manuscripta math. 167, 589–612 (2022)

Jeffrey Hatley · Antonio Lei · Stefano Vigni

Λ-submodules of finite index of anticyclotomic plus and minus Selmer groups of elliptic curves

Received: 22 April 2020 / Accepted: 16 January 2021 /
Published online: 18 February 2021

Abstract. Let p be an odd prime and K an imaginary quadratic field where p splits. Under appropriate hypotheses, Bertolini showed that the Selmer group of a p-ordinary elliptic curve over the anticyclotomic $\mathbb{Z}_p$-extension of K does not admit any proper Λ-submodule of finite index, where Λ is a suitable Iwasawa algebra. We generalize this result to the plus and minus Selmer groups (in the sense of Kobayashi) of p-supersingular elliptic curves. In particular, in our setting the plus/minus Selmer groups have Λ-corank one, so they are not Λ-cotorsion. As an application of our main theorem, we prove results in the vein of Greenberg–Vatsal on Iwasawa invariants of p-congruent elliptic curves, extending to the supersingular case results for p-ordinary elliptic curves due to Hatley–Lei.

1. Introduction

When studying Selmer groups in the context of Iwasawa theory, it is often desirable to show that these Selmer groups have no proper Λ-submodules of finite index or, equivalently, that their Pontryagin duals have no nontrivial finite Λ-submodules, where Λ is an appropriate p-adic Iwasawa algebra for a prime number p (to fix ideas, in this introduction we can take Λ to be the $\mathbb{Z}_p$-algebra $\mathbb{Z}_p[\![X]\!]$ of formal power series over the p-adic integers $\mathbb{Z}_p$). For instance, a finitely generated Λ-module M (which, in our context, will always be the Pontryagin dual of a suitable Selmer group) admits a map

$$M \longrightarrow \Lambda^{\oplus r} \oplus \bigoplus_{i=1}^{s} \Lambda/(p^{a_i}) \oplus \bigoplus_{j=1}^{t} \Lambda\Big/\big(F_j^{n_j}\big)$$

The second named author's research is supported by the NSERC Discovery Grants Program RGPIN-2020-04259 and RGPAS-2020-00096 (Grant No. 05710). The third named author's research is partially supported by PRIN 2017 "Geometric, algebraic and analytic methods in arithmetic"

J. Hatley (✉): Department of Mathematics, Union College, Bailey Hall 202, Schenectady, NY 12308, USA e-mail: hatleyj@union.edu

A. Lei: Département de mathématiques et de statistique, Pavillon Alexandre-Vachon, Université Laval, Quebec, QC G1V 0A6, Canada e-mail: antonio.lei@mat.ulaval.ca

S. Vigni: Dipartimento di Matematica, Università di Genova, Via Dodecaneso 35, 16146 Genova, Italy e-mail: vigni@dima.unige.it

Mathematics Subject Classification: Primary 11R23; Secondary 11G05 · 11R20

https://doi.org/10.1007/s00229-021-01283-w

with finite kernel and cokernel, for integers $r, s, t \geq 0$, $a_i, n_j \geq 1$ and irreducible Weierstrass polynomials $F_j \in \mathbb{Z}_p[X]$. If M has no nontrivial finite Λ-submodules, then this map is in fact injective.

Such non-existence theorems have played a crucial role in certain strategies for proving cases of the Iwasawa Main Conjecture, as in [10,14,21], and by now they have been studied in great generality (see, e.g., [13]), although many specific cases of interest remain open to inquiry.

In [2] and [3], Bertolini approached this question for the Selmer groups attached to rational elliptic curves with good ordinary reduction at a prime p along the anticylotomic $\mathbb{Z}_p$-extension of a suitable imaginary quadratic field K, which is the unique $\mathbb{Z}_p$-extension of K that is Galois and non-abelian over $\mathbb{Q}$.

The splitting behavior in K of p and of the prime factors of the conductor N of E exerts a tremendous influence on the structure of the Selmer groups that one can attach to E and K_∞. In particular, when N is divisible by an odd number of primes that are inert in K the situation is remarkably similar to the cyclotomic (over $\mathbb{Q}$ or over K) setting. When the number of such primes is even, however, the sign of the functional equation for the relevant L-function is -1, which forces the Selmer groups to grow and thus become more complicated (see, e.g., [2] and [27]).

Another situation in which the Iwawawa theory for elliptic curves is more delicate is when E has good supersingular reduction at p. In this case, even in the cyclotomic setting over $\mathbb{Q}$ the usual Selmer groups fail to satisfy a control theorem as in [29], so the Selmer group over the full cyclotomic extension is unable to provide bounds on Selmer coranks at finite layers of the cyclotomic tower. Thus, for supersingular primes, it becomes necessary to consider special restricted plus/minus Selmer groups that turn out to be more amenable to classical arguments. This general program was first proposed and carried out over $\mathbb{Q}$ by Kobayashi in [25] and has admitted since then many generalizations such as [18] and [22]. It is worth remarking that the p-adic analytic counterpart of Kobayashi's theory was provided by Pollack in [33].

In this paper we take up the task of generalizing Bertolini's results in [3] to the case of elliptic curves with good supersingular reduction at p. Thus, we consider the complications that arise both from having supersingular reduction and from working over the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field satisfying the Heegner hypothesis with respect to the conductor of our elliptic curve.

1.1. Setup and notation

Throughout this article, p will denote an odd prime number. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N with good supersingular reduction at p and $a_p(E) = 0$, where $a_p(E)$ is the p-th Fourier coefficient of the weight 2 newform attached to E by modularity.

Let K be an imaginary quadratic field such that all the primes dividing pN split in K (in particular, K satisfies the *Heegner hypothesis* relative to N), write $\mathcal{O}_K$ for the ring of integers of K and let

$$p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^c$$

be the factorization of p as a product of (distinct) maximal ideals of $\mathcal{O}_K$ (here c denotes the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$). Fix algebraic closures $\bar{\mathbb{Q}}$ and $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}$ and $\mathbb{Q}_p$, respectively, write $\mathbb{C}_p$ for the completion of $\bar{\mathbb{Q}}_p$, choose an embedding $\iota_p : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ and suppose that $\mathfrak{p}$ is the prime above p that lands inside the valuation ideal of $\mathbb{C}_p$. Let T denote the p-adic Tate module of E, set $V := T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $A := V/T = E[p^\infty]$. For every integer $m \geq 1$, define $A_m := T/p^m T = E[p^m]$. Moreover, let $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$.

Let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K, whose n-th finite layer will be denoted by K_n, and let Λ be the associated Iwasawa algebra. We assume that the two primes of K above p are totally ramified in K_∞; this is a natural condition to require when working in the supersingular setting (cf., e.g., [9, Assumptions 1.7, (2)], [18, Hypothesis (S)], [34, Theorem 1.2, (2)]) and holds if p does not divide the class number of K. We shall denote the unique primes (of the finite layers) of K_∞ above $\mathfrak{p}$ and $\mathfrak{p}^c$ by the same symbols. For more details, see Sect. 2.

Finally, for any compact or discrete Λ-module M we write $M^\vee := \mathrm{Hom}^{\mathrm{cont}}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ for its Pontryagin dual, which may be equipped with the compact-open topology (here $\mathrm{Hom}^{\mathrm{cont}}_{\mathbb{Z}_p}(\bullet, \star)$ denotes continuous homomorphisms of $\mathbb{Z}_p$-modules and $\mathbb{Q}_p/\mathbb{Z}_p$ is equipped with the quotient, i.e., discrete, topology).

1.2. Important hypotheses

In this section, we collect some of the hypotheses that we will impose at various points throughout the paper. We assign labels to these hypotheses for easy recall. Some of the notation appearing in these hypotheses has not been introduced yet; we indicate where this notation is defined, as well as the first time each hypotheses is invoked.

(Heeg) Every prime number dividing Np splits in the imaginary quadratic field K, where the integer N is understood from context to be the conductor of some elliptic curve over $\mathbb{Q}$ with good supersingular reduction at p.

- This setup already appeared in 1.1, and it is assumed throughout the entirety of this paper (for various values of N).

(Tam) Given an elliptic curve $E/\mathbb{Q}$, the prime p does not divide $\#\big(E/E^0\big)$.

- This condition ensures that none of the local Tamagawa factors of E are divisible by p. This assumption is necessary in order to obtain an isomorphism in Proposition 3.9 rather than an injection with bounded cokernel; see, e.g., [11, Lemma 3.3] and the discussion that immediately follows it.

(Norm) For an elliptic curve $E/\mathbb{Q}$ satisfying **(Tam)**, the local norm maps $E(K_{n,v}) \to E(K_v)$ are surjective for all $n \geq 1$ and all primes of K that do not divide p.

- This assumption is introduced in 5.1 in order to generalize some cohomological lemmas from [4], where the surjectivity of the local norm maps at primes

above p is also required (see [4, Assumption 2.15]). However, this additional assumption guarantees that E is p-ordinary, which is not within the scope of the present paper.

(mod p) For an elliptic curve $E/\mathbb{Q}$ satisfying both $a_p(E) = 0$ and **(Norm)**, we have $\mathfrak{E}_n^{\pm} \neq 0$ and $Ш_p^{\pm}(E, K_{n+1}/K_n) = 0$ for all $n \in \mathbb{N}$.

- The notation $\mathfrak{E}_n^{\pm}$ (which conceals the fact that it depends on E) is defined in 4.2, while $Ш_p^{\pm}(E, K_{n+1}/K_n)$ is defined in 5.3. This hypothesis first appears in the statement of Theorem 5.15.

(Cong) Given two elliptic curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$, both of which satisfy **(mod p)**, there is an isomorphism $E_1[p] \simeq E_2[p]$ as $G_{\mathbb{Q}}$-modules.

- For pairs of elliptic curves satisfying this assumption, we will be able to compare the Iwasawa invariants of their plus/minus Selmer groups in 6.

We emphasize that assumption **(Heeg)** is always in effect and the other assumptions have a cumulative nature:

$$\textbf{(Cong)} \Rightarrow \textbf{(mod } p\textbf{)} \Rightarrow \textbf{(Norm)} \Rightarrow \textbf{(Tam)}.$$

1.3. Main results

For every $n \in \mathbb{N}$ we define plus and minus Mordell–Weil groups $E^{\pm}(K_n)$, which provide the local conditions in terms of which we introduce our plus and minus Selmer groups $\mathrm{Sel}_{p^\infty}^{\pm}(E/K_\infty)$ *à la* Kobayashi. It is worth remarking that our construction is inspired by Kim ([21]); in particular, we define plus/minus Selmer groups over the finite layers of K_∞/K somewhat differently from most of the literature (see, e.g., [8,9,18], [27]). This construction has the advantage of yielding a nicer control theorem and also some important duality properties that may be of independent interest.

Our main result, which corresponds to Theorem 5.15, can be stated as follows.

Theorem 1.1. *If **(Heeg)** and **(mod** p**)** hold, then the* Λ*-module* $\mathrm{Sel}_{p^\infty}^{\pm}(E/K_\infty)$ *has no proper* Λ*-submodule of finite index.*

As a sample application of this result, we are able to prove a theorem regarding the variation of Iwasawa invariants among *p-congruent* rational elliptic curves, that is, rational elliptic curves with Galois-isomorphic p-torsion subgroups.

Theorem 1.2. *Assume **(Heeg)** holds and let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ be elliptic curves satisfying **(Cong)**. Then*

$$\mu\big(\mathrm{Sel}_{p^\infty}^{\pm}(E_1/K_\infty)^\vee\big) = 0 \iff \mu\big(\mathrm{Sel}_{p^\infty}^{\pm}(E_2/K_\infty)^\vee\big) = 0.$$

Furthermore, if these μ-invariants vanish, then the λ-invariants of the Pontryagin duals of these Selmer groups are related by an explicit formula.

This result is in the vein of work by Greenberg–Vatsal ([14]) and extends to the supersingular setting results of Hatley–Lei in the p-ordinary case ([16,17]). The reader is referred to the introduction to Sect. 6 for the definitions of μ- and λ-invariants, and to Theorem 6.3 for the full statement.

Remark 1.3. Our arguments for obtaining these results have some significant differences from the strategy developed by Greenberg in [11], which has been generalized to many different settings (see, e.g., [15,16,20,22,24,35,37]). In [12], Greenberg showed that his strategy works for very general Selmer groups that can be defined by a surjective global-to-local map in cohomology. In the setting studied in this paper, the plus and minus Selmer groups cannot be defined in this way, since they fail Greenberg's so-called CRK hypothesis. On the other hand, both strategies utilize non-primitive Selmer groups, and the influence of Greenberg's approach is amply evident in our own.

1.4. Future directions

The original motivation for [3] was to strengthen some of the results from [2]. It would be interesting to study generalizations of results in [2] in the supersingular setting. For example, on adapting Bertolini's strategy in [3] to our plus/minus case, we have imposed a technical hypothesis on the vanishing of certain relative Shafarevich–Tate groups of E along finite layers of K_∞/K, denoted by $Ш^{\pm}_{p^m}(E, K_{n+1}/K_n)$ (see Lemma 5.12 for more details). It would be worthwhile to investigate this assumption further, e.g., to find sufficient conditions and give explicit examples.

The results of this paper should also have implications for the annihilators of anticyclotomic plus/minus Selmer groups, in the spirit of [1]; we plan to tackle this question in a future project.

Finally, the first two named authors recently generalized Bertolini's results to the case of p-ordinary modular forms of higher weight [17]; it would be interesting to make a similar study of non-ordinary modular forms.

2. Anticyclotomic Iwasawa algebras

2.1. The anticyclotomic $\mathbb{Z}_p$-extension of K

For every $m \in \mathbb{N}$ let H_{p^m} denote the ring class field of K of conductor p^m, then set $H_{p^\infty} := \cup_{m\in\mathbb{N}} H_{p^m}$. There is an isomorphism

$$\mathrm{Gal}(H_{p^\infty}/K) \simeq \mathbb{Z}_p \times \Delta,$$

where Δ is a finite group. The *anticyclotomic $\mathbb{Z}_p$-extension* K_∞/K is the unique $\mathbb{Z}_p$-extension of K contained in H_{p^∞}. It can be characterized as the unique $\mathbb{Z}_p$-extension of K that is Galois and non-abelian (in fact, generalized dihedral) over

$\mathbb{Q}$. We can write $K_\infty := \cup_{m\geq 0} K_n$, where K_n is the unique subfield of K_∞ such that

$$G_n := \mathrm{Gal}(K_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

In particular, $K_0 = K$. We also define

$$G_\infty := \varprojlim_m G_m = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p,$$

where the inverse limit is taken with respect to the natural restriction maps. Finally, for all $n, n' \in \mathbb{N} \cup \{\infty\}$ with $n \leq n'$ we set

$$\mathcal{G}_{n'/n} := \mathrm{Gal}(K_{n'}/K_n).$$

In particular, $\mathcal{G}_{n/0} = G_n$ for all $n \in \mathbb{N}$.

2.2. The Iwasawa algebra Λ

Throughout our article, we fix a topological generator γ_∞ of G_∞. Furthermore, we consider the Iwasawa algebra

$$\Lambda := \varprojlim_n \mathbb{Z}_p[G_n] = \mathbb{Z}_p[\![G_\infty]\!]$$

attached to K_∞/K, the inverse limit being taken with respect to the maps that are induced by restriction. As is well known (see, e.g., [31, Proposition 5.3.5]), γ_∞ determines an isomorphism of topological $\mathbb{Z}_p$-algebras $\Lambda \xrightarrow{\simeq} \mathbb{Z}_p[\![X]\!]$ such that $\gamma_\infty \mapsto 1 + X$. In the rest of the paper, we shall tacitly identify Λ with $\mathbb{Z}_p[\![X]\!]$ in this way.

3. Selmer groups and control theorems

3.1. Plus and minus Selmer groups over K_∞

We introduce plus and minus norm groups *à la* Kobayashi (see [25]). First of all, define the two sets of indices

$$S_n^+ := \{0, 1, \ldots, n\} \cap 2\mathbb{Z};$$
$$S_n^- := \{0, 1, \ldots, n\} \cap (2\mathbb{Z} + 1).$$

Let $n \geq 1$ be an integer. For $v \in \{\mathfrak{p}, \mathfrak{p}^c\}$, set

$$\hat{E}^\pm(K_{n,v}) := \left\{ P \in \hat{E}(\mathfrak{M}_{K_{n,v}}) \;\middle|\; \mathrm{Tr}_{n/m+1}(P) \in \hat{E}(\mathfrak{M}_{K_{m,v}}) \text{ for all } m \in S_n^\pm \right\},$$

where we write $\hat{E}(\mathfrak{M}_{K_{n,v}})$ for the formal group of E whose points are defined over the maximal ideal $\mathfrak{M}_{K_{n,v}}$ of the valuation ring of $K_{n,v}$ and

$$\mathrm{Tr}_{n/m+1} : \hat{E}(\mathfrak{M}_{K_{n,v}}) \longrightarrow \hat{E}(\mathfrak{M}_{K_{m+1,v}})$$

is the trace map on formal groups.

Let $v \in \{\mathfrak{p}, \mathfrak{p}^c\}$. Following [21, 3.3], we define

$$\mathbb{H}_v^{\pm} := \bigcup_{n \geq 0} \hat{E}^{\pm}(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p. \tag{3.1}$$

For $n \in \mathbb{N}$, we also set

$$\mathbb{H}_{n,v}^{\pm} := \left(\mathbb{H}_v^{\pm}\right)^{\mathrm{Gal}(K_{\infty,v}/K_{n,v})}.$$

Remark 3.1. Using the Kummer map and the fact (shown in the proof of Lemma 3.8 below) that the natural maps

$$H^1(K_n, E[p^\infty]) \to H^1(K_{\infty,v}, E[p^\infty])^{\mathcal{G}_{\infty/n}}$$

and

$$H^1(K_{n,v}, E[p^m]) \to H^1(K_{n,v}, E[p^\infty])[p^m]$$

are isomorphisms, we may identify $\mathbb{H}_v^{\pm}$ as a Λ-submodule of $H^1(K_{\infty,v}, A) := \varinjlim_n H^1(K_{n,v}, A)$. In turn, we may identify $\mathbb{H}_{n,v}^{\pm}$ and $\mathbb{H}_{n,v}^{\pm}[p^m]$ as submodules of $H^1(K_{n,v}, A)$ and $H^1(K_{n,v}, A_m)$, respectively.

In line with our general notational conventions, let $(\mathbb{H}_v^{\pm})^\vee$ be the Pontryagin dual of $\mathbb{H}_v^{\pm}$.

Proposition 3.2. *(a) The Λ-module $(\mathbb{H}_v^{\pm})^\vee$ is free of rank one.*
(b) Let $m, n \in \mathbb{N}$. Under the local Tate pairing

$$H^1(K_{n,v}, A_m) \times H^1(K_{n,v}, A_m) \longrightarrow \mathbb{Z}/p^m\mathbb{Z},$$

the exact annihilator of $\mathbb{H}_{n,v}^{\pm}[p^m]$ is $\mathbb{H}_{n,v}^{\pm}[p^m]$.

Proof. Part (a) is [21, Proposition 3.13] when the sign is $-$. This has been subsequently generalized to the $+$ case in [23, Proposition 2.11], as our ground field is $\mathbb{Q}_p$. Part (b) then follows from the proof of [21, Proposition 3.15]. □

Now we define Selmer groups for E over K_∞ and over the finite layers of K_∞/K. First of all, for every $n \in \mathbb{N}$ let S_n be the set of places of K_n dividing $Np\infty$, let K_{n,S_n} be the maximal extension of K_n unramified outside S_n and write $H^1_{S_n}(K_n, \star)$ as a shorthand for $H^1(K_{n,S_n}/K_n, \star)$. In the following, it is convenient to set also $A_\infty := A = E[p^\infty]$.

Definition 3.3. Let $m \in \mathbb{N} \cup \{\infty\}$ and $n \in \mathbb{N}$. The *p^m-Selmer group of E over K_n* is

$$\mathrm{Sel}_{p^m}(E/K_n) := \ker\left(H^1_{S_n}(K_n, A_m) \longrightarrow \prod_{v \in S_n} \frac{H^1(K_{n,v}, A_m)}{E(K_{n,v})/p^m}\right).$$

The *p^m-Selmer group of E over K_∞* is

$$\mathrm{Sel}_{p^m}(E/K_\infty) := \varinjlim_n \mathrm{Sel}_{p^m}(E/K_n),$$

the direct limit being taken with respect to the restriction maps.

We also introduce plus/minus Selmer groups *à la* Kobayashi, along the lines of [21].

Definition 3.4. Let $m \in \mathbb{N} \cup \{\infty\}$ and $n \in \mathbb{N}$. The *plus/minus Selmer groups of E over K_n* are

$$\mathrm{Sel}_{p^m}^{\pm}(E/K_n) := \ker\left(H^1_{S_n}(K_n, A_m) \longrightarrow \prod_{v \in S_n, v \nmid p} \frac{H^1(K_{n,v}, A_m)}{E(K_{n,v})/p^m} \times \prod_{v \mid p} \frac{H^1(K_{n,v}, A_m)}{\mathbb{H}^{\pm}_{n,v}[p^m]} \right).$$

The *plus/minus Selmer groups of E over K_∞* are

$$\mathrm{Sel}_{p^m}^{\pm}(E/K_\infty) := \varinjlim_n \mathrm{Sel}_{p^m}^{\pm}(E/K_n),$$

the direct limit being taken with respect to the restriction maps.

Remark 3.5. Our definitions are different from those in [18] and [25], unless the base field is $K_0 = K$ or K_∞. We have followed [21, 4.4] because we would like our Selmer conditions at p to satisfy part (b) of Proposition 3.2 for our applications later.

Remark 3.6. If $m = 1$, then we omit the superscript and simply write, e.g., $\mathrm{Sel}_p^{\pm}(E/K_n)$.

The next result deals with the $n = 0$ case.

Lemma 3.7. *For all $m \in \mathbb{N} \cup \{\infty\}$, there is an equality*

$$\mathrm{Sel}_{p^m}^{\pm}(E/K) = \mathrm{Sel}_{p^m}(E/K).$$

Proof. In light of Remark 3.1, it suffices to show that $\mathbb{H}^{\pm}_{0,v}[p^m]$ coincides with the image of $E(K_v)/p^m E(K_v)$ in $H^1(K_v, A_m)$ under the Kummer map. Indeed, $\mathbb{H}^{\pm}_{0,v}[p^m]$, $E(K_v)/p^m E(K_v)$ and $H^1(K_v, A_m)\big/\big(E(K_v)/p^m E(K_v)\big)$ are all free of rank one over $\mathbb{Z}/p^m\mathbb{Z}$. On the other hand, $E(K_v)/p^m E(K_v)$ is contained in $\mathbb{H}^{\pm}_{0,v}[p^m]$, as explained in the proof of [21, Proposition 3.15], and the result follows. □

3.2. Control theorems

Our goal is to prove a control theorem for the plus and minus Selmer groups in our context (Proposition 3.9) generalizing the corresponding result in the ordinary case (see, e.g., [2, 2.3]).

Lemma 3.8. *Let $v \in \{\mathfrak{p}, \mathfrak{p}^c\}$ and $m, n, n' \in \mathbb{N} \cup \{\infty\}$ with $n \leq n'$. The natural maps*

$$\frac{H^1(K_{n,v}, A_m)}{\mathbb{H}^{\pm}_{n,v}[p^m]} \longrightarrow \frac{H^1(K_{n',v}, A_m)}{\mathbb{H}^{\pm}_{n',v}[p^m]}, \qquad \frac{H^1(K_{n,v}, A_m)}{\mathbb{H}^{\pm}_{n,v}[p^m]} \longrightarrow \frac{H^1(K_{n,v}, A)}{\mathbb{H}^{\pm}_{n,v}} \tag{3.2}$$

are injective.

Proof. Since E has supersingular reduction at p, $H^0(K_{n',v}, A_m) = 0$ by the proof of [25, Proposition 7] (see also [18, Lemma 4.6]). The inflation-restriction exact sequence gives an isomorphism

$$\mathrm{res} : H^1(K_{n,v}, A_m) \xrightarrow{\simeq} H^1(K_{n',v}, A_m)^{\mathcal{G}_{n'/n}}. \tag{3.3}$$

In particular, it gives an injection $H^1(K_{n,v}, A_m) \hookrightarrow H^1(K_{n',v}, A_m)$. To show that the first map in (3.2) is injective, it is enough to show that

$$\mathbb{H}^{\pm}_{n,v}[p^m] = \mathbb{H}^{\pm}_{n',v}[p^m]^{\mathcal{G}_{n'/n}}. \tag{3.4}$$

But Proposition 3.2(a) tells us that there is an isomorphism of Λ-modules

$$\mathbb{H}^{\pm}_{n,v}[p^m] \simeq (\mathbb{Z}/p^m\mathbb{Z})[G_n]^{\vee},$$

and similarly for n'. Thus (3.4) holds.

Now we study the second map in (3.2). Consider the short exact sequence

$$0 \longrightarrow A_m \longrightarrow A \xrightarrow{p^m \cdot} A \longrightarrow 0.$$

The fact that $H^0(K_{n,v}, A) = 0$ implies that

$$H^1(K_{n,v}, A_m) = H^1(K_{n,v}, A)[p^m], \tag{3.5}$$

which gives the second injection. □

We are now in a position to prove a strong control theorem for our plus/minus Selmer groups. In order to obtain an isomorphism (rather than an injection with bounded cokernel) we need the following hypothesis.

(Tam) Given an elliptic curve $E/\mathbb{Q}$, the prime p does not divide $\#\big(E/E^0\big)$.

Proposition 3.9. *Let $E/\mathbb{Q}$ be an elliptic curve satisfying **(Tam)**. Let $m, m', n, n' \in \mathbb{N} \cup \{\infty\}$ with $m \leq m'$ and $n \leq n'$. The restriction map induces an isomorphism of Λ-modules*

$$\mathrm{Sel}^{\pm}_{p^m}(E/K_n) \simeq \mathrm{Sel}^{\pm}_{p^{m'}}(E/K_{n'})[p^m]^{\mathcal{G}_{n'/n}}.$$

Proof. Consider the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}^{\pm}_{p^m}(E/K_{n'}) & \longrightarrow & H^1_{S_{n'}}(K_{n'}, A_m) & \longrightarrow & \prod_{v\in S_{n'}} \frac{H^1(K_{n',v}, A_m)}{\mathbb{H}^{\pm}_{n',v}[p^m]} \\
 & & \downarrow & & \downarrow & & \downarrow \delta^{\pm}_v \\
0 & \longrightarrow & \mathrm{Sel}^{\pm}_{p^{m'}}(E/K_{n'})[p^m] & \longrightarrow & H^1_{S_{n'}}(K_{n'}, A_{m'})[p^m] & \longrightarrow & \left(\prod_{v\in S_{n'}} \frac{H^1(K_{n',v}, A_{m'})}{\mathbb{H}^{\pm}_{n',v}[p^{m'}]}\right)[p^m],
\end{array}$$

where we have written $\mathbb{H}^{\pm}_{n',v}[p^m]$ and $\mathbb{H}^{\pm}_{n',v}[p^{m'}]$ for $E(K_{n',v})/p^m$ and $E(K_{n',v})/p^{m'}$ respectively when $v \nmid p$. The middle map is induced by taking cohomology of the short exact sequence

$$0 \longrightarrow A_m \longrightarrow A_{m'} \xrightarrow{p^m \cdot} A_{m'-m} \longrightarrow 0.$$

As in the proof of Lemma 3.8, we have $H^0(K_{n'}, A_{m'-m}) = 0$. In particular, the middle vertical map is an isomorphism. When $v|p$, Lemma 3.8 says that $\delta^{\pm}_v$ is injective. When $v \nmid p$, the local condition for the plus/minus Selmer group is the same as that for the "full" Selmer group, so the injectivity follows from [2, 2.3, Lemma 1, (1)]. The snake lemma then shows that the first vertical map is an isomorphism as claimed.

Now, consider the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}^{\pm}_{p^m}(E/K_n) & \longrightarrow & H^1_{S_n}(K_n, A_m) & \longrightarrow & \prod_{v\in S_n} \frac{H^1(K_{n,v}, A_m)}{\mathbb{H}^{\pm}_{n,v}[p^m]} \\
 & & \downarrow & & \downarrow & & \downarrow \gamma^{\pm}_v \\
0 & \longrightarrow & \mathrm{Sel}^{\pm}_{p^m}(E/K_{n'})^{\mathcal{G}_{n'/n}} & \longrightarrow & H^1_{S_{n'}}(K_{n'}, A_m)^{\mathcal{G}_{n'/n}} & \longrightarrow & \left(\prod_{v\in S_{n'}} \frac{H^1(K_{n',v}, A_m)}{\mathbb{H}^{\pm}_{n',v}[p^m]}\right)^{\mathcal{G}_{n'/n}},
\end{array}$$

where we have written $\mathbb{H}^{\pm}_{n,v}[p^m]$ and $\mathbb{H}^{\pm}_{n',v}[p^m]$ for $E(K_{n,v})/p^m$ and $E(K_{n',v})/p^m$ respectively when $v \nmid p$. As before, $H^0(K_{n'}, A_m) = 0$. Thus, the inflation-restriction exact sequence says that the middle map is an isomorphism. When $v|p$, Lemma 3.8 says that $\gamma^{\pm}_v$ is injective. For $v \nmid p$, it is well-known (see e.g. [11, Lemma 3.3] and the discussion immediately following it) that the kernel of $\gamma^{\pm}_v$ is trivial under hypothesis **(Tam)**. We conclude once again by the snake lemma. □

4. Plus and minus Heegner points

4.1. Plus/minus Mordell–Weil groups

Let $n \geq 1$ be an integer. We define plus and minus norm subgroups of $E(K_n)$ that are global counterparts of the plus/minus norm groups introduced in 3.1. For all $m \in S^{\pm}_n$ with $m < n$, let

$$\mathrm{Tr}_{n/m+1} : E(K_n) \longrightarrow E(K_{m+1})$$

be the Galois trace map with respect to the group law on E.

Definition 4.1. The *plus/minus Mordell–Weil groups* of E over K_n are

$$E^{\pm}(K_n) := \left\{ P \in E(K_n) \mid \mathrm{Tr}_{n/m+1}(P) \in E(K_m) \text{for all} m \in S_n^{\pm} \text{with} m < n \right\}.$$

Similar to (3.1), we also define

$$\mathbb{H}_{\infty}^{\pm} := \bigcup_{n \geq 0} E^{\pm}(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p, \qquad \mathbb{H}_n^{\pm} := \left(\mathbb{H}_{\infty}^{\pm}\right)^{\mathrm{Gal}(K_{\infty}/K_n)}.$$

Remark 4.2. The Λ-module $\mathbb{H}_{\infty}^{\pm}$ (respectively, $\mathbb{H}_n^{\pm}$) may be identified with a submodule of $\mathrm{Sel}_{p^{\infty}}^{\pm}(E/K_{\infty})$ (respectively, $\mathrm{Sel}_{p^{\infty}}^{\pm}(E/K_n)$) via the usual Kummer map in Galois cohomology. Analogously, given an integer $m \geq 1$, we may view $\mathbb{H}_n^{\pm}[p^m]$ as a Λ-submodule of $\mathrm{Sel}_{p^m}^{\pm}(E/K_n)$.

4.2. Plus/minus Heegner points

Let $\left\{z_n \in E(K_n)\right\}_{n \geq 1}$ be a compatible family of Heegner points as in [27, 4.2]. Following [27, 4.3], we give

Definition 4.3. The *plus/minus Heegner points* are

$$z^+{}_n := \begin{cases} z_n & \text{if } n \text{ is even,} \\ z_{n-1} & \text{if } n \text{ is odd,} \end{cases} \qquad z^-{}_n := \begin{cases} z_{n-1} & \text{if } n \text{ is even,} \\ z_n & \text{if } n \text{ is odd.} \end{cases}$$

Since we have assumed that $a_p(E) = 0$, it is a consequence of the formulas in [32, 3.1, Proposition 1] that the points $z_m^{\pm}$ satisfy the following relations:

(a) $\mathrm{tr}_{K_m/K_{m-1}}(z_m^+) = -z_{m-1}^+$ for every even $m \geq 2$;
(b) $\mathrm{tr}_{K_m/K_{m-1}}(z_m^+) = pz_{m-1}^+$ for every odd $m \geq 1$;
(c) $\mathrm{tr}_{K_m/K_{m-1}}(z_m^-) = pz_{m-1}^-$ for every even $m \geq 2$;
(d) $\mathrm{tr}_{K_m/K_{m-1}}(z_m^-) = -z_{m-1}^-$ for every odd $m \geq 3$;
(e) $\mathrm{tr}_{K_1/K_0}(z_1^-) = \frac{p-1}{2} z_0^- = \frac{p-1}{2} z_0$.

In particular, we see that $z_m^{\pm} \in E^{\pm}(K_m)$.

For all $m, n \in \mathbb{N}$, set $R_{m,n} := (\mathbb{Z}/p^m\mathbb{Z})[G_n]$. As in [27, 4.4], we define $\mathcal{E}_{m,n}^{\pm}$ to be the $R_{m,n}$-submodule of $\mathrm{Sel}_{p^m}^{\pm}(E/K_n)$ generated by $z_n^{\pm}$. This in turn defines Λ-submodules

$$\mathcal{E}_{\infty}^{\pm} := \varinjlim_m \mathcal{E}_{m,m}^{\pm} \subset \mathrm{Sel}_{p^{\infty}}^{\pm}(E/K_{\infty})$$

as well as the Pontryagin duals

$$\mathcal{H}_{\infty}^{\pm} := (\mathcal{E}_{\infty}^{\pm})^{\vee} = \varprojlim_m (\mathcal{E}_{m,m}^{\pm})^{\vee}.$$

Finally, we introduce the $R_{m,n}$-module

$$\mathfrak{E}_{m,n}^{\pm} := (\mathcal{E}_{\infty}^{\pm})^{\mathrm{Gal}(K_{\infty}/K_n)}[p^m].$$

When $m = 1$, we shall omit the index m from the notation and simply write R_n, $\mathcal{E}_n^{\pm}$, $\mathfrak{E}_n^{\pm}$.

We recall the following result on $\mathcal{H}_{\infty}^{\pm}$.

Proposition 4.4. *The Λ-module $\mathcal{H}_\infty^\pm$ is finitely generated, torsion-free and of rank one.*

Proof. This is [27, Proposition 4.7]. □

We strengthen this slightly in the following proposition.

Proposition 4.5. *The Λ-module $\mathcal{H}_\infty^\pm$ is free of rank one.*

Proof. By definition, $\mathcal{E}_{m,m}^\pm$ is a cyclic $R_{m,m}$-module. Thus, $\varprojlim(\mathcal{E}_{m,m}^\pm)^\vee$ is a cyclic $\varprojlim R_{m,m}$-module. Thus, $\mathcal{H}_\infty^\pm$ is cyclic over Λ. Since it is also torsion-free, and since Λ is an integral domain, this implies $\mathcal{H}_\infty^\pm$ is free of rank 1. □

We deduce

Corollary 4.6. *The R_n-module $\mathfrak{E}_n^\pm$ is cyclic.*

Proof. Immediate from Proposition 4.5. □

Lemma 4.7. *There is an injection of R_n-modules*

$$\mathfrak{E}_{m,n}^\pm \hookrightarrow \mathrm{Sel}_{p^m}^\pm(E/K_n).$$

Proof. We may identify $\mathfrak{E}_{m,n}^\pm$ with a submodule of $H^1(K_n, A_m)$ via the Kummer map. On the other hand, the inclusion $\mathcal{E}_\infty^\pm \subset \mathbb{H}_\infty^\pm$ induces an inclusion $\mathfrak{E}_{m,n}^\pm \subset \mathbb{H}_n^\pm[p^m]$, and the lemma is proved. □

From now on we shall view $\mathfrak{E}_{m,n}^\pm$ as a submodule of $\mathrm{Sel}_{p^m}^\pm(E/K_n)$ via Lemma 4.7 without further notice.

Lemma 4.8. *Let $n \geq 1$ be an integer. There is a natural injection $\mathfrak{E}_{m,n}^\pm \hookrightarrow \mathfrak{E}_{m,n+1}^\pm$ whose image is $\left(\mathfrak{E}_{m,n+1}^\pm\right)^{\mathcal{G}_{n+1/n}}$.*

Proof. As in the proof of Lemma 4.7, we may identify $\mathfrak{E}_{m,n}^\pm$ and $\mathfrak{E}_{m,n+1}^\pm$ as submodules of $H^1(K_n, A_m)$ and $H^1(K_{n+1}, A_m)$, respectively. Furthermore, as in the proof of Lemma 3.8, the inflation-restriction exact sequence gives an isomorphism

$$H^1(K_n, A_m) \simeq H^1(K_{n+1}, A_m)^{\mathcal{G}_{n+1/n}},$$

and the result follows. □

5. On proper Λ-submodules of finite index

5.1. Admissible classes

We prove the supersingular analogues of [4, Theorem 3.2], which will serve as one of the key ingredients in the proof of Proposition 5.6 below. Throughout, we fix integers $m, n \in \mathbb{N}$. We also assume that the hypothesis **(Tam)** holds.

Definition 5.1. A prime v of K is *admissible* for (E, K_n, p^m) if

(1) E has good reduction at v;
(2) v does not divide p;
(3) v splits completely in K_n/K;
(4) the group $E(K_v)/p^m$ is isomorphic to $(\mathbb{Z}/p^m)^2$.

A set Σ of primes of K is *admissible* for (E, K_n, p^m) if

(1) all $v \in \Sigma$ are admissible for (E, K_n, p^m);
(2) the map $\mathrm{Sel}_{p^m}(E/K) \to \prod_{v\in\Sigma} E(K_v)/p^m$ is injective.

We recall from [4, Lemma 2.23] that admissible sets exist. In the rest of this section, we fix an admissible set Σ. We give the following supersingular analogues of admissible classes defined in [4, Definition 2.24].

Definition 5.2. The group of plus/minus admissible classes with respect to Σ in $H^1(K_n, A_m)$ is

$$H^1_{\Sigma,\pm}(K_n, A_m) = \ker\left(H^1(K_n, A_m) \longrightarrow \prod_{v\notin\Sigma, v\nmid p} \frac{H^1(K_{n,v}, A_m)}{E(K_{n,v})/p^m} \times \prod_{v|p} \frac{H^1(K_{n,v}, A_m)}{\mathbb{H}^{\pm}_{n,v}[p^m]}\right).$$

Remark 5.3. Note that $H^1_{\Sigma,\pm}(K_n, A_m) \subset H^1_{S_n}(K_n, A_m)$, as Σ contains no bad primes.

We can generalize Lemmas 2.25, 2.26, 2.27 and 3.1 of [4] to the supersingular setting.

Lemma 5.4. *(a) The map* $\mathrm{Sel}^{\pm}_{p^m}(E/K_n) \to \bigoplus_{v\in\Sigma} E(K_{n,v})/p^m$ *is injective.*
(b) The map $\prod_{v\in\Sigma} \frac{H^1(K_{n,v},A_m)}{E(K_{n,v})/p^m} \to \mathrm{Hom}(\mathrm{Sel}^{\pm}_{p^m}(E/K_n), \mathbb{Z}/p^m)$ *is surjective.*
(c) The restriction map $H^1_{\Sigma,\pm}(K, A_m) \to H^1_{\Sigma,\pm}(K_n, A_m)^{\mathcal{G}_{n/0}}$ *is an isomorphism.*
(d) There is an exact sequence

$$0 \longrightarrow \mathrm{Sel}^{\pm}_{p^m}(E/K_n) \longrightarrow H^1_{\Sigma,\pm}(K_n, A_m) \longrightarrow \prod_{v\in\Sigma} \frac{H^1(K_{n,v}, A_m)}{E(K_{n,v})/p^m}$$
$$\longrightarrow \mathrm{Sel}^{\pm}_{p^m}(E/K_n)^{\vee} \longrightarrow 0.$$

Proof. Part (a) follows from the same proof as [4, Lemma 2.25] once we replace the control theorem in the ordinary case ([4, Lemma 2.19]) by Proposition 3.9.

Part (b) follows from part (a), as in the proof of [4, Lemma 2.26]; namely, this is dual to property (2) in the definition of an admissible set of primes.

Part (c) can be proved in the same way as Proposition 3.9.

Part (d) now follows from part (b) as in the proof of [4, Lemma 3.1]. □

This allows us to prove the following generalization of [4, Theorem 3.2].

Theorem 5.5. *The* $R_{m,n}$*-module* $H^1_{\Sigma,\pm}(K_n, A_m)$ *is isomorphic to* $\left(R_{m,n}\right)^{2|\Sigma|}$.

Proof. This follows from the same proof as [4, Theorem 3.2], where we replace the appropriate lemmas in [4] with their counterparts given in Lemma 5.4. □

5.2. Cohomology, universal norms and perfect pairings

For all $m, n \in \mathbb{N}$, write $I_{m,n}$ for the augmentation ideal of $R_{m,n}$. The following result generalizes [3, Proposition 6.3] to our plus/minus setting under the following hypothesis.

(Norm) The local norm maps

$$E(K_{n,v}) \longrightarrow E(K_v)$$

are surjective for all $n \geq 1$ and all primes of K that are coprime to p.

Note that **(Norm)** is slightly weaker than [3, Assumption 4] and [4, Assumption 2.15].

Proposition 5.6. *Let $m, n \in \mathbb{N}$. Suppose that **(Norm)** holds. There is a perfect pairing of Tate cohomology groups*

$$\langle \cdot, \cdot \rangle_{m,n} : \hat{H}^0\big(G_n, \mathrm{Sel}^{\pm}_{p^m}(E/K_n)\big) \times \hat{H}^{-1}\big(G_n, \mathrm{Sel}^{\pm}_{p^m}(E/K_n)\big) \longrightarrow I_{m,n}/I^2_{m,n}.$$

Proof. We fix an admissible set of primes for (E, K_n, p^m), which we denote by Σ. We write $\mathrm{Sel}^{\pm}_{p^m}(E/K_n)^0$ for the kernel of the corestriction map $\mathrm{Sel}^{\pm}_{p^m}(E/K_n) \to \mathrm{Sel}^{\pm}_{p^m}(E/K)$. Fix a generator γ_n of G_n. Recall from Lemma 5.4(d) that $\mathrm{Sel}^{\pm}_{p^m}(E/K_n)^0$ is contained in $H^1_{\Sigma,\pm}(K_n, A_m)$, which is a free $R_{m,n}$-module by Theorem 5.5. In particular, the kernel of the corestriction $H^1_{\Sigma,\pm}(K_n, A_m) \to H^1_{\Sigma,\pm}(K, A_m)$ is $(\gamma_n - 1)H^1_{\Sigma,\pm}(K_n, A_m)$. Therefore if $y \in \mathrm{Sel}^{\pm}_{p^m}(E/K_n)^0$, there exists $z \in H^1_{\Sigma,\pm}(K_n, A_m)$ satisfying

$$y = (\gamma_n - 1)z. \tag{5.1}$$

Let z_v denote the image of z in $H^1(K_{n,v}, A_m)/\mathbb{H}^{\pm}_{n,v}[p^m]$, where v is a place of K_n and we denote $E(K_{n,v})/p^m$ by $\mathbb{H}^{\pm}_{n,v}[p^m]$ when $v \nmid p$. Let us denote the pairing induced by local Tate duality by

$$[\cdot, \cdot]_v : \mathbb{H}^1_{n,v}[p^m] \times H^1(K_v, A_m)/\mathbb{H}^1_{n,v}[p^m] \longrightarrow \mathbb{Z}/p^m\mathbb{Z}.$$

The definition of y and (5.1) together imply that

$$z_v \in \Big(H^1(K_{n,v}, A_m)/\mathbb{H}^{\pm}_{n,v}[p^m]\Big)^{G_n}.$$

When $v \nmid p$, the surjectivity of the norm map given by **(Norm)** implies that the restriction map induces an isomorphism

$$\Big(H^1(K_{n,v}, A_m)/\mathbb{H}^{\pm}_{n,v}[p^m]\Big)^{G_n} \cong H^1(K_{0,v}, A_m)/\mathbb{H}^{\pm}_{0,v}[p^m] \tag{5.2}$$

since the restriction map on these quotients is dual to the norm map

$$E(K_{n,v})/p^m \to E(K_v)/p^m$$

as given by $[\cdot,\cdot]_v$. The same is true when $v|p$ since $(\mathbb{H}^{\pm}_v)^\vee$ is free of rank one over Λ by Proposition 3.2(a).

We define a pairing

$$[\cdot,\cdot]_{m,n} : \mathrm{Sel}^{\pm}_{p^m}(E/K) \times \mathrm{Sel}^{\pm}_{p^m}(E/K_n)^0 \longrightarrow I_{m,n}/I^2_{m,n}$$

by sending (x, y) to

$$\sum_v [x_v, z_v]_v(\gamma_n - 1) \mod I^2_{m,n},$$

where the sum runs over all primes of K, x_v is the natural image of x in $\mathbb{H}^{\pm}_{n,v}[p^m]$ and z_v is identified with its image in $H^1(K_v, A_m)/\mathbb{H}^{\pm}_{0,v}[p^m]$ as given by the isomorphism (5.2). The argument in [3, Proposition 6.3] to show that this pairing is independent of the choice of z or γ_n carries over to our setting, as it relies on algebraic properties of Galois cohomology only.

To check that $[\cdot,\cdot]_{m,n}$ induces a perfect pairing $\langle\cdot,\cdot\rangle_{m,n}$ on the Tate cohomology groups it is enough to show that we have a right non-degenerate pairing, as the two groups have the same order. We extend the proof of [30, Lemma 6.15] to our setting. Consider the commutative diagram

$$\begin{array}{ccccccc}
\bigoplus_{v\in S_n} H^1(K_{n,v}, A_m) & & & & & & \\
\downarrow \quad \nwarrow & & & & & & \\
\bigoplus_{v\in S_n} \frac{H^1(K_{n,v},A_m)}{\mathbb{H}^{\pm}_{n,v}[p^m]} & \longleftarrow & H^1_{S_n}(K_n, A_m) & \longleftarrow & \mathrm{Sel}^{\pm}_{p^m}(E/K_n) & \longleftarrow & 0.
\end{array}$$

If we take $\mathbb{Z}/p^m\mathbb{Z}$-linear duals, then Proposition 3.2 gives us a commutative diagram

$$\begin{array}{ccccccc}
\bigoplus_{v\in S_n} H^1(K_{n,v}, A_m) & & & & & & \\
\uparrow \quad \nearrow & & & & & & \\
\bigoplus_{v\in S_n} \mathbb{H}^{\pm}_{n,v}[p^m] & \longrightarrow & H^1_{S_n}(K_n, A_m)^* & \longrightarrow & \mathrm{Sel}^{\pm}_{p^m}(E/K_n)^* & \longrightarrow & 0.
\end{array}$$

Let y be an element of the right kernel of $[\cdot,\cdot]_{m,n}$ and let $z \in H^1_{\Sigma,\pm}(K_n, A_m)$ be as in (5.1). By Remark 5.3, we may consider it as an element of $H^1_{S_n}(K_n, A_m)$. As can be checked by a diagram chase, the image of z in $\bigoplus_{v\in S_n} H^1(K_{n,v}, A_m)$ splits as $a_1 + a_2$, where a_1 is in the image of $\bigoplus_{v\in S_n} \mathbb{H}^{\pm}_{n,v}[p^m]$ and a_2 is in the image of $H^1_S(K, A_m)$ under the restriction map composed with the localization maps. Therefore z itself decomposes as $z_1 + z_2$, where $z_1 \in \mathrm{Sel}^{\pm}_{p^m}(E/K_n)$ and $z_2 \in \mathrm{im}\big(H^1_S(K, A_m) \hookrightarrow H^1_{S_n}(K_n, A_m)\big)$. This shows that $y \in (\gamma_n - 1)\mathrm{Sel}^{\pm}_{p^m}(E/K_n)$. In particular, the image of y in $\hat{H}^{-1}\big(G_n, \mathrm{Sel}^{\pm}_{p^m}(E/K_n)\big)$ is zero. This shows that the pairing $\langle\cdot,\cdot\rangle_{m,n}$ is right non-degenerate, as required. □

For every $n \in \mathbb{N}$, define

$$S_p^{\pm}(E/K_n) := \varprojlim_m \mathrm{Sel}_{p^m}^{\pm}(E/K_n),$$

the inverse limit being taken with respect to the multiplication-by-p maps $E[p^{m+1}] \xrightarrow{p\cdot} E[p^m]$. For all $n, n' \in \mathbb{N}$ with $n \leq n'$ there is a natural corestriction map

$$\mathrm{cores}_{K_{n'}/K_n} : S_p^{\pm}(E/K_{n'}) \longrightarrow S_p^{\pm}(E/K_n). \tag{5.3}$$

We can then define the Λ-module

$$\hat{S}_p^{\pm}(E/K_\infty) := \varprojlim_n S_p^{\pm}(E/K_n),$$

the inverse limit being taken with respect to the corestriction maps in (5.3).

The next proposition will be used in the proof of our main result (Theorem 5.15).

Proposition 5.7. *There is a canonical isomorphism of Λ-modules*

$$\hat{S}_p^{\pm}(E/K_\infty) \simeq \mathrm{Hom}_\Lambda\big(\mathrm{Sel}_{p^\infty}^{\pm}(E/K_\infty)^\vee, \Lambda\big).$$

Proof. One can proceed as in the proof of [32, Lemme 5], replacing the control theorem used in [32] with Proposition 3.9. □

The *universal norm submodule* of $S_p^{\pm}(E/K)$ is

$$US_p^{\pm}(E/K) := \bigcap_{n \geq 1} \mathrm{cores}_{K_n/K}\big(S_p^{\pm}(E/K_n)\big) \subset S_p^{\pm}(E/K).$$

The following theorem is the counterpart for plus/minus Selmer groups of [3, Theorem 6.1].

Theorem 5.8. *There is a perfect pairing*

$$\langle\!\langle \cdot, \cdot \rangle\!\rangle : S_p^{\pm}(E/K)\big/US_p^{\pm}(E/K) \times \mathrm{Sel}_{p^\infty}^{\pm}(E/K_\infty)_{G_\infty} \longrightarrow G_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p.$$

Proof. Using Proposition 5.6, this follows as in the proof of [3, Theorem 6.1], where we replace the control theorem used to prove [3, Lemma 6.4] with the plus/minus analogue provided by Proposition 3.9. □

This in turn gives the following

Corollary 5.9. *The Λ-module $\mathrm{Sel}_{p^\infty}^{\pm}(E/K_\infty)$ admits no proper Λ-submodule of finite index if and only if $S_p^{\pm}(E/K)\big/US_p^{\pm}(E/K)$ has no $\mathbb{Z}_p$-torsion.*

Proof. Using Theorem 5.8 in place of [3, Theorem 6.1], one can proceed exactly as in the proof of [3, Corollary 6.2], which is completely algebraic in nature and does not depend on the definition of the Selmer groups involved. □

5.3. Computation of universal norms

Under appropriate hypotheses, we now compute the universal norm submodule $US_p^{\pm}(E/K)$, thus extending [3, Theorem 7.1] to our setting. In doing so, we follow [3, 7] closely. We begin with a generalization of [1, Lemma 9]. Recall that $R_n = R_{1,n} = (\mathbb{Z}/p\mathbb{Z})[G_n]$ and $\mathfrak{E}_n^{\pm} = \mathfrak{E}_{1,n}^{\pm}$.

Lemma 5.10. *If* $\mathfrak{E}_n^{\pm} \neq 0$*, then* $\mathrm{Sel}_p^{\pm}(E/K_n)$ *admits a free* R_n*-submodule* $U_n^{\pm}$ *such that* $\mathfrak{E}_n^{\pm} \subset U_n^{\pm}$.

Proof. For $m \in \{n, n+1\}$, fix a generator γ_m of G_m. Recall from Corollary 4.6 that $\mathfrak{E}_m^{\pm}$ is a cyclic R_m-module. Consequently, [1, Lemma 3] says that

$$\mathfrak{E}_m^{\pm} \simeq R_m/(\gamma_m - 1)^{p^m - t_m^{\pm}} \simeq (\gamma_m - 1)^{t_m^{\pm}} R_m, \tag{5.4}$$

where $t_m^{\pm} = p^m - \dim_{\mathbb{F}_p}(\mathfrak{E}_m^{\pm})$. Note that $\mathcal{G}_{n+1/n} = \langle \gamma_{n+1}^{p^n} \rangle$, which is cyclic of order p. Then

$$\begin{aligned}\big((\gamma_{n+1} - 1)^s R_{n+1}\big)^{\mathcal{G}} &= \Big(1 + \gamma_{n+1}^{p^n} + \cdots + \gamma_{n+1}^{p^n(p-1)}\Big)(\gamma_{n+1} - 1)^s R_{n+1} \\ &= (\gamma_{n+1} - 1)^{p^{n+1} - p^n + s} R_{n+1}\end{aligned}$$

for all $0 \leq s \leq p^{n+1}$. In particular, isomorphism deflist(5.4) tells us that

$$\dim_{\mathbb{F}_p}\big((\gamma_{n+1} - 1)^s R_{n+1}\big)^{\mathcal{G}} = p^n - s.$$

Recall from Lemma 4.8 that

$$\big(\mathfrak{E}_{n+1}^{\pm}\big)^{\mathcal{G}_{n+1/n}} = \mathfrak{E}_n^{\pm}.$$

Since $\dim_{\mathbb{F}_p} \mathfrak{E}_{n+1}^{\pm} = p^{n+1} - t_{n+1}^{\pm}$, we have

$$\dim_{\mathbb{F}_p}\big(\mathfrak{E}_{n+1}^{\pm}\big)^{\mathcal{G}} = p^n - t_{n+1}^{\pm} = p^n - t_n^{\pm},$$

so $t_{n+1}^{\pm} = t_n^{\pm}$. Let us write $t^{\pm}$ for this common value and define the cyclic R_{n+1}-module

$$U_n^{\pm} := (\gamma_{n+1} - 1)^{p^{n+1} - p^n - t^{\pm}} \mathfrak{E}_{n+1}^{\pm} \simeq (\gamma_{n+1} - 1)^{p^{n+1} - p^n} R_{n+1}.$$

Note that $U_n^{\pm}$ is contained in $\mathfrak{E}_{n+1}^{\pm}$ by definition and is isomorphic to $R_{n+1}^{\mathcal{G}_{n+1/n}}$. Therefore $U_n^{\pm}$ is invariant under $\mathcal{G}_{n+1/n}$, which makes it an R_n-module. On the one hand, $U_n^{\pm}$ contains $(\mathfrak{E}_{n+1}^{\pm})^{\mathcal{G}_{n+1/n}} = \mathfrak{E}_n^{\pm}$; on the other hand, $U_n^{\pm}$ is contained in $\mathrm{Sel}_p^{\pm}(E/K_{n+1})^{\mathcal{G}_{n+1/n}} \simeq \mathrm{Sel}_p^{\pm}(E/K_n)$. Finally, we deduce from (5.4) that $\dim_{\mathbb{F}_p} U_n^{\pm} = p^n$, hence $U_n^{\pm}$ is free of rank one over R_n. □

Now we introduce plus and minus analogues of Shafarevich–Tate groups over finite layers of K_∞/K and, following [3, 7], relative versions of them as well.

Definition 5.11. The *plus and minus p^m-Shafarevich–Tate groups* of E over K_n are

$$Ш^{\pm}_{p^m}(E/K_n) := \mathrm{Sel}^{\pm}_{p^m}(E/K_n)\big/\mathbb{H}^{\pm}_n[p^m].$$

The *relative plus and minus p^m-Shafarevich–Tate groups* are

$$Ш^{\pm}_{p^m}(E, K_{n+1}/K_n) := \ker\left(Ш^{\pm}_{p^m}(E/K_n) \longrightarrow Ш^{\pm}_{p^m}(E/K_{n+1})\right),$$

where the map on the right is induced by restriction.

Let $U^{\pm}_n$ be the free R_n-submodule of $\mathrm{Sel}^{\pm}_p(E/K_n)$ from Lemma 5.10, and recall the labels that were assigned to sets of hypotheses in Sect. 1.2.

Lemma 5.12. *Suppose that* $Ш^{\pm}_p(E, K_{n+1}/K_n) = 0$ *and* $\mathfrak{E}^{\pm}_n \neq 0$. *Then* $U^{\pm}_n \subset \mathbb{H}^{\pm}_n[p]$.

Proof. Consider the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{H}^{\pm}_n[p] & \longrightarrow & \mathrm{Sel}^{\pm}_p(E/K_n) & \longrightarrow & Ш^{\pm}_p(E/K_n) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow \simeq & & \downarrow & & \\
0 & \longrightarrow & \left(\mathbb{H}^{\pm}_{n+1}[p]\right)^{\mathcal{G}_{n+1/n}} & \longrightarrow & \mathrm{Sel}^{\pm}_p(E/K_{n+1})^{\mathcal{G}_{n+1/n}} & \longrightarrow & Ш^{\pm}_p(E/K_{n+1})^{\mathcal{G}_{n+1/n}} & \longrightarrow & 0
\end{array}$$

in which the middle vertical isomorphism comes from Proposition 3.9. By applying the snake lemma, one checks that

$$\mathbb{H}^{\pm}_n[p] = \left(\mathbb{H}^{\pm}_{n+1}[p]\right)^{\mathcal{G}_{n+1/n}}. \tag{5.5}$$

By construction, $U^{\pm}_n$ is contained in the module on the right-hand side of (5.5), and the result follows. □

Lemma 5.13. *There is an equality*

$$S^{\pm}_p(E/K) = \varprojlim_m \mathbb{H}^{\pm}_0[p^m].$$

Proof. By Lemma 3.7, $\mathbb{H}^{\pm}_0[p^m] = E(K)/p^m E(K)$ and $\mathrm{Sel}^{\pm}_{p^m}(E/K) = \mathrm{Sel}_{p^m}(E/K)$, therefore there is a short exact sequence

$$0 \longrightarrow \mathbb{H}^{\pm}_0[p^m] \longrightarrow \mathrm{Sel}^{\pm}_{p^m}(E/K) \longrightarrow Ш_{p^m}(E/K) \longrightarrow 0. \tag{5.6}$$

But $Ш_{p^m}(E/K)$ is finite and bounded independently of m ([26, Theorem A]), hence the result follows upon taking inverse limits in (5.6).

Recall from 1.2 the following hypothesis.

(mod p) For an elliptic curve $E/\mathbb{Q}$ satisfying both $a_p(E) = 0$ and **(Norm)**, we have $Ш^{\pm}_p(E, K_{n+1}/K_n) = 0$ and $\mathfrak{E}^{\pm}_n \neq 0$ for all $n \in \mathbb{N}$.

Remark 5.14. The condition $\mathfrak{E}_n^{\pm} \neq 0$ has been established in some cases which overlap with our own; see [5, Theorem 4.6].

The following theorem is the main result of this article.

Theorem 5.15. *Suppose that hypothesis* ***(mod*** *p)* *is satisfied. Then $US_p^{\pm}(E/K)$ is free of rank one over $\mathbb{Z}_p$ and the Λ-module $\mathrm{Sel}_{p^\infty}^{\pm}(E/K_\infty)$ admits no proper Λ-submodule of finite index.*

Proof. We first observe that $E(K)$ is p-torsion free; this is a consequence of our hypotheses that E has good supersingular reduction at primes above p and that p is unramified in K. Thus it follows from the proof of Lemma 5.13 that $S_p^{\pm}(E/K) \simeq E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is a free $\mathbb{Z}_p$-module of finite rank. Furthermore, by [27, Theorem 1.4] (see also [7, Theorem A]), the Λ-module $\mathrm{Sel}_{p^\infty}^{\pm}(E/K_\infty)^\vee$ has rank one. Combining this with Proposition 5.7, and arguing as in [2, 3.2], one sees that

$$\mathrm{rank}_{\mathbb{Z}_p} US_p^{\pm}(E/K) = \mathrm{rank}_{\Lambda} \hat{S}_p^{\pm}(E/K_\infty) = 1.$$

Then it suffices to show that $US_p^{\pm}(E/K)$ contains a non-trivial element of $S_p^{\pm}(E/K)$ not divisible by p. This would imply that $US_p^{\pm}(E/K) \simeq \mathbb{Z}_p$ and that the $\mathbb{Z}_p$-module $S_p^{\pm}(E/K)\big/US_p^{\pm}(E/K)$ is torsion-free. The last statement of the theorem would then follow from Corollary 5.9.

Thus let us set $T\mathbb{H}_n^{\pm} := \varprojlim_m \mathbb{H}_n^{\pm}[p^m]$ for the p-adic Tate module of $\mathbb{H}_n^{\pm}$; then

$$T\mathbb{H}_n^{\pm}\big/pT\mathbb{H}_n^{\pm} = \mathbb{H}_n^{\pm}[p].$$

Lemma 5.12 says that the free R_n-module $U_n^{\pm}$ from Lemma 5.10 lies inside $\mathbb{H}_n^{\pm}[p]$. Let $\tilde{U}_n^{\pm}$ be a free $\mathbb{Z}_p[G_n]$-submodule of $T\mathbb{H}_n^{\pm}$ of rank one lifting $U_n^{\pm}$ modulo p, generated by an element v_n. Then $\mathrm{cores}_{K_n/K}(v_n)$ is not divisible by p, thanks to the freeness of $\tilde{U}_n^{\pm}$. Lemma 5.13 tells us that

$$\mathrm{cores}_{K_n/K}(v_n) \in T\mathbb{H}_0^{\pm} = US_p^{\pm}(E/K).$$

By compactness, we may find a subsequence $\left(\mathrm{cores}_{K_{n_i}/K}(v_{n_i})\right)_{i\geq 0}$ converging to an element of $S_p^{\pm}(E/K)$ that lies in $US_p^{\pm}(E/K)$ and is not divisible by p, as required. □

6. An application: variation of Iwasawa invariants

6.1. *p-congruent elliptic curves*

In this section, we illustrate one application of Theorem 5.15. Recall that two elliptic curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ are *p-congruent* (or *congruent modulo p*) if $E[p] \simeq E'[p]$ as $G_{\mathbb{Q}}$-modules. Accordingly, in 1.2, we gave a name to the following hypothesis.

(Cong) Given two elliptic curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$, both of which satisfy **(mod** p**)**, there is an isomorphism $E_1[p] \simeq E_2[p]$ of $G_{\mathbb{Q}}$-modules.

In [14], Greenberg and Vatsal showed that the Iwasawa invariants (defined over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$) of p-congruent, p-ordinary elliptic curves are related by an explicit formula, and they used this to prove many cases of the Iwasawa Main Conjecture. These results were later extended to Hida families by Emerton, Pollack and Weston [10], while results in the non-ordinary case were established for elliptic curves by B. D. Kim [22] and for more general modular forms by the first two named authors [15].

An analogue for the anticyclotomic $\mathbb{Z}_p$-extension K_∞ of an imaginary quadratic field K of the results in [10] was obtained by Castella, C.-H. Kim and Longo [6] under the assumption that the tame level N of the Hida family is divisible by an *odd* number of primes that are inert in K; in this setting, results on the vanishing of the μ-invariant were obtained by Pollack and Weston [34]. When N satisfies this divisibility hypothesis, the usual Selmer groups over K_∞ are expected to be Λ-cotorsion, and the arguments regarding the variation of Iwasawa invariants closely mirror the cyclotomic case.

As we have seen in previous sections, when all the primes dividing N split in K the classical Selmer groups are not Λ-cotorsion, and extra care must be taken (this happens, more generally, when N is divisible by an *even* number of inert primes). Recently, analogues in this setting of the Greenberg–Vatsal result was proved for p-ordinary modular forms by the first two named authors [16,17]. In this final section of the paper, we will extend these results to setting of p-supersingular elliptic curves.

6.2. *Definitions of Iwasawa invariants*

Let us briefly recall the definition of the Iwasawa invariants. As explained in 2.2, we identify Λ with $\mathbb{Z}_p[\![X]\!]$ via our fixed topological generator γ_∞ of G_∞. Let M be a finitely generated Λ-module; there is a pseudo-isomorphism, i.e., a map with finite kernel and cokernel

$$M \sim \Lambda^{\oplus r} \oplus \bigoplus_{i=1}^{s} \Lambda/(p^{a_i}) \oplus \bigoplus_{j=1}^{t} \Lambda\Big/\big(F_j^{n_j}\big) \tag{6.1}$$

for suitable integers $r, s, t \geq 0, a_i, n_j \geq 1$ and irreducible Weierstrass polynomials $F_j \in \mathbb{Z}_p[X]$ (see, e.g., [31, Theorem 5.3.8]). The *μ-invariant* and the *λ-invariant* of M are

$$\mu(M) := \sum_{i=1}^{s} a_i, \qquad \lambda(M) := \sum_{j=1}^{t} n_j \deg(F_j).$$

Continue to assume that M is a finitely-generated Λ-module M, and let M_{tor} denote the maximal torsion submodule of M. Recall from [19, 1.8 and 3.1] that there is an exact sequence of Λ-modules

$$0 \to M_{\mathrm{tor}} \to M \to M^{++} \to T_2(M) \to 0, \tag{6.2}$$

where M^{++} is the reflexive hull of M, which is free over Λ and $T_2(M)$ is finite. In the same way as [17, Definition 3.3], we define an integer $c(M)$ as follows.

Definition 6.1. Let M be a finitely generated module over Λ. We define $c(M)$ to be the unique integer satisfying the equation

$$|T_2(M)[p]| = |\mathbb{F}_p|^{c(M)}.$$

When $M = \mathrm{Sel}_{p^\infty}^{\pm}(E/K_\infty)^\vee$ is the Pontryagin dual of the plus/minus Selmer group associated to an elliptic curve E, we write $c_\pm(E) = c(M)$.

6.3. Variation of Iwasawa invariants

For the rest of this paper, we fix elliptic curves E_1 and E_2 with square-free conductors N_1 and N_2, respectively, such that $E_1[p] \simeq E_2[p]$ as $G_\mathbb{Q}$-modules and $a_p(E_i) = 0$ for $i = 1, 2$. Moreover, we assume that, taken together, the field K, the prime p, and the product of the conductors N_1N_2 satisfy **(Heeg)**. We also assume that both curves satisfy the hypothesis **(Tam)**.

Our goal is to relate the Iwasawa invariants of $\mathrm{Sel}^{\pm}(E_i/K_\infty)$ for $i = 1, 2$ (or rather, the Pontryagin duals of these Selmer groups). To ease notation, let us write $\mathcal{X}^{\pm}(E_i) = \mathrm{Sel}_{p^\infty}^{\pm}(E_i/K_\infty)^\vee$ for the Pontryagin dual of each Selmer group, and let us set

$$\mu_\pm(E_i) := \mu\big(\mathcal{X}^{\pm}(E_i)\big) \quad \text{and} \quad \lambda_\pm(E_i) := \lambda\big(\mathcal{X}^{\pm}(E_i)\big).$$

Our first step is to observe that the $G_\mathbb{Q}$-isomorphism $E_1[p] \simeq E_2[p]$ induces an isomorphism of Selmer groups

$$\mathrm{Sel}_p^{\pm}(E_1/K_\infty) \simeq \mathrm{Sel}_p^{\pm}(E_2/K_\infty).$$

This amounts to showing that we have isomorphisms between the local conditions defining the Selmer groups. For the places away from p, the local condition is the unramified condition, so this is clear, and it remains only to check the local condition at places above p. But we have assumed that p splits in $K/\mathbb{Q}$, hence for a prime $\mathfrak{p} \mid p$ of K above p, we have $K_\mathfrak{p} = \mathbb{Q}_p$, in which case this compatibility is well-established; see e.g. [22, Proposition 2.8] and the proof of Theorem 4.1.1 of [36].

Thus, in light of Proposition 3.9, we have an isomorphism

$$\mathrm{Sel}_{p^\infty}^{\pm}(E_1/K_\infty)[p] \simeq \mathrm{Sel}_{p^\infty}^{\pm}(E_2/K_\infty)[p].$$

By duality, we have established the following result.

Proposition 6.2. *Suppose $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ are elliptic curves satisfying $a_p(E_i) = 0$ and **(Tam)** for $i = 1, 2$ and that $E_1[p] \simeq E_2[p]$ as $G_\mathbb{Q}$-modules. Assume further that the hypothesis **(Heeg)** holds. Then we have an isomorphism*

$$\mathcal{X}^{\pm}(E_1)/p \simeq \mathcal{X}^{\pm}(E_2)/p.$$

Recall that, when E is supersingular, $\mu_\pm(E)$ is always expected to vanish, and it is known to vanish in some cases (see, e.g., [28, Theorem B]). Furthermore, when these μ-invariants vanish, the corresponding λ-invariants can often be related to each other in an explicit manner, in the spirit of Greenerg-Vatsal [14]. In our present setting, we have the following result.

Theorem 6.3. *Let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ be elliptic curves for which the hypotheses* ***(Heeg)*** *and* ***(Cong)*** *hold. Then*

$$\mu_\pm(E_1) = 0 \iff \mu_\pm(E_2) = 0.$$

Suppose that $\mu_\pm(E_1) = \mu_\pm(E_2) = 0$. Then

$$\lambda_\pm(E_1) + c_\pm(E_1) = \lambda_\pm(E_2) + c_\pm(E_2).$$

Proof. Our assumptions that $E_1[p] \simeq E_2[p]$ and that **(Heeg)** holds allow us to invoke Proposition 6.2 to deduce an isomorphism

$$\mathcal{X}^\pm(E_1)/p \simeq \mathcal{X}^\pm(E_2)/p.$$

By [27, Theorem 1.4], both $\mathcal{X}_\pm(E_1)$ and $\mathcal{X}_\pm(E_2)$ have Λ-rank 1, so we may apply [16, Corollary 2.4] to conclude that

$$\mu_\pm(E_1) = 0 \iff \mu_\pm(E_2) = 0.$$

Assume that the $\mu_\pm$-invariants vanish. Then since **(Cong)** holds, we know from Theorem 5.15 (and duality) that each $\mathcal{X}^\pm(E_i)$ contains no non-trivial finite Λ-submodules, so we may apply [17, Corollary 3.4] to deduce the claimed relationship between the $\lambda_\pm$-invariants, and we are finished. □

Acknowledgements We thank Mirela Çiperiani and Matteo Longo for interesting discussions on some of the topics of this paper. We are also grateful to the anonymous referee for several helpful suggestions which clarified some proofs and otherwise improved the exposition of the paper.

References

[1] Bertolini, M.: An annihilator for the p-Selmer group by means of Heegner points, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. **5**(2), 129–140 (1994)
[2] Bertolini, M.: Selmer groups and Heegner points in anticyclotomic Z_p-extensions. Compos. Math. **99**(2), 153–182 (1995)
[3] Bertolini, M.: Iwasawa theory for elliptic curves over imaginary quadratic fields. J. Théor. Nombres Bordeaux **13**(1), 1–25 (2001)
[4] Bertolini, M., Darmon, H.: Derived heights and generalized Mazur-Tate regulators. Duke Math. J. **76**(1), 75–111 (1994)
[5] Burungale, A.A.: On the non-triviality of the p-adic Abel-Jacobi image of generalised Heegner cycles modulo p, I: modular curves. J. Algebraic Geom. **29**(2), 329–371 (2020)
[6] Castella, F., Kim, C.-H., Longo, M.: Variation of anticyclotomic Iwasawa invariants in Hida families. Algebra Number Theory **11**(10), 2339–2368 (2017)
[7] Castella, F., Wan, X.: Perrin–Riou's main conjecture for elliptic curves at supersingular primes. arXiv:1607.02019 (2016)
[8] Çiperiani, M.: Tate-Shafarevich groups in anticyclotomic $\mathbb{Z}_p$-extensions at supersingular primes. Compos. Math. **145**(2), 293–308 (2009)

[9] Darmon, H., Iovita, A.: The anticyclotomic Main Conjecture for elliptic curves at supersingular primes. J. Inst. Math. Jussieu **7**(2), 291–325 (2008)
[10] Emerton, M., Pollack, R., Weston, T.: Variation of Iwasawa invariants in Hida families. Invent. Math. **163**(3), 523–580 (2006)
[11] Greenberg, R., Iwasawa theory for elliptic curves, Arithmetic theory of elliptic curves (Cetraro, : Lecture Notes in Math., vol. 1716. Springer, Berlin **1999**, 51–144 (1997)
[12] Greenberg, R.: Surjectivity of the global-to-local map defining a Selmer group. Kyoto J. Math. **50**(4), 853–888 (2011)
[13] Greenberg, R.: On the structure of Selmer groups, Elliptic curves, modular forms and Iwasawa theory, Springer Proc. Math. Stat., vol. 188, Springer, Cham, pp. 225–252 (2016)
[14] Greenberg, R., Vatsal, V.: On the Iwasawa invariants of elliptic curves. Invent. Math. **142**(1), 17–63 (2000)
[15] Hatley, J., Lei, A.: Arithmetic properties of signed Selmer groups at non-ordinary primes. Ann. Inst. Fourier (Grenoble) **69**(3), 1259–1294 (2019)
[16] Hatley, J., Lei, A.: Comparing anticyclotomic Selmer groups of positive coranks for congruent modular forms. Math. Res. Lett. **26**(4), 1115–1144 (2019)
[17] Hatley, J., Lei, A.: Comparing anticyclotomic Selmer groups of positive coranks for congruent modular forms – Part II, arXiv:2009.03772 (2020)
[18] Iovita, A., Pollack, R.: Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields. J. Reine Angew. Math. **598**, 71–103 (2006)
[19] Jannsen, U.: Iwasawa modules up to isomorphism, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, pp. 171–207 (1989)
[20] Kidwell, K.: On the structure of Selmer groups of p-ordinary modular forms over $\mathbf{Z}_p$-extensions. J. Number Theory **187**, 296–331 (2018)
[21] Kim, B.D.: The parity conjecture for elliptic curves at supersingular reduction primes. Compos. Math. **143**(1), 47–72 (2007)
[22] Kim, B.D.: The Iwasawa invariants of the plus/minus Selmer groups. Asian J. Math. **13**(2), 181–190 (2009)
[23] Kim, B.D.: Signed-Selmer groups over the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field. Canad. J. Math. **66**(4), 826–843 (2014)
[24] Kitajima, T., Otsuki, R.: On the plus and the minus Selmer groups for elliptic curves at supersingular primes. Tokyo J. Math. **41**(1), 273–303 (2018)
[25] Kobayashi, S.: Iwasawa theory for elliptic curves at supersingular primes. Invent. Math. **152**(1), 1–36 (2003)
[26] Kolyvagin, V.A.: Euler systems, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, pp. 435–483 (1990)
[27] Longo, M., Vigni, S.: Plus/minus Heegner points and Iwasawa theory of elliptic curves at supersingular primes. Boll. Unione Mat. Ital. **12**(3), 315–347 (2019)
[28] Matar, A.: Plus/minus Selmer groups and anticyclotomic $\mathbf{Z}_p$-extensions, available at http://www.ahmedmatar.net/Anticyclotomic_paper4_v2.pdf (2019)
[29] Mazur, B.: Rational points of abelian varieties with values in towers of number fields. Invent. Math. **18**(3–4), 183–266 (1972)
[30] Milne, J.: Arithmetic Duality Theorems, Perspectives in Mathematics, vol. 1. Academic Press Inc, Boston, MA (1986)
[31] Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of Number Fields, Grundlehren der Mathematischen Wissenschaften, vol. 323. Springer, Berlin (2000)
[32] Perrin-Riou, B.: Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner. Bull. Soc. Math. France **115**(4), 399–456 (1987)

[33] Pollack, R.: On the p-adic L-function of a modular form at a supersingular prime. Duke Math. J. **118**(3), 523–558 (2003)
[34] Pollack, R., Weston, T.: On anticyclotomic μ-invariants of modular forms. Compos. Math. **147**(5), 1353–1381 (2011)
[35] Ponsinet, G.: On the structure of signed Selmer groups. Math. Z. **294**(3–4), 1635–1658 (2020)
[36] Suman, A., Lim, M.F.: On the signed Selmer groups of congruent elliptic curves with semistable reduction at all primes above p (2019)
[37] Weston, T.: Iwasawa invariants of Galois deformations. Manuscripta Math. **118**(2), 161–180 (2005)