_{\mathfrak{r}}^{+}(\psi)$ (respectively, $\log_{\mathfrak{r}}^{-}(\psi)$) vanishes if and only if $\mathrm{ord}_{\mathfrak{r}}(\mathfrak{f}) > 0$ is odd

(respectively, even). On combining equations (6.6) and (6.7), we may deduce the following interpolation formulae for $\theta_{4,2}^{\bullet\circ}$. Let $\bullet, \circ \in \{+, -\}$. Let ψ be a finite Hecke character on $\widetilde{\Gamma}$ of conductor $\mathfrak{p}^m\mathfrak{q}^n$ such that $\log_{\mathfrak{p}}^{\bullet}(\psi) \log_{\mathfrak{q}}^{\circ}(\psi) \neq 0$. Then,

$$\theta_{4,2}^{++}(\psi) = \frac{(-1)^{(m+n)/2} p^{m+n}}{\tau_K(\psi^{-1}) \displaystyle\prod_{\substack{1 \leqslant k < m-1 \\ k \text{ even}}} \Phi_{p^k}(\zeta_{\mathfrak{p}}) \prod_{\substack{1 \leqslant l < n-1 \\ l \text{ even}}} \Phi_{p^l}(\zeta_{\mathfrak{q}})} \times \frac{L(E/K, \psi^{-1}, 1)}{\Omega_{f_E}^+ \Omega_{f_E}^-}, \quad (6.8)$$

$$\theta_{4,2}^{+-}(\psi) = \frac{(-1)^{(m+n+1)/2} p^{m+n}}{\tau_K(\psi^{-1}) \displaystyle\prod_{\substack{1 \leqslant k < m-1 \\ k \text{ even}}} \Phi_{p^k}(\zeta_{\mathfrak{p}}) \prod_{\substack{1 \leqslant l < n-1 \\ l \text{ odd}}} \Phi_{p^l}(\zeta_{\mathfrak{q}})} \times \frac{L(E/K, \psi^{-1}, 1)}{\Omega_{f_E}^+ \Omega_{f_E}^-}, \quad (6.9)$$

$$\theta_{4,2}^{-+}(\psi) = \frac{(-1)^{(m+n+1)/2} p^{m+n}}{\tau_K(\psi^{-1}) \displaystyle\prod_{\substack{1 \leqslant k < m-1 \\ k \text{ odd}}} \Phi_{p^k}(\zeta_{\mathfrak{p}}) \prod_{\substack{1 \leqslant l < n-1 \\ l \text{ even}}} \Phi_{p^l}(\zeta_{\mathfrak{q}})} \times \frac{L(E/K, \psi^{-1}, 1)}{\Omega_{f_E}^+ \Omega_{f_E}^-}, \quad (6.10)$$

$$\theta_{4,2}^{--}(\psi) = \frac{(-1)^{(m+n)/2+1} p^{m+n}}{\tau_K(\psi^{-1}) \displaystyle\prod_{\substack{1 \leqslant k < m-1 \\ k \text{ odd}}} \Phi_{p^k}(\zeta_{\mathfrak{p}}) \prod_{\substack{1 \leqslant l < n-1 \\ l \text{ odd}}} \Phi_{p^l}(\zeta_{\mathfrak{q}})} \times \frac{L(E/K, \psi^{-1}, 1)}{\Omega_{f_E}^+ \Omega_{f_E}^-}, \quad (6.11)$$

where $\zeta_{\mathfrak{r}} = \psi(\gamma_{\mathfrak{r}})$ for $\mathfrak{r} = \mathfrak{p}, \mathfrak{q}$. We now recall Conjecture 1.3 stated in the introduction.

CONJECTURE 1.3 [**62**, Conjecture 6.7]. *Let $\bullet, \circ \in \{+, -\}$. The $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module* $\mathrm{Sel}^{\bullet\circ}(\mathbb{Q}, D_{\rho_{4,2}})^{\vee}$ *is torsion. We have the following equality in* $Z^1(\mathbb{Z}_p[[\widetilde{\Gamma}]])$:

$$\mathrm{Div}(\mathrm{Sel}^{\bullet\circ}(\mathbb{Q}, D_{\rho_{4,2}})^{\vee}) \stackrel{?}{=} \mathrm{Div}(\theta_{4,2}^{\bullet\circ}).$$

REMARK 6.3. For $\mathfrak{r} \in \{\mathfrak{p}, \mathfrak{q}\}$, if a different topological generator of $\Gamma_{\mathfrak{r}}$ is chosen, then $\log_{\mathfrak{r}}^{\pm}$ would change by a factor $u_{\mathfrak{r}}^{\pm}$, for some unit $u_{\mathfrak{r}}^{\pm}$ in the ring $\mathbb{Z}_p[[\Gamma_{\mathfrak{r}}]]$. The p-adic L-functions $\theta_{4,2}^{\bullet\circ}$ would then change by the factor $(u_{\mathfrak{p}}^{\bullet} u_{\mathfrak{q}}^{\circ})^{-1}$. As a result, the divisors of the p-adic L-functions are independent of the choice of topological generators for $\Gamma_{\mathfrak{p}}$ and $\Gamma_{\mathfrak{q}}$.

Progress towards Conjecture 1.3 has been made by various authors under various technical hypotheses. We will cite the relevant works, referring the interested reader instead to these works for the statement of the hypotheses. Wan [**62**, Theorem 8.5] has made progress towards establishing the inequality $\mathrm{Div}(\theta_{4,2}^{++}) \leqslant \mathrm{Div}(\mathrm{Sel}^{++}(\mathbb{Q}, D_{\rho_{4,2}})^{\vee})$ in $Z^1(\mathbb{Z}_p[[\widetilde{\Gamma}]])$. For the reverse inequality, one can employ an argument involving Euler systems of Beilinson–Flach

elements constructed by Loeffler–Zerbes in [**34**]. Under some technical hypotheses, such an Euler system is constructed and used to prove this direction of the main conjecture in [**6**, Theorem 1.3]. Recently, a proof of Conjecture 1.3 has been announced in the work of Castella *et al.* [**7**, Theorem A].

7.   Proof of Theorem 1

Theorem 1 follows from Theorem 4.3. We will need to verify all the conditions stated in Theorem 4.3. Since we are working over the regular local ring $\mathbb{Z}_p[[\widetilde{\Gamma}]]$, condition (2) is automatically satisfied.

One has to verify all the hypotheses in Section 3.1.2. Hypothesis Loc(0) follows from [**40**, Proposition 4.1]. Since we are working over the regular local ring $\mathbb{Z}_p[[\widetilde{\Gamma}]]$, Hypothesis Reg(0) and Hypothesis Gor automatically hold.

It remains to verify Hypothesis Rank, Hypothesis LF and Hypothesis $\text{Loc}_p(0)$. Hypothesis $\text{Loc}_p(0)$ follows from Proposition 7.1. Hypothesis Rank follows from Corollaries 7.4, 7.6 and 7.8. Hypothesis LF follows from Corollaries 7.4, 7.6 and Proposition 7.9. Note that

$$d(\rho_{4,2}) = 4, \quad d^+(\rho_{4,2}) = 2, \quad d^-(\rho_{4,2}) = 2.$$

For the remainder of this section, it will be helpful to keep the following picture in mind:

Figure 1.

The identification of $H^1(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\text{cyc}}^{-1}})$ with $\text{Loc}_{\text{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}})$ is established in Corollary 7.6. All the remaining inclusions and isomorphisms given in Figure 1 follow from the discussions in Section 6.

7.1. Verifying the various hypotheses. Let $\mathfrak{m}$ be the maximal ideal of local ring $\mathbb{Z}_p[[\widetilde{\Gamma}]]$. Let $\mathbb{F}_p(\omega)$ denote the one-dimensional $\mathbb{F}_p$ vector on which G_Σ acts via the Teichmüller character. The residual representation

$$\overline{\rho}_E : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(\mathbb{F}_p)$$

associated to the elliptic curve E for the local decomposition group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is absolutely irreducible (see [13, Theorem 2.6]). This uses the fact that E is an elliptic curve defined over $\mathbb{Q}$ with good supersingular reduction at the prime p. As a result, we obtain the following proposition:

PROPOSITION 7.1.

(1) *The* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$*-modules* $D_{\rho_{4,2}}[\mathfrak{m}]$ *and* $D_{\rho_{4,2}^*}[\mathfrak{m}]$ *have no quotient isomorphic to the trivial representation.*

(2) *The* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_{\mathfrak{p}})$*-module* $D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}[\mathfrak{m}]$ *has no quotient isomorphic to the trivial representation or* $\mathbb{F}_p(\omega)$.

(3) *The* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_{\mathfrak{q}})$*-module* $D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}[\mathfrak{m}]$ *has no quotient isomorphic to the trivial representation or* $\mathbb{F}_p(\omega)$.

As an immediate corollary to Proposition 7.1, we have the following equalities:

$$H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p), D_{\rho_{4,2}})^\vee = H^2(\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p), D_{\rho_{4,2}})^\vee = 0.$$
$$H^0(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) = H^2(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) = 0.$$
$$H^0(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{q}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) = H^2(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{q}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) = 0.$$

The local Euler Poincaré characteristics [16, Proposition 4.2] along with [16, Proposition 5.10 and Remark 5.10.1] lets us immediately deduce the following corollary:

COROLLARY 7.2. *The* $\mathbb{Z}_p[[\widetilde{\Gamma}]]$*-module* $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p), D_{\rho_{4,2}})^\vee$ *is free of rank four. The* $\mathbb{Z}_p[[\widetilde{\Gamma}]]$*-modules* $H^1(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}})^\vee$ *and* $H^1(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{q}}^{-1}\kappa_{\mathrm{cyc}}^{-1}})^\vee$ *are free of rank two.*

Let us recall the following result of Kim.

PROPOSITION 7.3. *Let* $\bullet, \circ \in \{+, -\}$. *The following* $\mathbb{Z}_p[[\widetilde{\Gamma}]]$*-modules are free of rank one:*

$$\bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Loc}_\bullet((\widetilde{K}_\infty)_\mathfrak{P}, E[p^\infty])^\vee, \quad \bigoplus_{\mathfrak{Q}|\mathfrak{q}} \mathrm{Loc}_\circ((\widetilde{K}_\infty)_\mathfrak{Q}, E[p^\infty])^\vee.$$

Proof. We only show that the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Loc}_\bullet((\widetilde{K}_\infty)_\mathfrak{P}, E[p^\infty])^\vee$ is free of rank one. One can show similarly that the same holds true for $\bigoplus_{\mathfrak{Q}|\mathfrak{q}} \mathrm{Loc}_\circ((\widetilde{K}_\infty)_\mathfrak{Q}, E[p^\infty])^\vee$. Let us fix a prime $\mathfrak{P}_0$ above $\mathfrak{p}$ in $\widetilde{K}_\infty$. Let $\widetilde{\Gamma}_{\mathfrak{P}_0}$ denote the decomposition group of $\widetilde{\Gamma}$ for the prime $\mathfrak{P}_0$ lying above the prime $\mathfrak{p}$ in K. Note that we have the following isomorphism of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$\bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Loc}_\bullet((\widetilde{K}_\infty)_\mathfrak{P}, E[p^\infty])^\vee \cong \mathrm{Ind}_{\widetilde{\Gamma}_{\mathfrak{P}_0}}^{\widetilde{\Gamma}} (E^\bullet((\widetilde{K}_\infty)_{\mathfrak{P}_0}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee.$$

It suffices to show that the $\mathbb{Z}_p[[\widetilde{\Gamma}_{\mathfrak{P}_0}]]$-module $(E^\bullet((\widetilde{K}_\infty)_{\mathfrak{P}_0}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ is free of rank one. This follows from a result of Kim [**26**, Proposition 2.11]. □

Let $\bullet, \circ \in \{+, -\}$. Since we have the following equality of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$\mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}}) = \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Loc}_\bullet((\widetilde{K}_\infty)_\mathfrak{P}, E[p^\infty]) \oplus \bigoplus_{\mathfrak{Q}|\mathfrak{q}} \mathrm{Loc}_\circ((\widetilde{K}_\infty)_\mathfrak{Q}, E[p^\infty]),$$

we immediately have the following corollary:

COROLLARY 7.4. *Let* $\bullet, \circ \in \{+, -\}$. *The* $\mathbb{Z}_p[[\widetilde{\Gamma}]]$*-module* $\mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})^\vee$ *is free of rank two.*

LEMMA 7.5. *Let* $\mathfrak{Q}$ *(and* $\mathfrak{P}$ *respectively) be a prime of* $\widetilde{K}_\infty$ *lying above the prime* $\mathfrak{q}$ *(and* $\mathfrak{p}$ *respectively) of* K. *Then, we have*

$$H^0(I_\mathfrak{Q}, E[p^\infty]) = H^0(I_\mathfrak{P}, E[p^\infty]) = H^0(G_\mathfrak{Q}, E[p^\infty])$$
$$= H^0(G_\mathfrak{P}, E[p^\infty]) = 0.$$

Here, the groups $I_\mathfrak{Q}$, $G_\mathfrak{Q}$ (and $I_\mathfrak{P}$, $G_\mathfrak{P}$ respectively) denote the inertia and decomposition subgroups for the primes $\mathfrak{Q}$ (and $\mathfrak{P}$ respectively) inside $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\mathfrak{q})$ (and $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\mathfrak{p})$ respectively).

Proof. Note that if we show $H^0(I_\mathfrak{Q}, E[p^\infty]) = H^0(I_\mathfrak{P}, E[p^\infty]) = 0$, then we would have $H^0(G_\mathfrak{Q}, E[p^\infty]) = H^0(G_\mathfrak{P}, E[p^\infty]) = 0$. We will simply show that $H^0(I_\mathfrak{Q}, E[p^\infty]) = 0$. One can similarly prove that $H^0(I_\mathfrak{P}, E[p^\infty]) = 0$.

Since the quotient $I_\mathfrak{q}/I_\mathfrak{Q}$ is a pro-p group and since $E[p]$ is a discrete torsion p-group, we have

$$H^0(I_\mathfrak{Q}, E[p^\infty]) = 0 \iff H^0(I_\mathfrak{Q}, E[p]) = 0 \iff H^0(I_\mathfrak{q}, E[p]) = 0.$$

Therefore, to complete the proof, it suffices to show that $H^0(I_\mathfrak{q}, E[p]) = 0$. By [**13**, Theorem 2.6], we have the following isomorphism of $F_p[I_q]$-modules:

$$E[p] \cong \mathbb{F}_p(\psi) \oplus \mathbb{F}_p(\psi'),$$

where $\psi : I_q \to \mathbb{F}_{p^2}^\times$ and $\psi' : I_q \to \mathbb{F}_{p^2}^\times$ are two fundamental characters of level two. That is, Image(ψ) and Image(ψ') lie inside $\mathbb{F}_{p^2}$ but not inside $\mathbb{F}_p$. As a result,

$$H^0(I_q, E[p]) \cong H^0(I_q, \mathbb{F}_p(\psi)) \oplus H^0(I_q, \mathbb{F}_p(\psi)) = 0.$$

This completes the proof of the lemma.

Alternatively, to deduce the lemma, we can adopt the techniques of the proof appearing in Kobayashi's work [27, Proposition 8.7], which relies on the fact the $E[p]$ is isomorphic to the p-torsion points on a formal group of height two over the local ring $\mathbb{Z}_p$. See also Kim's work [26, discussion towards the end of page 829]. □

COROLLARY 7.6. *Under the isomorphism given in equation* (6.1)*, we can identify* $\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}})$ *with* $H^1(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}})$. *Consequently, the* $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-*module* $\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}})^\vee$ *is free of rank two.*

Proof. Under the isomorphism

$$D_{\rho_{4,2}} \cong D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}} \oplus D_{E,\kappa_{\mathfrak{q}}^{-1}\kappa_{\mathrm{cyc}}^{-1}},$$

we can identify $\mathrm{Fil}_+ D_{\rho_{4,2}}$ with $D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}$. As a result, under the isomorphism given in equation (6.1), we can identify $\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}})$ with

$$\begin{aligned}
&\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}}) \\
&\cong H^1(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) \oplus \ker(H^1(K_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) \to H^1(I_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}})).
\end{aligned}$$

Here, $I_{\mathfrak{q}}$ denotes the inertia group inside $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_{\mathfrak{q}})$. The inflation-restriction exact sequence gives us the following isomorphism of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$\begin{aligned}
&H^1(G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}}, H^0(I_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}})) \\
&\cong \ker(H^1(K_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) \to H^1(I_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}})).
\end{aligned}$$

Note that we have the following isomorphism of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$H^0(I_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) \cong \bigoplus_{\mathfrak{Q}|\mathfrak{q}} H^0(I_{\mathfrak{Q}}, E[p^\infty]).$$

Here, the direct sum is taken over all primes $\mathfrak{Q}$ of $\widetilde{K}_\infty$ lying above the prime $\mathfrak{q}$ of K. The groups $I_{\mathfrak{Q}}$ and $G_{\mathfrak{Q}}$ denote the inertia and decomposition subgroups of $\mathfrak{Q}$ inside $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_{\mathfrak{q}})$. By Lemma 7.5, we have

$$H^0(I_{\mathfrak{Q}}, E[p^\infty]) = 0, \quad \forall \mathfrak{Q} \mid \mathfrak{q}.$$

These observations now give us following isomorphism of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}}) \cong H^1(K_{\mathfrak{p}}, D_{E, \kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}).$$

The last part of the corollary follows from Corollary 7.2.   □

PROPOSITION 7.7. *Let* $\bullet, \circ \in \{+, -\}$. *The Pontryagin duals of the* $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-*modules*

$$\frac{\mathrm{Loc}_{+\circ}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{-\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})}, \quad \frac{\mathrm{Loc}_{\bullet+}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{\bullet-}(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})}$$

$$(7.1)$$

are free of rank one.

Proof. We will show the result for $\frac{\mathrm{Loc}_{\bullet+}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{\bullet-}(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})}$. The proof for $\frac{\mathrm{Loc}_{+\circ}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{-\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})}$ is similar.

Let $\mathfrak{Q}$ be any prime of $\widetilde{K}_\infty$ lying above p and write $\varkappa_{\mathfrak{Q}}$ for the Kummer map as before. Note that the p-power torsion points on the elliptic curve coincides with the p-power torsion points on the formal group $\widehat{E}$.

By Proposition 4.3 in the work of Coates and Greenberg [9] (see also Section 2 of Rubin's work [47]), we have

$$\varkappa_{\mathfrak{Q}}(E((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = H^1((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty]).$$

A result of Kim [26, Proposition 2.6] says that

$$E^+((\widetilde{K}_\infty)_{\mathfrak{Q}}) + E^-((\widetilde{K}_\infty)_{\mathfrak{Q}}) = \widehat{E}((\widetilde{K}_\infty)_{\mathfrak{Q}}). \tag{7.2}$$

Recall from §6.1 that we have injections

$$E^{\pm}((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \widehat{E}((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

This fact along with equation (7.2) now implies the following:

$$\bigoplus_{\mathfrak{Q}|\mathfrak{q}} (E^+((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) + \bigoplus_{\mathfrak{Q}|\mathfrak{q}} (E^-((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

$$= \bigoplus_{\mathfrak{Q}|\mathfrak{q}} (\widehat{E}((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

$$\cong \bigoplus_{\mathfrak{Q}|\mathfrak{q}} H^1((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty]),$$

$$\cong H^1(K_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}). \tag{7.3}$$

Therefore, the quotient appearing in (7.1) is isomorphic to $\dfrac{H^1(K_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}})}{\bigoplus_{\mathfrak{Q}|\mathfrak{q}} E^\circ((\widetilde{K}_\infty)_{\mathfrak{Q}})\otimes \mathbb{Q}_p/\mathbb{Z}_p}$.

Consider the short exact sequence

$$0 \to \left(\frac{H^1(K_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}})}{\displaystyle\bigoplus_{\mathfrak{Q}|\mathfrak{q}} E^\circ((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\vee \to H^1(K_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}})^\vee$$

$$\to \bigoplus_{\mathfrak{Q}|\mathfrak{q}} (E^\circ((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \to 0.$$

By Proposition 7.3, the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\bigoplus_{\mathfrak{Q}|\mathfrak{q}} (E^\circ((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ is free of rank one. By Corollary 7.2, the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $H^1(K_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}})^\vee$ is free of rank two. The proposition now follows. $\qquad\square$

COROLLARY 7.8. *Let* {I, II} *be any one of the following unordered pairs*

$$\{++, +-\}, \quad \{++, -+\}, \quad \{--, +-\}, \quad \{--, -+\},$$
$$\{++, \mathrm{Gr}\}, \quad \{+-, \mathrm{Gr}\}, \quad \{-+, \mathrm{Gr}\}, \quad \{--, \mathrm{Gr}\}.$$

Then, the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $(\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{4,2}}))^\vee$ is free of rank three.

Proof. We will prove the corollary when {I, II} equals $\{++, +-\}$ and when {I, II} equals $\{+-, \mathrm{Gr}\}$. The remaining cases of the corollary would follow similarly.

If {I, II} equals $\{++, +-\}$, then

$$\mathrm{Loc}_{++}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}})$$
$$= \bigoplus_{\mathfrak{P}|\mathfrak{p}} (E^+((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \oplus H^1(K_{\mathfrak{q}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}). \tag{7.4}$$

If {I, II} equals $\{+-, \mathrm{Gr}\}$, then

$$\mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}})$$
$$= H^1(K_{\mathfrak{p}}, D_{E,\kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) \oplus \bigoplus_{\mathfrak{Q}|\mathfrak{q}} (E^-((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p). \tag{7.5}$$

By Corollary 7.2 and Proposition 7.3, the Pontryagin duals of the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules appearing in equations (7.4) and (7.5) are free of rank three. $\qquad\square$

PROPOSITION 7.9. *Let* {I, II} *be one of the pairs appearing in the statement of Corollary* 7.8. *Then, the Pontryagin duals of*

$$\frac{\mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}, \qquad \frac{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}})}{\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{d,n}}) \bigcap \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{d,n}})}$$

are free $\mathbb{Z}_p[[\widetilde{\Gamma}]]$*-modules of rank one.*

Proof. We only consider the cases when {I, II} equals {Gr, $+-$} and {$++$, $+-$}. The remaining cases follow similarly.

The identifications in Figure 1 let us conclude that

$$\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}}) \cap \mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}}) = \bigoplus_{\mathfrak{P}|\mathfrak{p}} (E^+((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p).$$

Consequently,

$$\frac{\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}}) \cap \mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}})} \cong \bigoplus_{\mathfrak{P}|\mathfrak{p}} \frac{H^1((\widetilde{K}_\infty)_{\mathfrak{P}}, E[p^\infty])}{(E^+((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)}.$$

The Pontryagin dual of this $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module is free of rank one.

By Proposition 7.3, the Pontryagin dual of the quotient

$$\frac{\mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}}) \cap \mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}})} \cong \bigoplus_{\mathfrak{Q}|\mathfrak{q}} \mathrm{Loc}_{-}((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty])$$

is free of rank one over $\mathbb{Z}_p[[\widetilde{\Gamma}]]$.

The case when {I, II} equals {$++$, $+-$} follows from Proposition 7.7 and the isomorphisms

$$\frac{\mathrm{Loc}_{++}(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{++}(\mathbb{Q}_p, D_{\rho_{4,2}}) \cap \mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}})}$$
$$\cong \frac{\mathrm{Loc}_{++}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}})},$$

$$\frac{\mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{++}(\mathbb{Q}_p, D_{\rho_{4,2}}) \cap \mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}})}$$
$$\cong \frac{\mathrm{Loc}_{++}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{++}(\mathbb{Q}_p, D_{\rho_{4,2}})}. \qquad \square$$

7.2. **Description of the modules $\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})$ and $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^{\star}})$.** We will only describe the modules $\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})$ and $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^{\star}})$ when {I, II} equals {Gr, $+-$} and {$++$, $+-$}. The remaining cases follow similarly. Throughout the description, we will keep in mind the identifications provided by the inclusions and isomorphisms in Figure 1.

Recall that the module $\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})$ was defined to be the Pontryagin dual of

$$\ker\left(H^1(G_\Sigma, D_{\rho_{4,2}}) \to \frac{H^1(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_I(\mathbb{Q}_p, D_{\rho_{4,2}}) \bigcap \mathrm{Loc}_{II}(\mathbb{Q}_p, D_{\rho_{4,2}})} \times \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{4,2}})\right).$$

To describe $\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})$, it suffices to identify $\mathrm{Loc}_I(\mathbb{Q}_p, D_{\rho_{4,2}}) \bigcap \mathrm{Loc}_{II}(\mathbb{Q}_p, D_{\rho_{4,2}})$ in Figure 1.

When {I, II} equals {Gr, $+-$},

$$\mathrm{Loc}_I(\mathbb{Q}_p, D_{\rho_{4,2}}) \bigcap \mathrm{Loc}_{II}(\mathbb{Q}_p, D_{\rho_{4,2}}) = \bigoplus_{\mathfrak{P}|\mathfrak{p}}(E^+((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \bigoplus 0.$$

PROPOSITION 7.10. *When {I, II} equals {$++$, $+-$},*

$$\mathrm{Loc}_I(\mathbb{Q}_p, D_{\rho_{4,2}}) \bigcap \mathrm{Loc}_{II}(\mathbb{Q}_p, D_{\rho_{4,2}})$$
$$= \bigoplus_{\mathfrak{P}|\mathfrak{p}}(E^+((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \bigoplus_{\mathfrak{Q}|\mathfrak{q}}(\widehat{E}(K(\mathfrak{p}^\infty)_{\mathbb{Z}_p, \mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p).$$

Here, $K(\mathfrak{p}^\infty)_{\mathbb{Z}_p, \mathfrak{Q}}$ is the unique unramified $\mathbb{Z}_p$-extension of $K_{\mathfrak{q}}$. Note that we have the following inclusions:

$$K_{\mathfrak{q}} \subset K(\mathfrak{p}^\infty)_{\mathbb{Z}_p, \mathfrak{Q}} \subset (\widetilde{K}_\infty)_{\mathfrak{Q}}.$$

Proof. Fix a prime $\mathfrak{Q}$ in $\widetilde{K}_\infty$ above $\mathfrak{q}$. First note that there is a short exact sequence

$$0 \to \widehat{E}(K(\mathfrak{p}^\infty)_{\mathbb{Z}_p, \mathfrak{Q}}) \to E^+((\widetilde{K}_\infty)_{\mathfrak{Q}}) \oplus E^-((\widetilde{K}_\infty)_{\mathfrak{Q}}) \to \widehat{E}((\widetilde{K}_\infty)_{\mathfrak{Q}}) \to 0. \tag{7.6}$$

The first map is given by the diagonal map (obtained from the natural inclusions) and the second map is defined by $(a, b) \mapsto a - b$. The exactness at the middle term is given by an argument similar to the one in the proof of [27, Proposition 8.12(ii)]. The exactness at the last term is given in equation (7.2). Now, consider the following commutative diagram.

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \widehat{E}(K(\mathfrak{p}^\infty)_{\mathbb{Z}_p, \mathfrak{Q}}) & \longrightarrow & E^+((\widetilde{K}_\infty)_{\mathfrak{Q}}) \oplus E^-((\widetilde{K}_\infty)_{\mathfrak{Q}}) & \longrightarrow & \widehat{E}((\widetilde{K}_\infty)_{\mathfrak{Q}}) & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \widehat{E}(K(\mathfrak{p}^\infty)_{\mathbb{Z}_p, \mathfrak{Q}}) \otimes \mathbb{Q}_p & \longrightarrow & (E^+((\widetilde{K}_\infty)_{\mathfrak{Q}}) \oplus E^-((\widetilde{K}_\infty)_{\mathfrak{Q}})) \otimes \mathbb{Q}_p & \longrightarrow & \widehat{E}((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p & \longrightarrow & 0
\end{array}
$$

Using equation (7.6), one can conclude that both the rows are exact. All vertical maps turn out to be injective. This is because the kernel of each of the vertical maps is a subgroup of $\widehat{E}((\widetilde{K}_\infty)_{\mathfrak{Q}})[p^\infty]$, which equals zero by Proposition 7.1. The snake lemma then gives the following short exact sequence:

$$0 \to \widehat{E}(K(\mathfrak{p}^\infty)_{\mathbb{Z}_p, \mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to (E^+((\widetilde{K}_\infty)_{\mathfrak{Q}}) \oplus E^-((\widetilde{K}_\infty)_{\mathfrak{Q}})) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$
$$\to \widehat{E}((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0.$$

This lets us deduce the following equality in $\widehat{E}((K_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$:

$$(E^+((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \cap (E^-((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = \widehat{E}(K(\mathfrak{p}^\infty)_{\mathbb{Z}_p, \mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

The proposition follows. □

To describe $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^\star})$, we will need to consider the following isomorphism of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules induced by the Weil pairing:

$$T_{\rho_{4,2}^\star} \cong \operatorname{Ind}_{G_K}^{G_\mathbb{Q}} T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[\widetilde{\Gamma}]](\kappa). \tag{7.7}$$

Let $\iota : \mathbb{Z}_p[[\widetilde{\Gamma}]] \to \mathbb{Z}_p[[\widetilde{\Gamma}]]$ denote the involution defined by sending every element γ of $\widetilde{\Gamma}$ to γ^{-1}. If M is a $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module, then we let M^ι denote the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module which is equal to M as a set (and as a $\mathbb{Z}_p$-module) and on which $\gamma \in \widetilde{\Gamma}$ acts as $\iota(\gamma)$. The isomorphism in equation (7.7), in turn, lets us deduce that the discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $H^1(\mathbb{Q}_p, D_{\rho_{4,2}^\star})$ is isomorphic to $H^1(\mathbb{Q}_p, D_{\rho_{4,2}})^\iota$. For the rest of this section, using this isomorphism induced by the Weil pairing, we will identify $H^1(\mathbb{Q}_p, D_{\rho_{4,2}^\star})$ with $H^1(\mathbb{Q}_p, D_{\rho_{4,2}})^\iota$. We have the following pairing given by local duality:

$$H^1_{\mathrm{ct}}(\mathbb{Q}_p, T_{\rho_{4,2}}) \times \underbrace{H^1(\mathbb{Q}_p, D_{\rho_{4,2}^\star})}_{\cong H^1(\mathbb{Q}_p, D_{\rho_{4,2}})^\iota} \to \mathbb{Q}_p/\mathbb{Z}_p. \tag{7.8}$$

The $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^\star})$ is defined in equation (3.23) as the Pontryagin dual of

$$\ker\left(H^1(G_\Sigma, D_{\rho_{4,2}^\star}) \to \frac{H^1(\mathbb{Q}_p, D_{\rho_{4,2}^\star})}{\mathrm{Loc}_{\mathrm{I,II}}(\mathbb{Q}_p, D_{\rho_{4,2}^\star})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{4,2}^\star})\right),$$

where $\mathrm{Loc}_{\mathrm{I,II}}(\mathbb{Q}_p, D_{\rho_{4,2}^\star}) \subset H^1(\mathbb{Q}_p, D_{\rho_{4,2}^\star})$, is the orthogonal complement of

$$((\mathrm{Loc}_{\mathrm{I}}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{\mathrm{II}}(\mathbb{Q}_p, D_{\rho_{4,2}}))^\vee)^*$$

under the pairing given in equation (7.8). We will also keep in mind all the identifications in Figure 1.

If {I, II} equals {+−, Gr}, then

$$
\begin{aligned}
&\mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{\mathrm{Gr}}(\mathbb{Q}_p, D_{\rho_{4,2}}) \\
&= H^1(K_{\mathfrak{p}}, D_{E, \kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}) \oplus \bigoplus_{\mathfrak{Q}|\mathfrak{q}} (E^-((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p), \\
&\implies \mathrm{Loc}_{\mathrm{I,II}}(\mathbb{Q}_p, D_{\rho_{4,2}^\star}) \\
&= \bigoplus_{\mathfrak{P}|\mathfrak{p}} 0 \oplus \left(\bigoplus_{\mathfrak{Q}|\mathfrak{q}} E^-((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^\iota.
\end{aligned}
\tag{7.9}
$$

If {I, II} equals {++, +−}, then

$$
\begin{aligned}
&\mathrm{Loc}_{++}(\mathbb{Q}_p, D_{\rho_{4,2}}) + \mathrm{Loc}_{+-}(\mathbb{Q}_p, D_{\rho_{4,2}}) \\
&= \bigoplus_{\mathfrak{P}|\mathfrak{p}} (E^+((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \oplus H^1(K_{\mathfrak{q}}, D_{E, \kappa_{\mathfrak{p}}^{-1}\kappa_{\mathrm{cyc}}^{-1}}), \\
&\implies \mathrm{Loc}_{\mathrm{I,II}}(\mathbb{Q}_p, D_{\rho_{4,2}^\star}) = \left(\bigoplus_{\mathfrak{P}|\mathfrak{p}} E^+((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^\iota \oplus \bigoplus_{\mathfrak{Q}|\mathfrak{q}} 0.
\end{aligned}
\tag{7.10}
$$

Equations (7.9) and (7.10) follow from Proposition 7.11. Note that we have the following perfect pairings:

$$
H^1_{\mathrm{ct}}(K_{\mathfrak{p}}, T_{E,\widetilde{\kappa}^{-1}}) \times H^1(K_{\mathfrak{p}}, D_{E,\widetilde{\kappa}^{-1}})^\iota \to \mathbb{Q}_p/\mathbb{Z}_p
\tag{7.11}
$$

$$
H^1_{\mathrm{ct}}(K_{\mathfrak{p}}, T_{E,\widetilde{\kappa}^{-1}})^\iota \times H^1(K_{\mathfrak{p}}, D_{E,\widetilde{\kappa}^{-1}}) \to \mathbb{Q}_p/\mathbb{Z}_p.
\tag{7.12}
$$

PROPOSITION 7.11. *Let* $\bullet, \circ \in \{+, -\}$.

- *Under the pairing given in* (7.11)*,* $(\bigoplus_{\mathfrak{P}|\mathfrak{p}} E^\bullet((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\iota$ *equals the orthogonal complement of* $(\bigoplus_{\mathfrak{P}|\mathfrak{p}} (E^\bullet((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee)^*$.

- *Under the pairing for the field* $K_{\mathfrak{q}}$ *similar to the one given in equation* (7.11)*,* $(\bigoplus_{\mathfrak{Q}|\mathfrak{q}} E^\circ((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\iota$ *equals the orthogonal complement of* $(\bigoplus_{\mathfrak{Q}|\mathfrak{q}} (E^\circ((\widetilde{K}_\infty)_{\mathfrak{Q}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee)^*$.

Here, $T_{E,\widetilde{\kappa}^{-1}} = (T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[\widetilde{\Gamma}]](\widetilde{\kappa}^{-1}))$ and $D_{E,\widetilde{\kappa}^{-1}} = T_{E,\widetilde{\kappa}^{-1}} \otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee$.

Proof. We will show that $(\bigoplus_{\mathfrak{P}|\mathfrak{p}} E^+((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\iota$, under the pairing given in (7.11), equals the orthogonal complement of $(\bigoplus_{\mathfrak{P}|\mathfrak{p}} (E^+((\widetilde{K}_\infty)_{\mathfrak{P}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee)^*$.

The rest of the proposition would follow similarly. Let

$$H_+ \subset H^1_{\mathrm{ct}}(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}}), \quad H^\iota_+ \subset H^1_{\mathrm{ct}}(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}})^\iota,$$

respectively denote the orthogonal complements of

$$\left(\bigoplus_{\mathfrak{P}|\mathfrak{p}} E^+((\widetilde{K}_\infty)_\mathfrak{P}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^\iota, \quad \bigoplus_{\mathfrak{P}|\mathfrak{p}} E^+((\widetilde{K}_\infty)_\mathfrak{P}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

under the pairings given in equation (7.11) and equation (7.12) respectively. We will keep the following isomorphisms in mind:

$$\widetilde{\Gamma} \cong \varprojlim_\alpha \widetilde{\Gamma}_\alpha, \quad \Lambda \cong \varprojlim_{m,\alpha} \frac{\mathbb{Z}_p}{p^m \mathbb{Z}_p}[\widetilde{\Gamma}_\alpha].$$

Here, m varies over all the positive integers and $\widetilde{\Gamma}_\alpha$ varies over all finite quotients of $\widetilde{\Gamma}$. By abuse of notation, we let $\iota : \frac{\mathbb{Z}_p}{p^m \mathbb{Z}_p}[\widetilde{\Gamma}_\alpha] \to \frac{\mathbb{Z}_p}{p^m \mathbb{Z}_p}[\widetilde{\Gamma}_\alpha]$ also denote the $\mathbb{Z}_p$-linear involution obtained by sending every element $\gamma \in \widetilde{\Gamma}_\alpha$ to γ^{-1}.

To identify $(\bigoplus_{\mathfrak{P}|\mathfrak{p}} (E^+((\widetilde{K}_\infty)_\mathfrak{P}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee)^*$ inside $H^1_{\mathrm{ct}}(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}})$, it will be helpful to expand on the isomorphism

$$\mathrm{Hom}_\Lambda(H^1_{\mathrm{ct}}(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}})^\iota, \Lambda) \cong H^1_{\mathrm{ct}}(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}}),$$

which we obtain by combining equations (3.22) and (7.12), using the commutative diagram below.

Figure 2.

For a more explicit description of this identification, see works of Perrin-Riou [43, Section 3.6.1] along with Loeffler and Zerbes [33, Definition 2.3].

The isomorphism in the second row of Figure 2, in turn, relies on the isomorphism

$$H^1_{\mathrm{ct}}(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}}) \otimes_\Lambda \frac{\mathbb{Z}_p}{p^m \mathbb{Z}_p}[[\widetilde{\Gamma}_\alpha]] \cong H^1\left(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}} \otimes_\Lambda \frac{\mathbb{Z}_p}{p^m \mathbb{Z}_p}[[\widetilde{\Gamma}_\alpha]] \right),$$

where Hypothesis $\text{Loc}_p(0)$ comes into play. The isomorphism in the last row of Figure 2 is given by local duality as indicated in the commutative diagram below.

$$
\begin{array}{ccc}
H^1\left(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}} \otimes_\Lambda \frac{\mathbb{Z}_p}{p^m\mathbb{Z}_p}[[\widetilde{\Gamma}_\alpha]]\right)^\iota \times & H^1\left(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}} \otimes_\Lambda \frac{\mathbb{Z}_p}{p^m\mathbb{Z}_p}[[\widetilde{\Gamma}_\alpha]]\right) \longrightarrow & \frac{\mathbb{Z}_p}{p^m\mathbb{Z}_p} \\
\text{\scriptsize Weil pairing} \Big\downarrow \cong & & \Big\downarrow \cong \\
H^1\left(K_\mathfrak{p}, \text{Hom}_{\mathbb{Z}_p}\left(T_{E,\widetilde{\kappa}^{-1}} \otimes_\Lambda \frac{\mathbb{Z}_p}{p^m\mathbb{Z}_p}[[\widetilde{\Gamma}_\alpha]], \mu_{p^m}\right)\right) \times H^1\left(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}} \otimes_\Lambda \frac{\mathbb{Z}_p}{p^m\mathbb{Z}_p}[[\widetilde{\Gamma}_\alpha]]\right) \overset{\cup}{\longrightarrow} H^2\left(K_\mathfrak{p}, \mu_{p^m}\right)
\end{array}
$$

Figure 3.

To prove the proposition, we need to show that under the identification given in Figure 2, we have

$$
H_+ \overset{?}{=} \left(\bigoplus_{\mathfrak{P}|\mathfrak{p}}(E^+((\widetilde{K}_\infty)_\mathfrak{P}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right)^*. \tag{7.13}
$$

Observe that we have a short exact sequence of Λ-modules:

$$
0 \to H_+^\iota \to H_{ct}^1(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}})^\iota \to \bigoplus_{\mathfrak{P}|\mathfrak{p}}(E^+((\widetilde{K}_\infty)_\mathfrak{P}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \to 0.
$$

This allows us to describe $(\bigoplus_{\mathfrak{P}|\mathfrak{p}}(E^+((\widetilde{K}_\infty)_\mathfrak{P}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee)^*$ as the following:

$$
\{\phi \in \text{Hom}_\Lambda(H_{ct}^1(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}})^\iota, \Lambda) \text{ such that } \phi(x) = 0 \text{ for all } x \text{ in } H_+^\iota\}. \tag{7.14}
$$

For every element $y \in H_{ct}^1(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}})$, let ϕ_y denote the element in $\text{Hom}_\Lambda(H_{ct}^1(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}})^\iota, \Lambda)$ corresponding to isomorphism in Figure 2. Disregarding the involution ι, the pairing in the first row of Figure 3 is skew-symmetric since, as indicated by the pairing in the second row of Figure 3, it is induced by the cup-product on the first Galois cohomology groups. Note however that if x, y are two elements in $H_{ct}^1(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}})$, then in general $\phi_y(x^\iota)$ need not equal $-\phi_x(y^\iota)$. That is, the pairing $H_{ct}^1(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}})^\iota \times H_{ct}^1(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}}) \to \Lambda$, described using the identification in Figure 2, need not be skew-symmetric (disregarding the involution ι). This lets us conclude that if $y \in H_+$, then $\phi_y(x^\iota)$ equals zero for all x^ι in H_+^ι. As a result, using the description in equation (7.14), we have the following inclusion of Λ-modules inside $H_{ct}^1(K_\mathfrak{p}, T_{E,\widetilde{\kappa}^{-1}})$:

$$
H_+ \hookrightarrow \left(\bigoplus_{\mathfrak{P}|\mathfrak{p}}(E^+((\widetilde{K}_\infty)_\mathfrak{P}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right)^*. \tag{7.15}
$$

The Λ-modules H_+ and $(\bigoplus_{\mathfrak{P}|\mathfrak{p}}(E^+((\widetilde{K}_\infty)_{\mathfrak{P}})\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee)^*$ are free of rank one and are direct summands of the Λ-module $H^1_{\mathrm{ct}}(K_{\mathfrak{p}}, T_{E,\widetilde{\kappa}^{-1}})$. As a result, the inclusion in equation (7.15) must be an equality. This lets us assert the validity of equation (7.13). The Proposition follows. ☐

REMARK 7.12. The following table summarizes our discussion for the local Selmer conditions at p for $\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})$ and $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^\star})$ associated to the pairs $\{+-, \mathrm{Gr}\}$ and $\{++, +-\}$.

Table 1. Summary of local Selmer conditions at p.

	$\{+-, \mathrm{Gr}\}$		$\{++, +-\}$	
	Cond. at $\mathfrak{p}$	Cond. at $\mathfrak{q}$	Cond. at $\mathfrak{p}$	Cond. at $\mathfrak{q}$
$\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})$	Plus	Empty	Plus	See Proposition 7.10
$\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^\star})$	Empty	Minus	Plus	Empty

The discussion of the local Selmer conditions at p for the remaining pairs is very similar. For the pairs $\{++, \mathrm{Gr}\}$, $\{+-, \mathrm{Gr}\}$, $\{-+, \mathrm{Gr}\}$, $\{--, \mathrm{Gr}\}$, the description of the module $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^\star})$ associated to the Tate dual $\rho_{4,2}^\star$ is analogous to the description of $\mathcal{Z}(\mathbb{Q}, D_{\rho_{4,2}})$ associated to $\rho_{4,2}$ and matches the description given in equation (3.1). For the remaining pairs however, the description of the module $\mathcal{Z}^{(\star)}(\mathbb{Q}, D_{\rho_{4,2}^\star})$ for $\rho_{4,2}^\star$ does not match the description as given in equation (3.1).

7.3. Local fudge factors at primes $l \neq p$ when $p \geqslant 5$.

Throughout Section 7.3, we will assume that $p \geqslant 5$ and that $l \neq p$ is a prime number. Consider the Galois representation $\rho_{E,\widetilde{\kappa}^{-1}} : G_K \to \mathrm{GL}_2(\mathbb{Z}_p[[\widetilde{\Gamma}]])$ given by the action of G_K on the free rank two $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $T_{E,\widetilde{\kappa}^{-1}} := (T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[\widetilde{\Gamma}]](\widetilde{\kappa}^{-1}))$. The discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module associated to $\rho_{E,\widetilde{\kappa}^{-1}}$ is $D_{E,\widetilde{\kappa}^{-1}} := T_{E,\widetilde{\kappa}^{-1}} \otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee$. We have the following isomorphism of Galois representations over $\mathbb{Z}_p[[\widetilde{\Gamma}]]$:

$$\rho_{4,2} \cong \mathrm{Ind}_K^{\mathbb{Q}}(\rho_{E,\widetilde{\kappa}^{-1}}).$$

Let $l \neq p$ be a prime number. If the prime number l splits into two primes η_1 and η_2 in K, then we have the following isomorphism of discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$H^0(\mathbb{Q}_l, D_{\rho_{4,2}}) \cong H^0(K_{\eta_1}, D_{E,\widetilde{\kappa}^{-1}}) \oplus H^0(K_{\eta_2}, D_{E,\widetilde{\kappa}^{-1}}).$$

If there exists a unique prime η in K lying above l, then we have the following isomorphism of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$H^0(\mathbb{Q}_l, D_{\rho_{4,2}}) \cong H^0(K_\eta, D_{E,\widetilde{\kappa}^{-1}}).$$

Here, K_η denotes the completion of the imaginary quadratic field K at the prime η. Combining these observations, we have the following equality in $Z^2(\mathbb{Z}_p[[\widetilde{\Gamma}]])$:

$$\sum_{l \in \Sigma \setminus \{p\}} c_2((H^0(\mathbb{Q}_l, D_{\rho_{4,2}})^\vee)_{\text{P.N.}}) = \sum_{l \in \Sigma \setminus \{p\}} \sum_{\substack{\eta | l \\ \eta \text{ in } K}} c_2((H^0(K_\eta, D_{E,\widetilde{\kappa}^{-1}})^\vee)_{\text{P.N.}}). \quad (7.16)$$

The calculation of the invariant $c_2((H^0(K_\eta, D_{E,\widetilde{\kappa}^{-1}})^\vee)_{\text{P.N.}})$ depends on the reduction type of the elliptic curve E at the prime η in K. See Propositions 7.13, 7.14, 7.15 and 7.16.

Let K_η^{ur} denote the maximal unramified extension of K_η. Let $I_{\eta,ur}$ denote the corresponding inertia group $\text{Gal}(\overline{\mathbb{Q}}_l/K_\eta^{ur})$. The Galois group $\text{Gal}(K_\eta^{ur}/K_\eta)$, which is isomorphic to $\widehat{\mathbb{Z}}$, is topologically generated by the Frobenius element Frob_η. We make the following observations:

(7i)   The restriction of the character $\widetilde{\kappa}$ to the inertia group $I_{\eta,ur}$ is trivial.

(7ii)   Since the prime η does not split completely in the cyclotomic $\mathbb{Z}_p$-extension K_{cyc}/K, the image of the character $\widetilde{\kappa}$ lies inside $\mathbb{Z}_p[[\widetilde{\Gamma}]]$ but not inside $\mathbb{Z}_p$.

(7iii)   The residual representation, associated to the character

$$\widetilde{\kappa} : G_K \twoheadrightarrow \widetilde{\Gamma} \hookrightarrow \text{GL}_1(\mathbb{Z}_p[[\widetilde{\Gamma}]]),$$

is trivial.

(7iv)   Let $\chi_p : \text{Gal}(\overline{\mathbb{Q}}_l/K_\eta) \to \mathbb{Z}_p^\times$ denote the p-adic cyclotomic character given by the action of $\text{Gal}(\overline{\mathbb{Q}}_l/K_\eta)$ on μ_{p^∞}. The restriction of the p-adic cyclotomic character χ_p to the inertia group $I_{\eta,ur}$ is trivial.

7.3.1.   *E has good reduction at η.*

PROPOSITION 7.13.   *Suppose the elliptic curve E has good reduction at the prime η. Then,*

$$pd_{\mathbb{Z}_p[[\widetilde{r}]]} H^0(\text{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee \leqslant 1.$$

Consequently, we have

$$(H^0(\text{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee)_{\text{P.N.}} = 0.$$

Proof. Since η is a prime not lying above p and since the elliptic curve E has good reduction at the prime η, we can conclude that the action of the inertia group $I_{\eta,ur}$ on $D_{E,\widetilde{\kappa}^{-1}}$ is trivial. As a result, we have

$$H^0(\text{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\widetilde{\kappa}^{-1}}) = H^0(\text{Gal}(K_\eta^{ur}/K_\eta), D_{E,\widetilde{\kappa}^{-1}}).$$

The eigenvalues of Frob_η, say a and b, on the p-adic Tate module $T_p(E)$ are distinct (see Theorem 4.1 in Coleman and Edixhoven's work [11]). Hence, the action of Frob_η on the free $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $(D_{E,\widetilde{\kappa}^{-1}})^\vee$ is semisimple. Let O denote the ring of integers in a finite extension of $\mathbb{Q}_p$, containing the eigenvalues a and b. This lets us deduce the following isomorphisms of $O[[\widetilde{\Gamma}]]$-modules:

$$
\begin{aligned}
&H^0(\mathrm{Gal}(K_\eta^{ur}/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee \otimes_{\mathbb{Z}_p} O \\
&\cong \mathrm{coker}\left(O[[\widetilde{\Gamma}]]^2 \xrightarrow{\begin{bmatrix} a^{-1}\widetilde{\kappa}(\mathrm{Frob}_\eta) - 1 & 0 \\ 0 & b^{-1}\widetilde{\kappa}(\mathrm{Frob}_\eta) - 1 \end{bmatrix}} O[[\widetilde{\Gamma}]]^2 \right) \\
&\cong \left(\frac{O[[\widetilde{\Gamma}]]}{(a^{-1}\widetilde{\kappa}(\mathrm{Frob}_\eta) - 1)} \right) \oplus \left(\frac{O[[\widetilde{\Gamma}]]}{(b^{-1}\widetilde{\kappa}(\mathrm{Frob}_\eta) - 1)} \right).
\end{aligned}
$$

As a result, we have

$$
\mathrm{pd}_{O[[\widetilde{\Gamma}]]} H^0(\mathrm{Gal}(K_\eta^{ur}/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee \otimes_{\mathbb{Z}_p} O \leqslant 1.
$$

These observations, along with [63, Corollary 3.2.10] and the fact that the extension $\mathbb{Z}_p \to O$ is faithfully flat, let us deduce that

$$
\mathrm{pd}_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee \leqslant 1
$$

and the proposition follows. $\qquad\square$

7.3.2. *E has additive reduction at η.*

PROPOSITION 7.14. *Suppose the elliptic curve E has additive reduction at the prime η. Then, we have*

$$
H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee = 0.
$$

Proof. Let $\mathfrak{m}$ denote the maximal ideal of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$. Note that we have the following isomorphism of $\mathbb{F}_p[\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta)]$-modules (see Observation (7iii)):

$$
D_{E,\widetilde{\kappa}^{-1}}[\mathfrak{m}] \cong E[p].
$$

We now claim that the trivial character is not a component of $E[p]^{s.s.}$, the semisimplification of the $\mathbb{F}_p[I_{\eta,ur}]$-representation $E[p]$. As a result, we would have

$$
H^0(I_{\eta,ur}, E[p]^{s.s.}) \overset{?}{=} 0. \tag{7.17}
$$

The proposition would follow from this claim (see Corollary 3.1.1 in Greenberg's work [**16**]). We consider two cases.

Case 1: E has potentially good reduction at η. The action of $I_{\eta,ur}$ factors through a nontrivial finite group Δ, such that the only prime factors dividing Δ are in the set $\{2, 3\}$. When $l \neq 3$, then the elliptic curve E attains good reduction over the field $K_\eta(E[3])$. See Proposition 10.3(b) in Ch. 10 of Silverman's book [**53**]. Note that $|\mathrm{Gal}(K_\eta(E[3])/K_\eta)|$ divides $|\mathrm{GL}_2(\mathbb{F}_3)|$ (which equals 48). When $l = 3$, then E attains good reduction over the fields $K_\eta(E[5])$ and $K_\eta(E[7])$. The ramification degrees of the field extensions $K_\eta(E[5])/K_\eta$ and $K_\eta(E[7])/K_\eta$ are equal and hence must divide $|\mathrm{Gal}(K_\eta(E[5])/K_\eta)|$ (which divides $|\mathrm{GL}_2(\mathbb{F}_5)| = 2^5 * 3 * 5$) and $|\mathrm{Gal}(K_\eta(E[7])/K_\eta)|$ (which divides $|\mathrm{GL}_2(\mathbb{F}_7)| = 2^5 * 3^2 * 7$). See [**52**, Problem 7.9(a)].

Choose an element ς in Δ that acts nontrivially on $T_p(E)$. The action of ς on $T_p(E)$ is via a 2×2 matrix, say B, with values in $\mathbb{Z}_p$. Since $\det(B)$ must equal 1 (see Observation (7iv)), the two eigenvalues of B are of the form b and b^{-1}. Both eigenvalues must be nontrivial roots of unity in $\overline{\mathbb{Q}}_p$, of order prime to p (since $p \geqslant 5$). As a result, we have $b \not\equiv 1 \mod p$ and $b^{-1} \not\equiv 1 \mod p$. Let $\overline{B}$ denote the 2×2 matrix with values in $\mathbb{F}_p$ which gives us the action of ς on $E[p]$. Our observations let us conclude that the eigenvalues of $\overline{B}$, which are $\overline{b}$ and $\overline{b}^{-1}$, are both not equal to one. This lets us establish the validity of equation (7.17) in this case.

Case 2: E has potentially split multiplicative reduction at η. In this case, we have the following short exact sequence of $\mathbb{Z}_p$-modules, that is $\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta)$-equivariant:

$$0 \to \mathbb{Z}_p(\chi_p\chi) \to T_p(E) \to \mathbb{Z}_p(\chi) \to 0.$$

Here, χ is a quadratic ramified character of $\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta)$. As a result, we have the following isomorphism of $\mathbb{F}_p[I_{\eta,ur}]$-modules:

$$E[p]^{s.s.} \cong \mathbb{F}_p(\chi) \oplus \mathbb{F}_p(\chi).$$

Since the restriction of χ to the inertia group $I_{\eta,ur}$ is a nontrivial quadratic character, equation (7.17) follows in this case too. $\qquad\square$

7.3.3. *E has nonsplit multiplicative reduction at η.*

PROPOSITION 7.15. *Suppose the elliptic curve E has nonsplit multiplicative reduction at the prime η. Then, we have*

$$pd_{\mathbb{Z}_p[[\tilde{r}]]} H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\tilde{\kappa}^{-1}})^\vee \leqslant 1.$$

Consequently, we have

$$(H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee)_{\mathrm{P.N.}} = 0.$$

Proof. Since E has nonsplit multiplicative reduction at η, we have the following short exact sequence of $\mathbb{Z}_p$-modules that is $\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta)$-equivariant:

$$0 \to \mathbb{Z}_p(\chi_p\chi) \to T_p(E) \to \mathbb{Z}_p(\chi) \to 0.$$

Here, χ is an unramified quadratic character. If we take the tensor product $\otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee(\widetilde{\kappa}^{-1})$, we obtain the following short exact sequence of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules, that is $\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta)$-equivariant:

$$0 \to \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee(\chi_p\chi\widetilde{\kappa}^{-1}) \to D_{E,\widetilde{\kappa}^{-1}} \to \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee(\chi\widetilde{\kappa}^{-1}) \to 0. \qquad (7.18)$$

The residual representation associated to the character $\chi\widetilde{\kappa}^{-1}$ coincides with the nontrivial quadratic character χ. As a result, $H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee(\chi\widetilde{\kappa}^{-1}))$ equals 0. Also note that the restriction of the character $\chi_p\chi\widetilde{\kappa}^{-1}$ to the inertia group $I_{\eta,ur}$ is trivial. Combining these observations and considering the $\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta)$-invariants of the modules given in the short exact sequence (7.18) let us deduce the following isomorphism of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$\begin{aligned} H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), \ D_{E,\widetilde{\kappa}^{-1}}) &\cong H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), \ \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee(\chi_p\chi\widetilde{\kappa}^{-1})), \\ &\cong H^0(\mathrm{Gal}(K_{\eta,ur}/K_\eta), \ \mathbb{Z}_p[[\widetilde{\Gamma}]]^\vee(\chi_p\chi\widetilde{\kappa}^{-1})). \end{aligned}$$

As a result, we have

$$H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee \cong \frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\chi_p\chi\widetilde{\kappa}^{-1}(\mathrm{Frob}_\eta) - 1)}.$$

The proposition follows. $\qquad\square$

7.3.4. *E has split multiplicative reduction at η.*

PROPOSITION 7.16. *Suppose the elliptic curve E has split multiplicative reduction at the prime η.*

$$H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee \cong \frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\chi_p\widetilde{\kappa}^{-1}(\mathrm{Frob}_\eta) - 1)} \oplus \frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\mathrm{ord}_{\pi_\eta}(q_{E,\eta}), \ \widetilde{\kappa}^{-1}(\mathrm{Frob}_\eta) - 1)}.$$

Consequently,

$$(H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee)_{\mathrm{P.N.}} \cong \frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\mathrm{ord}_{\pi_\eta}(q_{E,\eta}), \ \widetilde{\kappa}^{-1}(\mathrm{Frob}_\eta) - 1)}.$$

REMARK 7.17. Before proving Proposition 7.16, we make the following observations:

- If $K_\eta/\mathbb{Q}_l$ is an unramified quadratic extension, then $\chi_p(\mathrm{Frob}_\eta) = l^2$. Otherwise, $\chi_p(\mathrm{Frob}_\eta) = l$.

- p does not divide the element $\widetilde{\kappa}^{-1}(\mathrm{Frob}_\eta) - 1$.

- Proposition 7.16 lets us conclude that if the elliptic curve E has split multiplicative reduction at η, then $c_2((H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee)_{\mathrm{P.N.}})$ is nontrivial if and only if p divides $\mathrm{ord}_{\pi_\eta}(q_{E,\eta})$.

Proof of Proposition 7.16. Since E has split multiplicative reduction at η, there exists an element $q_{E,\eta} \in K_\eta^\times$ (usually called the Tate parameter) that gives us the following isomorphism $E(\overline{\mathbb{Q}}_l) \cong \overline{\mathbb{Q}}_l^\times/q_{E,\eta}$. We have the following short exact sequence of $\mathbb{Z}_p$-modules that is $\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta)$-equivariant:

$$0 \to \mathbb{Z}_p(\chi_p) \to T_p(E) \to \mathbb{Z}_p \to 0. \tag{7.19}$$

The action of $\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta)$ on $T_p(E)$ factors through $\mathrm{Gal}(K_\eta^{ur}(q_{E,\eta}^{1/p^\infty})/K_\eta)$, which fits into the following short exact sequence:

$$1 \to \underbrace{\mathrm{Gal}(K_\eta^{ur}(q_{E,\eta}^{1/p^\infty})/K_\eta^{ur})}_{\cong \mathbb{Z}_p} \to \mathrm{Gal}(K_\eta^{ur}(q_{E,\eta}^{1/p^\infty})/K_\eta) \to \underbrace{\mathrm{Gal}(K_\eta^{ur}/K_\eta)}_{\cong \widehat{\mathbb{Z}}} \to 1.$$

Let t_p denote a topological generator of $\mathrm{Gal}(K_\eta^{ur}(q_{E,\eta}^{1/p^\infty})/K_\eta^{ur})$. The action of t_p on $T_p(E)$ can be described by a 2×2 matrix $\begin{bmatrix} 1 & a_{t_p} \\ 0 & 1 \end{bmatrix}$ with values in $\mathbb{Z}_p$, where a_{t_p} is an element in $\mathbb{Z}_p$ satisfying

$$a_{t_p} = \mathrm{ord}_{\pi_\eta}(q_{E,\eta})u \quad \text{for some element } u \in \mathbb{Z}_p^\times.$$

One can choose a lift $\widetilde{\mathrm{Frob}}_\eta$ of Frob_η in $\mathrm{Gal}(K_\eta^{ur}(q_{E,\eta}^{1/p^\infty})/K_\eta)$ so that the action of $\widetilde{\mathrm{Frob}}_\eta$ on $T_p(E)$ is given by the 2×2 matrix $\begin{bmatrix} \chi_p(\mathrm{Frob}_\eta) & 0 \\ 0 & 1 \end{bmatrix}$.

The actions of t_p and $\widetilde{\mathrm{Frob}}_\eta$ on $D_{E,\widetilde{\kappa}^{-1}}$ are given by the following 2×2 matrices with values in $\mathbb{Z}_p[[\widetilde{\Gamma}]]$:

$$t_p \to \begin{bmatrix} 1 & a_{t_p} \\ 0 & 1 \end{bmatrix}, \quad \widetilde{\mathrm{Frob}}_\eta \to \begin{bmatrix} \chi_p\widetilde{\kappa}^{-1}(\mathrm{Frob}_\eta) & 0 \\ 0 & \widetilde{\kappa}^{-1}(\mathrm{Frob}_\eta) \end{bmatrix}.$$

Combining all the observations stated above, we have the following isomorphism of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$H^0(\mathrm{Gal}(\overline{\mathbb{Q}}_l/K_\eta), D_{E,\widetilde{\kappa}^{-1}})^\vee \cong \frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\chi_p\widetilde{\kappa}^{-1}(\mathrm{Frob}_\eta) - 1)} \oplus \frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{(\mathrm{ord}_{\pi_\eta}(q_{E,\eta}),\ \widetilde{\kappa}^{-1}(\mathrm{Frob}_\eta) - 1)}.$$

This completes the proof of the Proposition. $\square$

8. Numerical evidence towards the validity of Assumption GCD

In this section, we wish to provide some evidence towards the existence of elliptic curves E with supersingular reduction at an odd prime p such that the following two conditions hold:

(8i)   Assumption GCD holds for the pair $\{\theta_{4,2}^{++}, \theta_{4,2}^{+-}\}$. That is, the elements $\theta_{4,2}^{++}$, $\theta_{4,2}^{+-}$ have no common irreducible factor in the UFD $\mathbb{Z}_p[[\widetilde{\Gamma}]]$.

(8ii)   In $Z^2(\mathbb{Z}_p[[\widetilde{\Gamma}]])$, we have $c_2((\mathbb{Z}_p[[\widetilde{\Gamma}]])/((\theta_{4,2}^{++}, \theta_{4,2}^{+-}))) \neq 0$.

Let E_K denote the elliptic curve corresponding to the quadratic twist of E by the quadratic character $\epsilon_K : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \to \{\pm 1\}$. Since p splits in the imaginary quadratic field K, the elliptic curve E_K also has good supersingular reduction at p with $a_p(E_K) = 0$. In all the examples we consider, we also indicate how to unconditionally verify Conjecture 1.4.

8.1. Kobayashi's $\pm$ Selmer groups and Pollack's p-adic L-function.

We will recall the description of the p-adic L-functions $\theta_E^\pm$ and the Selmer groups $\mathrm{Sel}^\pm(\mathbb{Q}, D_{\rho_{2,1}})$ associated to the elliptic curve E. The p-adic L-functions $\theta_{E_K}^\pm$ and the Selmer groups $\mathrm{Sel}^\pm(\mathbb{Q}, D_{\rho_{2,1}(\epsilon_K)})$ associated to the elliptic curve E_K are defined similarly.

Let $\rho_{2,1} : G_\Sigma \to \mathrm{GL}_2(\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]])$ denote the Galois representation given by the action of G_Σ on the following free $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$-module of rank two:

$$T_{\rho_{2,1}} := T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]](\kappa_{\mathrm{cyc}}^{-1}).$$

We will also need to consider the following discrete $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$-module:

$$D_{\rho_{2,1}} := T_{\rho_{2,1}} \otimes_{\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]} \mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]], \mathbb{Q}_p/\mathbb{Z}_p).$$

We will recall Kobayashi's construction of $\pm$ Selmer groups over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ in [27]. We have the following local conditions at p:

$$E^+(\mathbb{Q}_p(\mu_{p^n}))$$
$$= \{P \in \widehat{E}(\mathbb{Q}_p(\mu_{p^n})) : \mathrm{Tr}_{n/m+1} P \in \widehat{E}(\mathbb{Q}_p(\mu_{p^m})), \text{ for odd } m < n\};$$
$$E^-(\mathbb{Q}_p(\mu_{p^n}))$$
$$= \{P \in \widehat{E}(\mathbb{Q}_p(\mu_{p^n})) : \mathrm{Tr}_{n/m+1} P \in \widehat{E}(\mathbb{Q}_p(\mu_{p^m})), \text{ for even } m < n\}.$$

Here, $\mathrm{Tr}_{n/m+1} : \widehat{E}(\mathbb{Q}_p(\mu_{p^n})) \to \widehat{E}(\mathbb{Q}_p(\mu_{p^{m+1}}))$ denotes the trace map. We set

$$E^\pm(\mathbb{Q}_{p,\mathrm{cyc}}) = \left(\bigcup_{n \geqslant 1} E^\pm(\mathbb{Q}_p(\mu_{p^n})) \right)^{\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_{p,\mathrm{cyc}})},$$

and $\mathrm{Loc}_\pm(\mathbb{Q}_p, D_{\rho_{2,1}}) \subset H^1(\mathbb{Q}_p, D_{\rho_{2,1}})$ is defined to be the image of the group $E^\pm(\mathbb{Q}_{p,\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ under the Kummer map. The $\pm$ Selmer groups are then given by

$$\mathrm{Sel}^\pm(\mathbb{Q}, D_{\rho_{2,1}})$$
$$= \ker\left(H^1(G_\Sigma, D_{\rho_{2,1}}) \to \frac{H^1(\mathbb{Q}_p, D_{\rho_{2,1}})}{\mathrm{Loc}_\pm(\mathbb{Q}_p, D_{\rho_{2,1}})} \oplus \bigoplus_{l \in \Sigma \setminus \{p\}} H^1(\mathbb{Q}_l, D_{\rho_{2,1}}) \right).$$

The Pontryagin duals of the $\pm$ Selmer groups are torsion modules over the ring $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$. See [27, Theorem 1.2].

REMARK 8.1. Our choice of signs $+$ and $-$ is opposite to the one used by Kobayashi [27]. The Selmer group that we have denoted by $\mathrm{Sel}^+(\mathbb{Q}, D_{\rho_{2,1}})$ (and $\mathrm{Sel}^-(\mathbb{Q}, D_{\rho_{2,1}})$ respectively) corresponds to Kobayashi's Selmer group in [27] with the minus sign (and plus sign respectively).

An important point to note is that since p splits in K, the $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules $\mathrm{Res}_K^{\mathbb{Q}}(D_{\rho_{2,1}})$, $D_{\rho_{2,1}}$ and $D_{\rho_{2,1}(\epsilon_K)}$ are isomorphic. This allows us to make the following identifications:

$$H^1(\mathbb{Q}_p, \mathrm{Res}_K^{\mathbb{Q}}(D_{\rho_{2,1}})) \cong H^1(\mathbb{Q}_p, D_{\rho_{2,1}}) \cong H^1(\mathbb{Q}_p, D_{\rho_{2,1}(\epsilon_K)}). \qquad (8.1)$$

Let $\bullet, \circ \in \{+, -\}$. Since the local Selmer conditions at p only depend on the isomorphism class of the elliptic curve over $\mathbb{Q}_p$, under the identification given in equation (8.1), we have the following identifications:

$$\mathrm{Loc}_\bullet(\mathbb{Q}_p, \mathrm{Res}_K^{\mathbb{Q}}(D_{\rho_{2,1}})) \cong \mathrm{Loc}_\bullet(\mathbb{Q}_p, D_{\rho_{2,1}}) \cong \mathrm{Loc}_\bullet(\mathbb{Q}_p, D_{\rho_{2,1}(\epsilon_K)}),$$
$$\mathrm{Loc}_\circ(\mathbb{Q}_p, \mathrm{Res}_K^{\mathbb{Q}}(D_{\rho_{2,1}})) \cong \mathrm{Loc}_\circ(\mathbb{Q}_p, D_{\rho_{2,1}}) \cong \mathrm{Loc}_\circ(\mathbb{Q}_p, D_{\rho_{2,1}(\epsilon_K)}).$$

The $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$-modules $\left(\frac{H^1(\mathbb{Q}_p, D_{\rho_{2,1}})}{\mathrm{Loc}_\bullet(\mathbb{Q}_p, D_{\rho_{2,1}})} \right)^\vee$ and $\left(\frac{H^1(\mathbb{Q}_p, D_{\rho_{2,1}(\epsilon_K)})}{\mathrm{Loc}_\circ(\mathbb{Q}_p, D_{\rho_{2,1}(\epsilon_K)})} \right)^\vee$ are both free of rank one by [27, Theorem 6.2]. Let us choose generators $b^\bullet$ and b° respectively

for these free modules inside $H^1(\mathbb{Q}_p, D_{\rho_{2,1}})^\vee$ (and thus, we have also chosen these generators inside $H^1(\mathbb{Q}_p, D_{\rho_{2,1}(\epsilon_K)})^\vee$). We also have the short exact sequences of $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$-modules:

$$0 \to \left(\frac{H^1(\mathbb{Q}_p, D_{\rho_{2,1}})}{\mathrm{Loc}_\bullet(\mathbb{Q}_p, D_{\rho_{2,1}})} \right)^\vee \xrightarrow{\mathrm{rest}_E} H^1(G_\Sigma, D_{\rho_{2,1}})^\vee \to \mathrm{Sel}^\bullet(\mathbb{Q}, D_{\rho_{2,1}})^\vee \to 0,$$
(8.2)

$$0 \to \left(\frac{H^1(\mathbb{Q}_p, D_{\rho_{2,1}(\epsilon_K)})}{\mathrm{Loc}_\circ(\mathbb{Q}_p, D_{\rho_{2,1}(\epsilon_K)})} \right)^\vee \xrightarrow{\mathrm{rest}_{E_K}} H^1(G_\Sigma, D_{\rho_{2,1}(\epsilon_K)})^\vee \to$$
$$\to \mathrm{Sel}^\circ(\mathbb{Q}, D_{\rho_{2,1}(\epsilon_K)})^\vee \to 0.$$

As mentioned above, the Pontryagin duals of the Selmer groups appearing in equation (8.2) are torsion [**27**, Theorem 1.2]. Consequently, the $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$-modules $H^1(G_\Sigma, D_{\rho_{2,1}})^\vee$ and $H^1(G_\Sigma, D_{\rho_{2,1}(\epsilon_K)})^\vee$ must have rank one. We can thus identify their reflexive hulls with the ring $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$. Moreover, the elements $\mathrm{rest}_E(b^\bullet)$ and $\mathrm{rest}_{E_K}(b^\circ)$ must be torsion-free over $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$. This in turn allows us to identify $\mathrm{rest}_E(b^\bullet)$ and $\mathrm{rest}_{E_K}(b^\circ)$ with elements of the ring $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$. Let us denote these elements by $\widetilde{\mathrm{rest}}_E(b^\bullet)$ and $\widetilde{\mathrm{rest}}_{E_K}(b^\circ)$ respectively. One may similarly define $\widetilde{\mathrm{rest}}_E(b^\circ)$ and $\widetilde{\mathrm{rest}}_{E_K}(b^\bullet)$. Let us also fix two elements c_E and c_{E_K} in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$ such that

$$\mathrm{Div}(c_E) = \mathrm{Div}(H^1_{\Sigma_0}(G_\Sigma, D_{\rho_{2,1}})^\vee_{\mathrm{tor}}) \text{ and } \mathrm{Div}(c_{E_K}) = \mathrm{Div}(H^1_{\Sigma_0}(G_\Sigma, D_{\rho_{2,1}(\epsilon_K)})^\vee_{\mathrm{tor}}).$$

Let us define the following elements in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$:

$$\begin{aligned} \vartheta_E^\bullet &:= \widetilde{\mathrm{rest}}_E(b^\bullet) \times c_E, & \vartheta_E^\circ &:= \widetilde{\mathrm{rest}}_E(b^\circ) \times c_E, \\ \vartheta_{E_K}^\bullet &:= \widetilde{\mathrm{rest}}_{E_K}(b^\bullet) \times c_{E_K}, & \vartheta_{E_K}^\circ &:= \widetilde{\mathrm{rest}}_{E_K}(b^\circ) \times c_{E_K}. \end{aligned}$$
(8.3)

Combining these observations and using the structure theorem for modules over principal ideal domains (PIDs), we have the following equality of divisors in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$:

$$\begin{aligned} \mathrm{Div}(\vartheta_E^\bullet) &= \mathrm{Div}(\mathrm{Sel}^\bullet(\mathbb{Q}, D_{\rho_{2,1}})^\vee), & \mathrm{Div}(\vartheta_E^\circ) &= \mathrm{Div}(\mathrm{Sel}^\circ(\mathbb{Q}, D_{\rho_{2,1}})^\vee), \\ \mathrm{Div}(\vartheta_{E_K}^\bullet) &= \mathrm{Div}(\mathrm{Sel}^\bullet(\mathbb{Q}, D_{\rho_{2,1}(\epsilon_K)})^\vee), & \mathrm{Div}(\vartheta_{E_K}^\circ) &= \mathrm{Div}(\mathrm{Sel}^\circ(\mathbb{Q}, D_{\rho_{2,1}(\epsilon_K)})^\vee). \end{aligned}$$

REMARK 8.2. Choosing a different generator for $\left(\frac{H^1(\mathbb{Q}_p, D_{\rho_{2,1}})}{\mathrm{Loc}_\bullet(\mathbb{Q}_p, D_{\rho_{2,1}})} \right)^\vee$ changes $\widetilde{\mathrm{rest}}_E(b^\bullet)$ and $\widetilde{\mathrm{rest}}_{E_K}(b^\bullet)$ by the same unit in the ring $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$. One obtains a similar conclusion by replacing $\bullet$ with $\circ$. By choosing a different identification of the reflexive hull of $H^1(G_\Sigma, D_{\rho_{2,1}})^\vee$ with the ring $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$, one modifies $\widetilde{\mathrm{rest}}_E(b^\bullet)$ and $\widetilde{\mathrm{rest}}_E(b^\circ)$ by the same unit in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$. One obtains a similar

conclusion by replacing E with E_K. We may also modify c_E and c_{E_K} by units in $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$. However, for all these different choices, the ideal $(\vartheta_E^\bullet \vartheta_{E_K}^\circ + \vartheta_E^\circ \vartheta_{E_K}^\bullet)$ in $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$ remains the same.

Kobayashi's Selmer groups are related to Pollack's $\pm$ one-variable p-adic L-functions defined in [44]. Let L_λ denote the classical p-adic L-function of Amice and Vélu [1] and Višik [60], where λ is of one the two roots of the Hecke polynomial $X^2 + p$. We may consider L_λ as a power series in $\mathbb{Q}_p(\sqrt{-p})[[\gamma - 1]]$ (where γ is a fixed topological generator of Γ_{cyc}) and a $\mathbb{Q}_p(\sqrt{-p})$-valued distribution on Γ_{cyc} interchangeably via Amice's transform. There exist two elements $\theta_E^\pm \in \mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$ such that

$$L_\lambda = \log_p^+ \theta_E^+ + \lambda \log_p^- \theta_E^-,$$

where $\log_p^\pm$ is the power series defined in Pollack's work [44] using cyclotomic polynomials in γ. See [12] for a description of the corresponding distributions under Amice transform.

The p-adic L-functions $\theta_E^\pm$ satisfy the following interpolation properties: let ψ be a nontrivial Dirichlet character of conductor p^n on Γ_{cyc}, with n odd. Then,

$$\theta_E^-(\psi) = (-1)^{(n+1)/2} \frac{p^n}{\tau_{\mathbb{Q}}(\psi^{-1}) \prod_{\substack{1 \leqslant k < n \\ k \text{ odd}}} \Phi_{p^k}(\zeta)} \times \frac{L(E, \psi^{-1}, 1)}{\Omega_E^-}. \tag{8.4}$$

Similarly, if ψ is a nontrivial Dirichlet character of conductor p^n on Γ_{cyc}, with n even, then

$$\theta_E^+(\psi) = (-1)^{n/2} \frac{p^n}{\tau_{\mathbb{Q}}(\psi^{-1}) \prod_{\substack{1 \leqslant k < n \\ k \text{ even}}} \Phi_{p^k}(\zeta)} \times \frac{L(E, \psi^{-1}, 1)}{\Omega_E^+}. \tag{8.5}$$

Here, $\tau_{\mathbb{Q}}(\psi^{-1})$ denotes the Gauss sum of ψ^{-1}, Φ_{p^k} denotes the p^kth cyclotomic polynomial, ζ denotes $\psi(\gamma)$ which is a primitive p^{n-1}-root of unity, the complex numbers $\Omega_E^\pm$ denote the real (and imaginary) Néron periods associated to the elliptic curve E.

Note that $\theta_E^\pm$ are uniquely determined by equation (8.4) and equation (8.5) respectively. As in the two-variable case (cf. Remark 6.3), choosing a different topological generator of Γ_{cyc} changes the p-adic L-function by a factor u, for some unit u in the ring $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$.

We will consider the following Iwasawa main conjecture formulated by Kobayashi [27]:

CONJECTURE 8.3. *Let* $\bullet, \circ \in \{\pm\}$. *We have*

$$\text{Div}(\vartheta_E^\bullet) = \text{Div}(\theta_E^\bullet), \quad \text{Div}(\vartheta_{E_K}^\circ) = \text{Div}(\theta_E^\circ)$$

as equalities in $Z^1(\mathbb{Z}_p[[\Gamma_{\text{cyc}}]])$.

8.2.   Outline of strategy.   We briefly outline our strategy to prove the existence of elliptic curves verifying (8i) and (8ii). Consider the one-variable p-adic L-functions $\theta_E^\pm$, $\theta_{E_K}^\pm$ associated to the elliptic curves E and E_K respectively and $\vartheta_E^\pm$, $\vartheta_{E_K}^\pm$ as defined in equation (8.3). For any $\bullet, \circ \in \{\pm\}$, let $\vartheta_{4,2}^{\bullet\circ}$ be an element in $\mathbb{Z}_p[[\widetilde{\Gamma}]]$ such that $\mathrm{Div}(\vartheta_{4,2}^{\bullet\circ})$ equals $\mathrm{Div}(\mathrm{Sel}^{\bullet\circ}(\mathbb{Q}, D_{\rho_{4,2}})^\vee)$ in $Z^1(\mathbb{Z}_p[[\widetilde{\Gamma}]])$.

Under the natural projection map (which one can view as the 'cyclotomic specialization')

$$\pi_{\mathrm{cyc}} : \mathbb{Z}_p[[\widetilde{\Gamma}]] \to \mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]],$$

we prove the following equalities of ideals in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$:

$$(\pi_{\mathrm{cyc}}(\vartheta_{4,2}^{++})) = (\vartheta_E^+ \vartheta_{E_K}^+), \quad (\pi_{\mathrm{cyc}}(\vartheta_{4,2}^{+-})) = (\vartheta_E^+ \vartheta_{E_K}^- + \vartheta_E^- \vartheta_{E_K}^+). \tag{8.6}$$

Equation (8.6) is proved in Section 8.3. If we assume the validity of Conjectures 1.3 and 8.3, there exists a unit u in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$ such that we have the following equalities of ideals in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$:

$$(\pi_{\mathrm{cyc}}(\theta_{4,2}^{++})) = (\theta_E^+ \theta_{E_K}^+), \quad (\pi_{\mathrm{cyc}}(\theta_{4,2}^{+-})) = (\theta_E^+ \theta_{E_K}^- + u\theta_E^- \theta_{E_K}^+). \tag{8.7}$$

The table given in Section 8.4 has examples of elliptic curves E, primes p and imaginary quadratic fields K satisfying the following conditions:

(8a) θ_E^+ is a unit in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$.

(8b) $\theta_{E_K}^+$ and $\theta_{E_K}^-$ have no common irreducible factor in the UFD $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$.

(8c) $\theta_{E_K}^+$ and $\theta_{E_K}^-$ are not units in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$.

Suppose, as indicated by condition (8a), that θ_E^+ is a unit in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$. The ratio of the two values obtained by specializing the p-adic L-functions θ_E^+ and θ_E^- at the trivial character is a p-adic unit (in fact, it is equal to $(p-1)/2$). See [27, Equation (3.6)]. As a result, θ_E^- is also a unit in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$. In this case, $\theta_E^+ \theta_{E_K}^+$ and $\theta_E^+ \theta_{E_K}^- + u\theta_E^- \theta_{E_K}^+$ have no common irreducible factor in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$ if and only if $\theta_{E_K}^+$ and $\theta_{E_K}^-$ have no common irreducible factor in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$.

Note that Assumption GCD holds for the pair $\{\vartheta_{4,2}^{++}, \vartheta_{4,2}^{+-}\}$ if $\pi_{\mathrm{cyc}}(\vartheta_{4,2}^{++})$ and $\pi_{\mathrm{cyc}}(\vartheta_{4,2}^{+-})$ have no common irreducible factor in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$. Assume the validity of Conjectures 1.3 and 8.3. Conditions (8a) and (8b), along with equation (8.7), then let us deduce that Assumption GCD holds for the pair $\{\theta_{4,2}^{++}, \theta_{4,2}^{+-}\}$. Condition (8c) lets us deduce that $c_2((\mathbb{Z}_p[[\widetilde{\Gamma}]])/(\theta_{4,2}^{++}, \theta_{4,2}^{+-})) \neq 0$.

For all the curves given in the table in Section 8.4, it will be possible to unconditionally verify Conjecture 1.4. When the elliptic curve has complex multiplication (CM), Pollack and Rubin [45] have proved Conjecture 8.3. If E

and E_K are elliptic curves without CM such that the p-adic Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$, given by the action of $G_{\mathbb{Q}}$ on the corresponding p-adic Tate modules is surjective, Kobayashi [**27**, Theorem 4.1] has shown that we have the following inequality of divisors in $Z^1(\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]])$:

$$\mathrm{Div}(\vartheta_E^{\pm}) \leqslant \mathrm{Div}(\theta_E^{\pm}), \quad \mathrm{Div}(\vartheta_{E_K}^{\pm}) \leqslant \mathrm{Div}(\theta_{E_K}^{\pm}). \tag{8.8}$$

If the Galois representations given by the action of $G_{\mathbb{Q}}$ on the p-adic Tate modules are not known to be surjective, then Kobayashi establishes the inequality (8.8) in $Z^1(\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]][1/p])$. When the elliptic curve does not have CM, further progress under certain hypotheses towards Conjecture 8.3 has been made by Wan [**62**].

We use Sage [**59**] to numerically establish that the Galois representations given by the action of $G_{\mathbb{Q}}$ on the p-adic Tate modules are surjective; hence in these examples the inequalities in equation (8.8) hold unconditionally. We can argue as we did earlier. Using conditions (8a) and (8b) along with equation (8.6), we can conclude that $\pi_{\mathrm{cyc}}(\vartheta_{4,2}^{++})$ and $\pi_{\mathrm{cyc}}(\vartheta_{4,2}^{+-})$ have no common irreducible factor in $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$. As a result, $\vartheta_{4,2}^{++}$ and $\vartheta_{4,2}^{+-}$ must have no common irreducible factor in $\mathbb{Z}_p[[\widetilde{\Gamma}]]$ and we can thus conclude that the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\mathrm{III}^1(\mathbb{Q}, D_{\rho_{4,2}})^{\vee}$ is pseudonull (see equations (8.27) and (8.29)).

8.3. Projection to the cyclotomic line.

Consider the following ring homomorphism, induced by the natural surjection $\widetilde{\Gamma} \to \Gamma_{\mathrm{cyc}}$:

$$\pi_{\mathrm{cyc}} : \mathbb{Z}_p[[\widetilde{\Gamma}]] \to \mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]].$$

PROPOSITION 8.4. *Let* $\bullet, \circ \in \{\pm\}$. *Then, we have the following equality of ideals in* $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$:

$$(\pi_{\mathrm{cyc}}(\vartheta_{4,2}^{\bullet\circ})) = (\vartheta_E^{\bullet}\vartheta_{E_K}^{\circ} + \vartheta_E^{\circ}\vartheta_{E_K}^{\bullet}). \tag{8.9}$$

As a result, if we assume the validity of Conjectures 1.3 *and* 8.3, *there exists a unit* u *in* $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$ *such that we have the following equalities of ideals in* $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$:

$$(\pi_{\mathrm{cyc}}(\theta_{4,2}^{++})) = (\theta_E^+\theta_{E_K}^+), \quad (\pi_{\mathrm{cyc}}(\theta_{4,2}^{--})) = (\theta_E^-\theta_{E_K}^-),$$
$$(\pi_{\mathrm{cyc}}(\theta_{4,2}^{+-})) = (\pi_{\mathrm{cyc}}(\theta_{4,2}^{-+})) = (\theta_E^+\theta_{E_K}^- + u\theta_E^-\theta_{E_K}^+).$$

Proof. The equality of divisors

$$\mathrm{Div}(\vartheta_{4,2}^{\bullet\circ}) = \mathrm{Div}(\mathrm{Sel}^{\bullet\circ}(\mathbb{Q}, D_{\rho_{4,2}})^{\vee})$$

in $Z^1(\mathbb{Z}_p[[\widetilde{\Gamma}]])$ lets us deduce the following equality of divisors in $Z^1(\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]])$:

$$\mathrm{Div}(\pi_{\mathrm{cyc}}(\vartheta_{4,2}^{\bullet\circ})) = \mathrm{Div}(\mathrm{Sel}^{\bullet\circ}(\mathbb{Q}, D_{\rho_{4,2}})^{\vee} \otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} \mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]). \tag{8.10}$$

We adopt a convention that sets the divisor of a torsion-free module and $\text{Div}(0)$ to equal 'infinity'.

Equation (8.10) follows by applying [**40**, Proposition 5.2] to the specialization map $\pi_{\text{cyc}} : \mathbb{Z}_p[[\widetilde{\Gamma}]] \to \mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$ of regular local rings. The only hypotheses from [**40**, Proposition 5.2] that needs to be verified is that the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\text{Sel}^{\bullet\circ}(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ has no nontrivial pseudonull submodules. This follows from Proposition 4.1.1 in Greenberg's work [**18**].

Let Σ_0 denote $\Sigma \setminus \{p\}$. Following [**16**], we define

$$H^1_{\Sigma_0}(G_\Sigma, D_{\rho_{4,2}}) := \ker\left(H^1(G_\Sigma, D_{\rho_{4,2}}) \to \bigoplus_{v \in \Sigma_0} H^1(\mathbb{Q}_v, D_{\rho_{4,2}}) \right). \quad (8.11)$$

One can define a discrete $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-module $D_{\pi_{\text{cyc}} \circ \rho_{4,2}}$ associated to the Galois representation $\pi_{\text{cyc}} \circ \rho_{4,2}$, similar to the definition of the discrete $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $D_{\rho_{4,2}}$ associated to $\rho_{4,2}$. We may also similarly define $H^1_{\Sigma_0}(G_\Sigma, D_{\pi_{\text{cyc}} \circ \rho_{4,2}})$, $H^1_{\Sigma_0}(G_\Sigma, D_{\rho_{2,1}})$ and $H^1_{\Sigma_0}(G_\Sigma, D_{\rho_{2,1}(\epsilon_K)})$.

Using [**16**, Proposition 3.4] along with Hypothesis $\text{Loc}_p(0)$, we have the following isomorphisms of $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-modules:

$$H^1(G_\Sigma, D_{\pi_{\text{cyc}} \circ \rho_{4,2}}) \cong H^1(G_\Sigma, D_{\rho_{4,2}})[\ker(\pi_{\text{cyc}})]. \quad (8.12)$$

$$H^1(\mathbb{Q}_p, D_{\pi_{\text{cyc}} \circ \rho_{4,2}}) \cong H^1(\mathbb{Q}_p, D_{\rho_{4,2}})[\ker(\pi_{\text{cyc}})]. \quad (8.13)$$

For $\ell \nmid p$, the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_{l,\text{cyc}}$ is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}_l$. Consequently, the decomposition group of any prime of K over ℓ in $\text{Gal}(\widetilde{K}_\infty/K_{\text{cyc}})$ is trivial. This lets us obtain the following isomorphism of $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-modules:

$$H^1(\mathbb{Q}_\ell, D_{\pi_{\text{cyc}} \circ \rho_{4,2}}) \cong H^1(\mathbb{Q}_\ell, D_{\rho_{4,2}})[\ker(\pi_{\text{cyc}})]. \quad (8.14)$$

Equations (8.12) and (8.14) let us deduce the following isomorphism of $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-modules

$$H^1_{\Sigma_0}(G_\Sigma, D_{\pi_{\text{cyc}} \circ \rho_{4,2}}) \cong H^1_{\Sigma_0}(G_\Sigma, D_{\rho_{4,2}})[\ker(\pi_{\text{cyc}})]. \quad (8.15)$$

The ring map π_{cyc} induces the following decomposition of Galois representations:

$$\pi_{\text{cyc}} \circ \rho_{4,2} \cong \rho_{2,1} \oplus \rho_{2,1}(\epsilon_K). \quad (8.16)$$

As a manifestation of the isomorphism in (8.16), we have the following isomorphism of $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-modules:

$$H^1(G_\Sigma, D_{\pi_{\mathrm{cyc}} \circ \rho_{4,2}}) \cong H^1(G_\Sigma, D_{\rho_{2,1}}) \oplus H^1(G_\Sigma, D_{\rho_{2,1}(\epsilon_K)}), \qquad (8.17)$$
$$H^1(\mathbb{Q}_p, D_{\pi_{\mathrm{cyc}} \circ \rho_{4,2}}) \cong H^1(\mathbb{Q}_p, D_{\rho_{2,1}}) \oplus H^1(\mathbb{Q}_p, D_{\rho_{2,1}(\epsilon_K)}),$$
$$H^1(\mathbb{Q}_l, D_{\pi_{\mathrm{cyc}} \circ \rho_{4,2}}) \cong H^1(\mathbb{Q}_l, D_{\rho_{2,1}}) \oplus H^1(\mathbb{Q}_l, D_{\rho_{2,1}(\epsilon_K)}), \quad \forall l \in \Sigma \setminus \{p\}.$$

These observations, along with equation (8.15), let us deduce the following isomorphism of $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$-modules:

$$H^1_{\Sigma_0}(G_\Sigma, D_{\rho_{4,2}})[\ker(\pi_{\mathrm{cyc}})] \cong H^1_{\Sigma_0}(G_\Sigma, D_{\rho_{2,1}}) \oplus H^1_{\Sigma_0}(G_\Sigma, D_{\rho_{2,1}(\epsilon_K)}). \quad (8.18)$$

The discrete module $D_{\pi_{\mathrm{cyc}} \circ \rho_{4,2}}$ can be identified with

$$\mathrm{Res}^{\mathbb{Q}}_K(D_{\rho_{2,1}}) \oplus \widetilde{\delta} \otimes \mathrm{Res}^{\mathbb{Q}}_K(D_{\rho_{2,1}}).$$

Here, $\widetilde{\delta}$ denotes a complex conjugation, which is an element of order 2 in G_Σ. We can also describe the Galois action on $\mathrm{Res}^{\mathbb{Q}}_K(D_{\rho_{2,1}}) \oplus \widetilde{\delta} \otimes \mathrm{Res}^{\mathbb{Q}}_K(D_{\rho_{2,1}})$:

$$\widetilde{\delta} \cdot (x, \widetilde{\delta} \otimes y) = (y, \widetilde{\delta} \otimes x),$$
$$h \cdot (x, \widetilde{\delta} \otimes y) = (hx, \widetilde{\delta} \otimes (\widetilde{\delta} h \widetilde{\delta} y)), \quad \forall h \in \mathrm{Gal}(\mathbb{Q}_\Sigma/K).$$

We can identify $D_{\rho_{2,1}(\epsilon_K)}$ with $D_{\rho_{2,1}}(\epsilon_K)$. It will be helpful to make the isomorphism in equation (8.16) explicit.

$$\mathrm{Res}^{\mathbb{Q}}_K(D_{\rho_{2,1}}) \oplus \widetilde{\delta} \otimes \mathrm{Res}^{\mathbb{Q}}_K(D_{\rho_{2,1}}) \cong D_{\rho_{2,1}} \oplus D_{\rho_{2,1}(\epsilon_K)}, \qquad (8.19)$$
$$(x, 0) \to (x, x),$$
$$(0, \widetilde{\delta} \otimes y) \to (y, -y).$$

Throughout the proof, we will keep the identifications in equation (8.1) in mind. We now proceed to establish control for the local condition at p. Following Section 6, the discrete module $H^1(\mathbb{Q}_p, D_{\rho_{4,2}})$ can be identified with

$$\bigoplus_{\mathfrak{P} \mid \mathfrak{p}} H^1((\widetilde{K}_\infty)_{\mathfrak{P}}, E[p^\infty]) \oplus \bigoplus_{\mathfrak{Q} \mid \mathfrak{q}} H^1((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty]),$$

whereas $H^1(\mathbb{Q}_p, D_{\pi_{\mathrm{cyc}} \circ \rho_{4,2}})$ can be identified with

$$H^1(\mathbb{Q}_p, \mathrm{Res}^{\mathbb{Q}}_K(D_{\rho_{2,1}})) \oplus \widetilde{\delta} \otimes H^1(\mathbb{Q}_p, \mathrm{Res}^{\mathbb{Q}}_K(D_{\rho_{2,1}})).$$

We have natural injections of $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$-modules:

$$\mathrm{Loc}_\bullet(\mathbb{Q}_p, \mathrm{Res}^{\mathbb{Q}}_K(D_{\rho_{2,1}})) \hookrightarrow \left(\bigoplus_{\mathfrak{P} \mid \mathfrak{p}} \mathrm{Loc}_\bullet((\widetilde{K}_\infty)_{\mathfrak{P}}, E[p^\infty]) \right)[\ker(\pi_{\mathrm{cyc}})], \quad (8.20)$$
$$\widetilde{\delta} \otimes \mathrm{Loc}_\circ(\mathbb{Q}_p, \mathrm{Res}^{\mathbb{Q}}_K(D_{\rho_{2,1}})) \hookrightarrow \left(\bigoplus_{\mathfrak{Q} \mid \mathfrak{q}} \mathrm{Loc}_\circ((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty]) \right)[\ker(\pi_{\mathrm{cyc}})].$$

On the one hand, Proposition 2.11 in Kim's work [26] lets us deduce that the Pontryagin duals of the $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$-modules

$$\left(\bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Loc}_\bullet((\widetilde{K}_\infty)_{\mathfrak{P}}, E[p^\infty])\right)[\ker(\pi_{\mathrm{cyc}})],$$

$$\left(\bigoplus_{\mathfrak{Q}|\mathfrak{q}} \mathrm{Loc}_\circ((\widetilde{K}_\infty)_{\mathfrak{Q}}, E[p^\infty])\right)[\ker(\pi_{\mathrm{cyc}})], \tag{8.21}$$

are free of rank one. On the other hand, Theorems 2.7 and 2.8 in Kim's work [26] let us deduce that the Pontryagin duals of the $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$-modules

$$\mathrm{Loc}_\bullet(\mathbb{Q}_p, \mathrm{Res}_K^{\mathbb{Q}}(D_{\rho_{2,1}})), \quad \widetilde{\delta} \otimes \mathrm{Loc}_\circ(\mathbb{Q}_p, \mathrm{Res}_K^{\mathbb{Q}}(D_{\rho_{2,1}})),$$

are also free of rank one. Consequently, the maps in equation (8.20) must be isomorphisms.

Recall that we have a short exact sequence

$$0 \to \left(\frac{H^1(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})}\right)^\vee \to H^1(\mathbb{Q}_p, D_{\rho_{4,2}})^\vee \to \mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})^\vee \to 0$$

of free $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules. Taking the tensor product $\otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]}\frac{\mathbb{Z}_p[[\widetilde{\Gamma}]]}{\ker(\pi_{\mathrm{cyc}})}$ and then considering the Pontryagin dual, we obtain the following isomorphism of discrete $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$-modules:

$$\frac{H^1(\mathbb{Q}_p, D_{\rho_{4,2}})}{\mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})}[\ker(\pi_{\mathrm{cyc}})] \cong \frac{H^1(\mathbb{Q}_p, D_{\rho_{4,2}})[\ker(\pi_{\mathrm{cyc}})]}{\mathrm{Loc}_{\bullet\circ}(\mathbb{Q}_p, D_{\rho_{4,2}})[\ker(\pi_{\mathrm{cyc}})]}. \tag{8.22}$$

We have the following commutative diagram

Note that coker(rest $\circ$ j) is isomorphic to coker(rest$_0$ $\circ$ j_0). Analysing the maps on the left side, we have the following isomorphism of $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$-modules:

$$\mathrm{coker}(\mathrm{rest} \circ j) \cong \mathrm{Sel}^{\bullet\circ}(\mathbb{Q}, D_{\rho_{4,2}})^\vee \otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} \mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]. \tag{8.23}$$

Using equation (8.10), we can deduce the following equality of divisors:

$$\text{Div}(\text{coker}(\text{rest} \circ j)) = \text{Div}(\pi_{\text{cyc}}(\vartheta_{4,2}^{\bullet\circ})). \tag{8.24}$$

Using the description given in equation (8.19), we have

$$j_0(b^\bullet, 0) = (b^\bullet, b^\bullet), \quad j_0(0, \widetilde{\delta} \otimes b^\circ) = (b^\circ, -b^\circ).$$

The $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-module $\text{Image}(\text{rest}_0 \circ j_0)$ is generated by the two vectors $(\text{rest}_E(b^\bullet), \text{rest}_{E_K}(b^\bullet))$ and $(\text{rest}_E(b^\circ), \text{rest}_{E_K}(b^\circ))$. Suppose $\text{coker}(\text{rest}_0 \circ j_0)$ is a torsion $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-module. Note that $\text{Image}(\text{rest}_0 \circ j_0)$ must be a torsion-free $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-module. To see this, it is enough to observe that the domain of $\text{rest}_0 \circ j_0$ is a free $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-module of rank two, whereas the codomain of the map is a $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-module of rank two. By localizing at every height one prime ideal of the ring $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$ and using the structure theorem for PIDs, we can conclude that the divisor $\text{Div}(\text{coker}(\text{rest}_0 \circ j_0))$ is equal to

$$\text{Div}\left(\det\begin{bmatrix} \widetilde{\text{rest}}_E(b^\bullet) & \widetilde{\text{rest}}_{E_K}(b^\bullet) \\ \widetilde{\text{rest}}_E(b^\circ) & -\widetilde{\text{rest}}_{E_K}(b^\circ) \end{bmatrix}\right)$$
$$+ \text{Div}(H^1_{\Sigma_0}(G_\Sigma, D_{\rho_{2,1}})^\vee_{\text{tor}}) + \text{Div}(H^1_{\Sigma_0}(G_\Sigma, D_{\rho_{2,1}(\epsilon_K)})^\vee_{\text{tor}}).$$

Combining the above observation with equation (8.3), we have

$$\text{Div}(\text{coker}(\text{rest}_0 \circ j_0)) = \text{Div}(\vartheta_E^\bullet \vartheta_{E_K}^\circ + \vartheta_E^\circ \vartheta_{E_K}^\bullet). \tag{8.25}$$

Combining equations (8.24) and (8.25), we have the following equality of divisors in $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$:

$$\text{Div}(\pi_{\text{cyc}}(\vartheta_{4,2}^{\bullet\circ})) = \text{Div}(\vartheta_E^\bullet \vartheta_{E_K}^\circ + \vartheta_E^\circ \vartheta_{E_K}^\bullet). \tag{8.26}$$

If the $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-module $\text{coker}(\text{rest}_0 \circ j_0)$ is not torsion, then the determinant $\det\begin{bmatrix} \widetilde{\text{rest}}_E(b^\bullet) & \widetilde{\text{rest}}_{E_K}(b^\bullet) \\ \widetilde{\text{rest}}_E(b^\circ) & -\widetilde{\text{rest}}_{E_K}(b^\circ) \end{bmatrix}$ must equal zero. By (8.23), the $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$-module

$$\text{Sel}^{\bullet\circ}(\mathbb{Q}, D_{\rho_{4,2}})^\vee \otimes_{\mathbb{Z}_p[[\widetilde{\Gamma}]]} \mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$$

is also not torsion. Equality in equation (8.26) still holds, where both terms now equal 'infinity'. The proposition follows. □

REMARK 8.5. In the equal sign case, since p is odd, Proposition 8.4 lets us deduce the equality of ideals in $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$ given by $(\pi_{\text{cyc}}(\vartheta_{4,2}^{++})) = (\vartheta_E^+ \vartheta_{E_K}^+)$ and $(\pi_{\text{cyc}}(\vartheta_{4,2}^{--})) = (\vartheta_E^- \vartheta_{E_K}^-)$. By [27, Theorem 1.2], the elements $\vartheta_E^\pm$ and $\vartheta_{E_K}^\pm$ are nonzero. Thus, the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules $\text{Sel}^{++}(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ and $\text{Sel}^{--}(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ are torsion. It is possible to deduce the following equality of ideals in $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$:

$$(\pi_{\text{cyc}}(\theta_{4,2}^{++})) = (\theta_E^+ \theta_{E_K}^+), \quad (\pi_{\text{cyc}}(\theta_{4,2}^{--})) = (\theta_E^- \theta_{E_K}^-),$$

without assuming the validity of Conjectures 1.3 and 8.3. Consider a finite Galois character $\psi : \text{Gal}(K_{\text{cyc}}/K) \to \overline{\mathbb{Q}}_p^\times$ with conductor (p^n), for some even positive integer n. Abusing notation, we also let $\psi : \mathbb{Z}_p[[\text{Gal}(K_{\text{cyc}}/K)]] \to \overline{\mathbb{Q}}_p$ denote the corresponding ring homomorphism. Recall that we chose $\gamma_{\mathfrak{q}}$ to be the image of $\gamma_{\mathfrak{p}}$ under the ring automorphism $\mathbb{Z}_p[[\widetilde{\Gamma}]] \to \mathbb{Z}_p[[\widetilde{\Gamma}]]$ induced by complex conjugation. We have $\psi(\gamma_{\mathfrak{p}}) = \psi(\gamma_{\mathfrak{q}})$ whenever ψ factors through $\text{Gal}(K_{\text{cyc}}/K)$. Using equation (6.8), we obtain the following equalities:

$$\psi(\pi_{\text{cyc}}(\theta_{4,2}^{++})) = \frac{p^{2n}}{\tau_K(\psi^{-1})} \times \frac{L(E/K, \psi^{-1}, 1)}{\Omega_{f_E}^+ \Omega_{f_E}^- \left(\prod_{\substack{1 \leqslant k < n \\ k \text{ even}}} \Phi_{p^k}(\zeta)\right)^2}$$

$$= \frac{p^{2n}}{\tau_K(\psi^{-1})} \times \frac{L(E, \psi^{-1}, 1) L(E_K, \psi^{-1}, 1)}{\Omega_{f_E}^+ \Omega_{f_E}^- \left(\prod_{\substack{1 \leqslant k < n \\ k \text{ even}}} \Phi_{p^k}(\zeta)\right)^2}.$$

We may identify $\text{Gal}(K_{\text{cyc}}/K)$ with Γ_{cyc} and choose $\gamma_{\text{cyc}} := (\gamma_{\mathfrak{p}}\gamma_{\mathfrak{q}})^{1/2}$ to be the topological generator of Γ_{cyc} (it is possible to take a square root, since p is odd). Then, $\psi(\gamma_{\mathfrak{p}}) = \psi(\gamma_{\mathfrak{q}}) = \psi(\gamma_{\text{cyc}})$ for all characters ψ on $\text{Gal}(K_{\text{cyc}}/K)$. Observe that $\tau_K(\psi^{-1}) = \tau_{\mathbb{Q}}(\psi^{-1})^2$. On comparing the interpolation formula above with equation (8.5), we deduce that the following equality in $\overline{\mathbb{Q}}_p$:

$$\psi(\pi_{\text{cyc}}(\theta_{4,2}^{++})) = \frac{\Omega_E^+}{\Omega_{f_E}^+} \frac{\Omega_{E_K}^+}{\Omega_{f_{E_K}}^+} \frac{\Omega_{f_{E_K}}^+}{\Omega_{f_E}^-} \times \psi(\theta_E^+ \theta_{E_K}^+).$$

Since this holds for infinitely many characters ψ, we have the following equality in $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$:

$$\pi_{\text{cyc}}(\theta_{4,2}^{++}) = \frac{\Omega_E^+}{\Omega_{f_E}^+} \frac{\Omega_{E_K}^+}{\Omega_{f_{E_K}}^+} \frac{\Omega_{f_{E_K}}^+}{\Omega_{f_E}^-} \times \theta_E^+ \theta_{E_K}^+.$$

The ratios $\Omega_E^+/\Omega_{f_E}^+$ and $\Omega_{E_K}^+/\Omega_{f_{E_K}}^+$ are units in the localization $\mathbb{Z}_{(p)}$. See Remark 5.5 in Rob Pollack's work [44]. The ratio $\Omega_{f_{E_K}}^+/\Omega_{f_E}^-$ is also a unit in the localization $\mathbb{Z}_{(p)}$. See Skinner–Zhang's work [55, Lemma 9.6]). Our claim now follows.

By considering cyclotomic characters whose conductors are odd powers of p, we may deduce in the same way the following factorization in $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$:

$$\pi_{\text{cyc}}(\theta_{4,2}^{--}) = \frac{\Omega_E^-}{\Omega_{f_E}^-} \frac{\Omega_{E_K}^-}{\Omega_{f_{E_K}}^-} \frac{\Omega_{f_{E_K}}^-}{\Omega_{f_E}^+} \times \theta_E^- \theta_{E_K}^-.$$

REMARK 8.6. In the mixed sign case, Proposition 8.4 lets us deduce the equality of ideals in $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$ given by $(\pi_{\text{cyc}}(\vartheta_{4,2}^{+-})) = (\pi_{\text{cyc}}(\vartheta_{4,2}^{-+})) = (\vartheta_E^+ \vartheta_{E_K}^- + \vartheta_E^- \vartheta_{E_K}^+)$.

After the completion of our project, we learnt that in the preprint [**7**, Proposition 3.5], the authors have explained how to deduce a factorization of p-adic L-functions in the mixed sign case using rank-two Beilinson–Flach elements. In general, we are not able to rule out the possibility that $\vartheta_E^+ \vartheta_{E_K}^- + \vartheta_E^- \vartheta_{E_K}^+$ could be zero. If it does equal zero, Proposition 8.4 asserts that $\ker(\pi_{\mathrm{cyc}})$ belongs to the support of the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules $\mathrm{Sel}^{+-}(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ and $\mathrm{Sel}^{-+}(\mathbb{Q}, D_{\rho_{4,2}})^\vee$. However in the examples that we consider in Section 8.4, we can use the arguments given at the beginning of Section 8 to conclude that $\vartheta_E^+ \vartheta_{E_K}^- + \vartheta_E^- \vartheta_{E_K}^+$ is in fact nonzero. For these examples, we can conclude that the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules $\mathrm{Sel}^{+-}(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ and $\mathrm{Sel}^{-+}(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ are torsion.

8.4. Examples. The following data is computed in Sage [**59**] using Rob Pollack's algorithms. Here, $\lambda(\theta_{E_K}^+)$ and $\lambda(\theta_{E_K}^-)$ denote the Lambda invariants of $\theta_{E_K}^+$ and $\theta_{E_K}^-$ respectively. The μ-invariants for these p-adic L-functions turn out to equal zero.

Table 2. Examples.

E	K	p	$\lambda(\theta_{E_K}^+)$	Roots for $\theta_{E_K}^+$	$\lambda(\theta_{E_K}^-)$	Roots for $\theta_{E_K}^-$
32A	$\mathbb{Q}(\sqrt{-43})$	3	8	$(2:\frac{1}{2}), (6:\frac{1}{6})$	2	$(2:1)$
	$\mathbb{Q}(\sqrt{-107})$	3	2	$(2:1)$	6	$(2:\frac{1}{2}), (4:\frac{1}{4})$
	$\mathbb{Q}(\sqrt{-283})$	3	6	$(2:\frac{1}{2}), (4:\frac{1}{4})$	2	$(2:1)$
40A	$\mathbb{Q}(\sqrt{-331})$	3	6	$(2:\frac{1}{2}), (4:\frac{1}{4})$	2	$(2:1)$
56A	$\mathbb{Q}(\sqrt{-139})$	3	6	$(2:\frac{1}{2}), (4:\frac{1}{4})$	2	$(2:1)$
	$\mathbb{Q}(\sqrt{-487})$	3	6	$(2:\frac{1}{2}), (4:\frac{1}{4})$	2	$(2:1)$

Assume the validity of Conjectures 1.3 and 8.3. To ensure that Condition (8a) is satisfied for all the elliptic curves in Table 2, that is, θ_E^+ is a unit in the ring $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$, one can glean from Rob Pollack's tables on his website http://math.bu.edu/people/rpollack/Data/data.html that $\lambda(\theta_E^+) = \mu(\theta_E^+) = 0$.

To ensure that Condition (8b) is satisfied for all the elliptic curves in Table 2, that is, $\theta_{E_K}^+$ and $\theta_{E_K}^-$ have no common irreducible factor in the UFD $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$, it is sufficient to observe that the valuation of the roots of $\theta_{E_K}^+$ and $\theta_{E_K}^-$ are different. The entries $(r : s)$, under the columns for the roots of the p-adic L-functions, denote r roots with p-adic valuation s.

To ensure that Condition (8c) is satisfied for all the elliptic curves in Table 2, that is, $\theta_{E_K}^\pm$ are not units in the ring $\mathbb{Z}_p[[\Gamma_{\mathrm{cyc}}]]$, one can glean the following

inequality of Iwasawa invariants of the p-adic L-functions $\theta_{E_K}^+$ and $\theta_{E_K}^-$ in the ring $\mathbb{Z}_p[[\Gamma_{\text{cyc}}]]$ from Rob Pollack's tables:

$$\lambda(\theta_{E_K}^+) \neq 0, \quad \lambda(\theta_{E_K}^-) \neq 0.$$

We remark that the validity of conditions (8a) and (8b) is sufficient to assert Assumption GCD (one does not need Condition (8c)). For more evidence towards Assumption GCD, we refer the interested reader to Pollack's tables on his website http://math.bu.edu/people/rpollack/Data/data.html, and to use the heuristics provided by Problem 3.2 in the work of Kurihara and Pollack [28]. See also the examples in Section 3.3 of their work.

Without assuming the validity of the two-variable Iwasawa main conjectures (Conjecture 1.3), one can still use Pollack's algorithms and results of Kobayashi to obtain unconditional results towards the pseudonullity conjecture of Coates–Sujatha in this setup.

Note that we have natural surjections of $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-modules:

$$\text{Sel}^{++}(\mathbb{Q}, D_{\rho_{4,2}})^\vee \twoheadrightarrow \text{III}^1(\mathbb{Q}, D_{\rho_{4,2}})^\vee, \quad \text{Sel}^{+-}(\mathbb{Q}, D_{\rho_{4,2}})^\vee \twoheadrightarrow \text{III}^1(\mathbb{Q}, D_{\rho_{4,2}})^\vee. \tag{8.27}$$

Consider the elliptic curve $E = 32A$ and the corresponding quadratic twists in Table 2. These elliptic curves have CM by the imaginary quadratic field $\mathbb{Q}(\sqrt{-1})$. The one-variable Iwasawa main conjecture (Conjecture 8.3) is known due to the work of Pollack and Rubin [45] when the elliptic curve (with supersingular reduction at p) has CM. We have the following equality of divisors in $Z^1(\mathbb{Z}_p[[\Gamma_{\text{cyc}}]])$:

$$\text{Div}(\text{Sel}^+(\mathbb{Q}, D_{\rho_{2,1}})^\vee) = \text{Div}(\theta_E^+) = 0,$$
$$\text{Div}(\text{Sel}^+(\mathbb{Q}, D_{\rho_{2,1(\epsilon_K)}})^\vee) = \text{Div}(\theta_{E_K}^+),$$
$$\text{Div}(\text{Sel}^-(\mathbb{Q}, D_{\rho_{2,1(\epsilon_K)}})^\vee) = \text{Div}(\theta_{E_K}^-).$$

Using Proposition 8.4 along with the data in Table 2, we have

$$\text{Supp}_{\text{Ht}=1}(\text{Sel}^{++}(\mathbb{Q}, D_{\rho_{4,2}})^\vee) \bigcap \text{Supp}_{\text{Ht}=1}(\text{Sel}^{+-}(\mathbb{Q}, D_{\rho_{4,2}})^\vee) = \varnothing,$$

for the elliptic curve $E = 32A$, $p = 3$ and the corresponding imaginary quadratic fields in Table 2. Equation (8.27) now lets us conclude that the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\text{III}^1(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ is pseudonull in these examples.

We can also unconditionally assert that the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\text{III}^1(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ is pseudonull for the elliptic curves $E = 40A$ and $E = 56A$, $p = 3$ and the corresponding imaginary quadratic fields in Table 2. Let E equal either $40A$ or $56A$. We will first need to show that the 3-adic Galois representations

$\rho : G_{\mathbb{Q}} \to \text{GL}_2(\mathbb{Z}_3)$, given by the action of $G_{\mathbb{Q}}$ on the 3-adic Tate modules are surjective. The computations and arguments turn out to be similar for both the elliptic curves $40A$ and $56A$.

To show that ρ is surjective it suffices to show that the $\rho_9 : G_{\mathbb{Q}} \to \text{GL}_2(\mathbb{F}_9)$, given by the action of $G_{\mathbb{Q}}$ on the 9-division points, is surjective. This observation combines the fact that the determinant $\det(\rho) : G_{\mathbb{Q}} \to \mathbb{Z}_3^{\times}$ is surjective (since it coincides with the 3-adic cyclotomic character) and Exercise 1(b), Ch. IV, Section 3 from Serre's book [**49**] (so that $\text{Image}(\rho_9) \supset \text{SL}_2(\mathbb{F}_9)$).

We will first show that $\text{Gal}(\mathbb{Q}(E[9])/\mathbb{Q}) \overset{?}{=} \text{GL}_2(\mathbb{F}_9)$. One can perform computations on Sage to conclude that $\text{Gal}(\mathbb{Q}(E[3])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_3)$. Note that

$$|\text{GL}_2(\mathbb{F}_9)| = 2^4 * 3^5, \quad |\text{GL}_2(\mathbb{F}_3)| = 2^4 * 3.$$

To show that $\text{Gal}(\mathbb{Q}(E[9])/\mathbb{Q}) \overset{?}{=} \text{GL}_2(\mathbb{F}_9)$, it then suffices to show that 3^5 divides $[\mathbb{Q}(E[9]) : \mathbb{Q}]$.

Let $f(t)$ in $\mathbb{Q}[t]$ denote the polynomial corresponding to the 9-division points of E. One can use Sage and deduce that there exists an irreducible polynomial $f_{36}(t)$ in $\mathbb{Q}[t]$ of degree 36 dividing $f(t)$. Let α denote a root of $f_{36}(t)$. So, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 36$. Once again, one can use Sage to deduce that there exists an irreducible polynomial $g_{27}(t)$ in the polynomial ring $\mathbb{Q}(\alpha)[t]$ dividing $f_{36}(t)$. So, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 27$. Since $\mathbb{Q}(\alpha, \beta) \subset \mathbb{Q}(E[9])$, we have $2^2 * 3^5$ divides $[\mathbb{Q}(E[9]) : \mathbb{Q}]$. These observations let us conclude that $\text{Gal}(\mathbb{Q}(E[9])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_9)$.

$\mathbb{Q}(\mu_3)$ is the unique quadratic subfield of $\mathbb{Q}(E[9])$. This is because $\text{SL}_2(\mathbb{F}_3)$ is the unique subgroup of $\text{GL}_2(\mathbb{F}_3)$ with index 2. As a result, we have the following natural isomorphisms:

$$\text{Gal}(\mathbb{Q}(E[9])/\mathbb{Q}) \cong \text{Gal}(K(E[9])/K) \cong \text{Gal}(\mathbb{Q}(E_K[9])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_9).$$

These observations let us conclude that ρ is surjective for both E and E_K, when E equals either $40A$ and $56A$, p equals 3 and K is one of the corresponding imaginary quadratic fields in Table 2.

When the p-adic Galois representation $\rho : G_{\mathbb{Q}} \to \text{GL}_2(\mathbb{Z}_p)$, given by the action of $G_{\mathbb{Q}}$ on the p-adic Tate modules is surjective, Kobayashi [**27**, Theorem 4.1] has shown that we have the following inequality of divisors in $Z^1(\mathbb{Z}_p[[\Gamma_{\text{cyc}}]])$:

$$\text{Div}(\vartheta_E^{\pm}) \leqslant \text{Div}(\theta_E^{\pm}), \quad \text{Div}(\vartheta_{E_K}^{\pm}) \leqslant \text{Div}(\theta_{E_K}^{\pm}). \tag{8.28}$$

Using equation (8.28), Proposition 8.4 along with the data in Table 2, our observations let us conclude that

$$\text{Supp}_{\text{Ht}=1}(\text{Sel}^{++}(\mathbb{Q}, D_{\rho_{4,2}})^{\vee}) \bigcap \text{Supp}_{\text{Ht}=1}(\text{Sel}^{+-}(\mathbb{Q}, D_{\rho_{4,2}})^{\vee}) = \varnothing, \tag{8.29}$$

for the elliptic curves $E = 40A$ and $E = 56A$, $p = 3$ and the corresponding imaginary quadratic fields in Table 2. Equation (8.27) now lets us conclude that the $\mathbb{Z}_p[[\widetilde{\Gamma}]]$-module $\text{III}^1(\mathbb{Q}, D_{\rho_{4,2}})^\vee$ is pseudonull in these examples too.

Acknowledgements

References

[1] Y. Amice and J. Vélu, 'Distributions p-adiques associées aux séries de Hecke', *Astérisque* **24–25** (1975), 119–131.

[2] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra* (Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969).

[3] F. Bleher, T. Chinburg, R. Greenberg, M. Kakde, G. Pappas, R. Sharifi and M. Taylor, 'Higher Chern classes in Iwasawa theory', *Amer. J. Math.*, 2019, to appear, available at arXiv:1512.00273.

[4] W. Bruns and J. Herzog, *Cohen–Macaulay Rings*, Cambridge Studies in Advanced Mathematics, 39 (Cambridge University Press, Cambridge, 1993).

[5] K. Büyükboduk and A. Lei, 'Functional equation for p-adic Rankin–Selberg L-functions', *Ann. Math. Qué.*, 2019, to appear, available at doi:10.1007/s40316-019-00117-2.

[6] K. Büyükboduk and A. Lei, 'Iwasawa theory of elliptic modular forms over imaginary quadratic fields at non-ordinary primes', *Int. Math. Res. Not. IMRN*, 2019, to appear, available at arXiv:1605.05310.

[7] F. Castella, M. Çiperiani, C. Skinner and F. Sprung, 'On the Iwasawa main conjectures for modular forms at non-ordinary primes', Preprint, 2018, arXiv:1804.10993.

[8] F. Castella and X. Wan, 'Perrin-Riou's main conjecture for elliptic curves at supersingular primes', Preprint, 2018, arXiv:1607.02019.

[9] J. Coates and R. Greenberg, 'Kummer theory for abelian varieties over local fields', *Invent. Math.* **124**(1) (1996), 129–174.

[10] J. Coates and R. Sujatha, 'Fine Selmer groups of elliptic curves over p-adic Lie extensions', *Math. Ann.* **331**(4) (2005), 809–839.

[11] R. F. Coleman and B. Edixhoven, 'On the semi-simplicity of the U_p-operator on modular forms', *Math. Ann.* **310**(1) (1998), 119–127.

[12] C. Dion and A. Lei, 'Plus and minus logarithms and Amice transform', *C. R. Math. Acad. Sci. Paris* **355**(9) (2017), 942–948.

[13] B. Edixhoven, 'The weight in Serre's conjectures on modular forms', *Invent. Math.* **109**(3) (1992), 563–594.

[14] R. Greenberg, 'Iwasawa theory and p-adic deformations of motives', in *Motives (Seattle, WA, 1991)*, Proc. Sympos. Pure Math., 55 (American Mathematical Society, Providence, RI, 1994), 193–223.

[15] R. Greenberg, 'Iwasawa theory—past and present', in *Class Field Theory—its Centenary and Prospect (Tokyo, 1998)*, Adv. Stud. Pure Math., 30 (Mathematical Society of Japan, Tokyo, 2001), 335–385.

[16] R. Greenberg, 'On the structure of certain Galois cohomology groups', *Doc. Math.* **Extra Vol.** (2006), 335–391 (electronic).

[17] R. Greenberg, 'Surjectivity of the global-to-local map defining a Selmer group', *Kyoto J. Math.* **50**(4) (2010), 853–888.

[18] R. Greenberg, 'On the structure of Selmer groups', in *Elliptic Curves, Modular Forms and Iwasawa Theory: In Honour of John H. Coates' 70th Birthday, Cambridge, UK, March 2015* (Springer International Publishing, Switzerland, 2016), 225–252.

[19] R. Greenberg and G. Stevens, 'On the conjecture of Mazur, Tate, and Teitelbaum', in *p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture (Boston, MA, 1991)*, Contemp. Math., 165 (American Mathematical Society, Providence, RI, 1994), 183–211.

[20] R. Hartshorne, *Residues and Duality*, Lecture Notes in Mathematics, 20 (Springer, New York, 1966). Lecture notes of a seminar on the work of A. Grothendieck, given at Harvard 1963/64. With an appendix by P. Deligne.

[21] H. Hida, 'On p-adic L-functions of $GL(2) \times GL(2)$ over totally real fields', *Ann. Inst. Fourier (Grenoble)* **41**(2) (1991), 311–391.

[22] H. Hida, 'On the search of genuine p-adic modular L-functions for $GL(n)$', *Mém. Soc. Math. Fr. (N.S.)* (67) (1996), vi+110, With a correction to: 'On p-adic L-functions of $GL(2) \times GL(2)$ over totally real fields' [*Ann. Inst. Fourier (Grenoble)* **41**(2) (1991), 311–391].

[23] K. Iwasawa, 'On $\mathbf{Z}_l$-extensions of algebraic number fields', *Ann. of Math. (2)* **98** (1973), 246–326.

[24] U. Jannsen, 'Iwasawa modules up to isomorphism', in *Algebraic Number Theory*, Adv. Stud. Pure Math., 17 (Academic Press, Boston, MA, 1989), 171–207.

[25] U. Jannsen, 'A spectral sequence for Iwasawa adjoints', *Münster J. Math.* **7**(1) (2014), 135–148.

[26] B. D. Kim, 'Signed-Selmer groups over the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field', *Canad. J. Math.* **66**(4) (2014), 826–843.

[27] S. Kobayashi, 'Iwasawa theory for elliptic curves at supersingular primes', *Invent. Math.* **152**(1) (2003), 1–36.

[28] M. Kurihara and R. Pollack, 'Two p-adic L-functions and rational points on elliptic curves with supersingular reduction', in *L-functions and Galois Representations*, London Mathematical Society, Lecture Note Series, 320 (Cambridge University Press, Cambridge, 2007), 300–332.

[29] A. Lei, 'Factorisation of two-variable p-adic L-functions', *Canad. Math. Bull.* **57**(4) (2014), 845–852.

[30] A. Lei and B. Palvannan, 'Codimension two cycles in Iwasawa theory and tensor product of Hida families'. Preprint, 2019, arXiv:1901.09301.

[31] M. F. Lim, 'On the pseudo-nullity of the dual fine Selmer groups', *Int. J. Number Theory* **11**(7) (2015), 2055–2063.

[32] D. Loeffler, 'p-adic integration on ray class groups and non-ordinary p-adic L-functions', in *Iwasawa theory 2012*, Contrib. Math. Comput. Sci., 7 (Springer, Heidelberg, 2014), 357–378.

[33] D. Loeffler and S. L. Zerbes, 'Iwasawa theory and p-adic L-functions over $\mathbb{Z}_p^2$-extensions', *Int. J. Number Theory* **10**(8) (2014), 2045–2095.

[34] D. Loeffler and S. L. Zerbes, 'Rankin–Eisenstein classes in Coleman families', *Res. Math. Sci.* **3** (2016), Paper No. 29, 53.

[35] M. Longo and S. Vigni, 'Plus/minus Heegner points and Iwasawa theory of elliptic curves at supersingular primes', *Boll. Unione Mat. Ital.*, 2018, to appear, available at doi:10.1007/s40574-018-0162-4.

[36] H. Matsumura, *Commutative Ring Theory*, 2nd edn, Cambridge Studies in Advanced Mathematics, 8 (Cambridge University Press, Cambridge, 1989). Translated from the Japanese by M. Reid.

[37] J. Nekovář, 'Selmer complexes', *Astérisque* (310) (2006), viii+559.

[38] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, 2nd edn, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 323 (Springer, Berlin, 2008).

[39] Y. Ochi, 'A remark on the pseudo-nullity conjecture for fine Selmer groups of elliptic curves', *Comment. Math. Univ. St. Pauli* **58**(1) (2009), 1–7.

[40] B. Palvannan, 'On Selmer groups and factoring p-adic L-functions', *Int. Math. Res. Not. IMRN* **2018**(24) (2018), 7483–7554, 05.

[41] B. Palvannan, 'Height one specializations of selmer groups', *Ann. Inst. Fourier (Grenoble)* **69**(1) (2019), 303–334.

[42] B. Perrin-Riou, 'Théorie d'Iwasawa p-adique locale et globale', *Invent. Math.* **99**(2) (1990), 247–292.

[43] B. Perrin-Riou, 'Théorie d'Iwasawa des représentations p-adiques sur un corps local', *Invent. Math.* **115**(1) (1994), 81–161. With an appendix by Jean-Marc Fontaine.

[44] R. Pollack, 'On the p-adic L-function of a modular form at a supersingular prime', *Duke Math. J.* **118**(3) (2003), 523–558.

[45] R. Pollack and K. Rubin, 'The main conjecture for CM elliptic curves at supersingular primes', *Ann. of Math. (2)* **159**(1) (2004), 447–464.

[46] R. Pollack and G. Stevens, 'Overconvergent modular symbols and p-adic L-functions', *Ann. Sci. Éc. Norm. Supér. (4)* **44**(1) (2011), 1–42.

[47] K. Rubin, 'Elliptic curves and $\mathbf{Z}_p$-extensions', *Compos. Math.* **56**(2) (1985), 237–250.

[48] K. Rubin, 'Local units, elliptic units, Heegner points and elliptic curves', *Invent. Math.* **88**(2) (1987), 405–422.

[49] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves* (W. A. Benjamin, Inc., New York-Amsterdam, 1968). McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute.

[50] S. Shekhar, 'Comparing the corank of fine Selmer group and Selmer group of elliptic curves', *J. Ramanujan Math. Soc.* **33**(2) (2018), 205–217.

[51] G. Shimura, 'On the periods of modular forms', *Math. Ann.* **229**(3) (1977), 211–221.

[52] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106 (Springer, New York, 1986).

[53] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 151 (Springer, New York, 1994).

[54] C. Skinner and E. Urban, 'The Iwasawa main conjectures for GL_2', *Invent. Math.* **195**(1) (2014), 1–277.

[55] C. Skinner and W. Zhang, 'Indivisibility of Heegner points in the multiplicative case', Preprint, 2014, arXiv:1407.1099.

[56] F. Sprung, 'The Iwasawa Main Conjecture for elliptic curves at odd supersingular primes', Preprint, 2016, arXiv:1610.10017.

[57] G. Stevens, 'Rigid analytic modular symbols', Preprint, 1994.

[58] J. Tate, *Algorithm for Determining the Type of a Singular Fiber in an Elliptic Pencil*, Lecture Notes in Mathematics, 476 (Springer, Berlin, 1975), 33–52.

[59] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.2)*, 2016, http://www.sagemath.org.

[60] M. M. Višik, 'Nonarchimedean measures associated with Dirichlet series', *Mat. Sb. (N.S.)* **99**(141(2)) (1976), 248–260, 296.

[61] X. Wan, 'Iwasawa main conjecture for non-ordinary modular forms', Preprint, 2016, arXiv:1607.07729.

[62] X. Wan., 'Iwasawa main conjecture for supersingular elliptic curves', Preprint, 2016, arXiv:1411.6352v4.

[63] C. A. Weibel, *An Introduction to Homological Algebra*, Cambridge Studies in Advanced Mathematics, 38 (Cambridge University Press, Cambridge, 1994).