Glasgow Mathematical Journal (2026), 1–47
doi:10.1017/S0017089526100901

Glasgow Mathematical Journal

RESEARCH ARTICLE

Congruent elliptic curves and $\mathbb{Z}_p^d$-extensions

Sören Kleine[1] and Ahmed Matar[2]

[1]Universität der Bundeswehr München, Germany
[2]University of Bahrain, Bahrain
Corresponding author: Sören Kleine; Email: soeren.kleine@unibw.de

Received: 3 July 2024; **Revised:** 12 January 2026; **Accepted:** 12 January 2026

Keywords: congruent elliptic curves; generalised Iwasawa invariants; Greenberg Selmer groups; strict Selmer groups

2020 Mathematics Subject Classification: *Primary* - 11R23

Abstract
Let p be an odd prime, and let E_1 and E_2 be two elliptic curves defined over a number field K, with good ordinary reduction at p. We compare the Λ-ranks and (generalized) Iwasawa invariants of the Pontryagin duals of the Selmer groups of E_1 and E_2 over $\mathbb{Z}_p^d$-extensions $\mathbb{L}_\infty$ of K for general $d \geq 1$ under the hypothesis that $E_1[p^i] \cong E_2[p^i]$ as Galois modules for a sufficiently large i. This generalizes and complements previous work over $\mathbb{Z}_p$-extensions. The comparison of generalized Iwasawa invariants is related via an up-down approach to the comparison of the variation of classical Iwasawa invariants over the $\mathbb{Z}_p$-extensions of K which are contained in $\mathbb{L}_\infty$.

1. Introduction

Let K be a number field and p an odd prime. Two elliptic curves E_1 and E_2 defined over K are said to be p-congruent if $E_1[p] \cong E_2[p]$ as $\mathrm{Gal}(\bar{K}/K)$-modules, where $\bar{K}$ denotes any fixed algebraic closure of K. More generally, we will study in this article pairs of elliptic curves E_1 and E_2 such that $E_1[p^i] \cong E_2[p^i]$ for some positive integer i, which we will simply call *congruent elliptic curves* in this paper. Let K_∞/K be a $\mathbb{Z}_p$-extension and let $\mathrm{Sel}(E_i/K_\infty)$ be the p-primary classical Selmer group of E_i over K_∞. We denote the Pontryagin dual of $\mathrm{Sel}(E_i/K_\infty)$ by $X(E_i/K_\infty)$. Now assume for $i = 1, 2$ that E_i has good ordinary reduction at all primes of K dividing p and that $X(E_i/K_\infty)$ is a $\Lambda := \mathbb{Z}_p[[T]] \cong \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-torsion module. When $K = \mathbb{Q}$ (so $K_\infty = \mathbb{Q}_{cyc}$, the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$) the Greenberg-Vatsal paper [20] studies the relations between the lambda invariants $\lambda(X(E_1/K_\infty))$ and $\lambda(X(E_2/K_\infty))$ under the assumption that $\mu(X(E_i/K_\infty)) = 0$ for $i = 1$ or 2. These results were later generalized by Kidwell [28] to arbitrary number fields. The paper of Kundu and Ray [37] refines the results of Greenberg-Vatsal and Kidwell, and the authors use their results to construct elliptic curves E over an imaginary quadratic field K such that $X(E/K_{ac})$ has a large λ-invariant where K_{ac} is the anticyclotomic $\mathbb{Z}_p$-extension of K.

In a similar fashion to the above results, the aim of this paper is to study relationships between *generalized Iwasawa invariants* of Pontryagin duals of Selmer groups for congruent elliptic curves over $\mathbb{Z}_p^d$-extensions. The generalized Iwasawa invariants were introduced by Cuoco and Monsky in [11]. These are defined as follows: Let G be a profinite group isomorphic to $\mathbb{Z}_p^d$ for some $d \geq 1$. The Iwasawa algebra $\Lambda_d = \mathbb{Z}_p[[G]]$ attached to G may be identified (by choosing a set of topological generators of G) with $\mathbb{Z}_p[[T_1, T_2, \ldots, T_d]]$. Now let M be a finitely generated torsion Λ_d-module that is not pseudo-null. Then there exists a pseudo-null module A and an exact sequence

$$0 \longrightarrow \bigoplus_{i=1}^{s} \Lambda_d/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda_d/h_j^{n_j} \longrightarrow M \longrightarrow A \longrightarrow 0. \tag{1}$$

In the above, the exponents are natural numbers and the h_j are irreducible elements of Λ_d which are prime to p. The module $\bigoplus_{i=1}^{s} \Lambda_d/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda_d/h_j^{n_j}$ is called an *elementary* Λ_d-module attached to M. The

element $f_M = \prod_{i=1}^{s} p^{m_i} \cdot \prod_{j=1}^{t} h_j^{n_j}$ is the *characteristic power series* of M. One then defines the generalized Iwasawa invariants of M as follows. First, $m_0(M) = \sum_{i=1}^{s} m_i$. The definition of the second invariant is more involved. We write $f_M = p^{m_0(M)} \cdot g_M$, and we consider the (nonzero) image $\overline{g_M}$ of g_M in the quotient ring $\Omega_d = \Lambda_d/p$. We let $l_0(M)$ be the sum of the valuations $v_{\mathfrak{p}}(\overline{g_M})$, where $\mathfrak{p}$ runs over the primes of Ω_d of the form $\overline{\gamma - 1}$, with $\gamma \in G$ not a p-th power (since Λ_d/p is a unique factorization domain, this sum is in fact finite). Finally, for a pseudo-null Λ_d-module M, we define $f_M = 0$ and $m_0(M) = l_0(M) = 0$.

In [35], we introduced a modified l_0-invariant which is defined as follows. Let $d > 1$. Recall that $\Lambda_d \cong \mathbb{Z}_p[[G]]$, where G is topologically isomorphic to $\mathbb{Z}_p^d$. As above, let M be any finitely generated torsion Λ_d-module that is not pseudo-null, and let f_M be the characteristic power series of M. Write $f_M = p^{m_0(M)} \cdot g_M$ with $p \nmid g_M$, as usual, and consider the image $\overline{g_M}$ of g_M in Ω_d.

Definition 1.1. *Let $\mathcal{T}$ be the set of tuples $(\gamma_1, \ldots, \gamma_{d-1})$ of elements of G which topologically generate subgroups isomorphic to $\mathbb{Z}_p^{d-1}$. We let*

$$\widehat{l_0}(M) = \widehat{l_0}(\overline{g_M}) = \sum_{\mathfrak{p}} v_{\mathfrak{p}}(\overline{g_M}),$$

where $\mathfrak{p}$ runs over the minimal prime ideals of $(\overline{g_M}) \subseteq \Omega_d$ which are contained in some prime ideal $\mathcal{P}_t$ of the form $(\overline{\gamma_1 - 1}, \ldots, \overline{\gamma_{d-1} - 1})$, for any tuple $t = (\gamma_1, \ldots, \gamma_{d-1})$ of $\mathcal{T}$.

Note that $\widehat{l_0}(M) \geq l_0(M)$ by the definitions, and that $\widehat{l_0}(M) = l_0(M)$ if $d = 2$.

If $d = 1$, that is, for Λ-modules, we can define Iwasawa invariants even for non-torsion modules. To be more precise, let M be a finitely generated (non-necessarily torsion) Λ-module. Then there exist finite Λ-modules A and B and an exact sequence

$$0 \longrightarrow A \longrightarrow M \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda/h_j^{n_j} \longrightarrow B \longrightarrow 0. \tag{2}$$

In the above, the exponents are again natural numbers and the h_j are now irreducible polynomials in $\mathbb{Z}_p[T]$ which are prime to p. The module $\Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda/h_j^{n_j}$ is again called an *elementary* Λ_d-module attached to M, r is called the rank of M, and $f_M = \prod_{i=1}^{s} p^{m_i} \cdot \prod_{j=1}^{t} h_j^{n_j}$ is the characteristic power series of M, which is now a polynomial in $\mathbb{Z}_p[T]$. In fact, $\prod_{j=1}^{t} h_j^{n_j}$ is a so-called *distinguished polynomial*, that is, it is monic and congruent to some power of T modulo p in the ring Λ. We define the Iwasawa invariants of M as follows: $\mu(M) = \sum_i m_i$ ($= m_0(M)$ for a torsion Λ-module M) and we let $\lambda(M)$ be the degree of f_M (i.e. $\prod_{j=1}^{t} h_j^{n_j} \equiv T^{\lambda(M)} \pmod{p}$). One can show that $\lambda(M) = l_0(M)$ for a torsion Λ-module M.

Let $\mathbb{L}_\infty$ be a fixed $\mathbb{Z}_p^d$-extension of K. If $\sigma_1, \sigma_2, \ldots, \sigma_d$ are topological generators of $\mathrm{Gal}(\mathbb{L}_\infty/K)$, we let $T_i = \sigma_i - 1$ for each i. Suppose that E_1 and E_2 are two elliptic curves over K. We let $\Lambda_d = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}_\infty/K)]]$ be the Iwasawa algebra attached to $\mathbb{L}_\infty/K$, identified with the power series ring $\mathbb{Z}_p[[T_1, T_2, \ldots, T_d]]$. We assume that neither $X(E_1/\mathbb{L}_\infty)$ nor $X(E_2/\mathbb{L}_\infty)$ is a pseudo-null Λ_2-module, that is, their characteristic power series are nonzero. If $X(E_j/\mathbb{L}_\infty)$ is a torsion Λ_d-module, then let $m_{0,j} = m_0(X(E_j/\mathbb{L}_\infty))$, $\widehat{l_{0,j}} = \widehat{l_0}(X(E_j/\mathbb{L}_\infty))$, and $l_{0,j} = l_0(X(E_j/\mathbb{L}_\infty))$ and let f_j be the characteristic power series of $X(E_j/\mathbb{L}_\infty)$. We can write $f_j = p^{m_{0,j}} g_j$ so that $p \nmid g_j$. Let S_p be the set of primes of K above p.

We fix a finite set S of nonarchimedean primes of K containing S_p and all the primes where either E_1 or E_2 has bad reduction.

Definition 1.2. *Let $\mathcal{E}$ be the set of $\mathbb{Z}_p$-extensions of K which are contained in our fixed $\mathbb{Z}_p^d$-extension $\mathbb{L}_\infty$. Define $\mathcal{E}_p$ (resp. $\mathcal{E}_{ns}$) to be the set of all $\mathbb{Z}_p$-extensions $K_\infty \in \mathcal{E}$ in which all primes in S_p ramify (resp. no prime in S splits completely).*

As examples of $\mathbb{Z}_p$-extensions which belong or do not belong to E_p and E_{ns}, we mention that the cyclotomic $\mathbb{Z}_p$-extension of K is contained in $\mathcal{E}_p \cap \mathcal{E}_{ns}$. If K is a quadratic imaginary field and the prime

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

of $\mathbb{Q}$ below some prime in S is inert in $K/\mathbb{Q}$, then that prime in S splits completely in the anticyclotomic $\mathbb{Z}_p$-extension of K and hence this extension is not in $\mathcal{E}_{ns}$. Furthermore, for this field K if p splits in $K/\mathbb{Q}$, then K has two $\mathbb{Z}_p$-extensions not contained in $\mathcal{E}_p$.

Definition 1.3. *Let E be an elliptic curve defined over K. If v is a prime of K, then we say that E satisfies $(\star)$ at v if either E has good reduction at v or one of the following two conditions is met:*

(i) E has additive reduction at v, and $p \geq 5$, or
(ii) E has multiplicative reduction at v, and $p \nmid c_v$ and $p \nmid \#k_v^\times$ where k_v is the residue field of K_v and c_v is the Tamagawa number.

Throughout this paper, we assume that E_1 and E_2 have good ordinary reduction at all primes of K above p.

We let μ_p denote the group of p-th roots of unity. Throughout the paper, we make the following assumption on our field K:

Condition (Δ): For every prime $\mathfrak{p}$ of K above p, we have that the inertia subgroup of the extension $K_\mathfrak{p}(\mu_p)/K_\mathfrak{p}$ is nontrivial.

This condition is needed for the proof of the central Lemma 3.5. Note that it is a rather mild assumption (see also Remark 1.6).

The main results of this paper are the following two theorems. Actually, the first theorem was obtained by Lim in a more general setting (see [39, Theorem 4.2.1]). We give a different proof of this result which will, in contrast to Lim's approach, be strong enough to derive also results on generalized λ-invariants (see Theorem 1.5, and cf. also the introduction to Section 6).

Theorem 1.4. *Assume that $\mathcal{E}_p \neq \emptyset$ and $\mathcal{E}_{ns} \neq \emptyset$. If $X(E_1/\mathbb{L}_\infty)$ is a Λ_d-torsion module and $E_1[p^i] \cong E_2[p^i]$ for some integer $i > m_{0,1}$, then $X(E_2/\mathbb{L}_\infty)$ is a Λ_d-torsion module with $m_{0,2} = m_{0,1}$.*

Recall that we denote by $f_1 = p^{m_{0,1}} g_1$ and $f_2 = p^{m_{0,2}} g_2$ the characteristic power series of $X(E_1/\mathbb{L}_\infty)$ and $X(E_2/\mathbb{L}_\infty)$, and that $f_1, f_2 \neq 1$ since we assume that $X(E_1/\mathbb{L}_\infty)$ and $X(E_2/\mathbb{L}_\infty)$ are not pseudo-null over Λ_d. Let $\Omega_d = \Lambda_d/p$ be the 'mod p' Iwasawa algebra, and denote by $\overline{g_1}$ and $\overline{g_2}$ the cosets of g_1 and g_2 in Ω_d.

Theorem 1.5. *Assume that $\mathcal{E}_p \neq \emptyset$, $\mathcal{E}_{ns} \neq \emptyset$, and that both E_1 and E_2 satisfy condition $(\star)$ for all $v \in S$. Furthermore, we assume*

(i) Both $E_1(\mathbb{L}_\infty)[p^\infty]$ and $E_2(\mathbb{L}_\infty)[p^\infty]$ are finite.
(ii) If $d > 2$, the maximal pseudo-null submodules of $X(E_1/\mathbb{L}_\infty)$ and $X(E_2/\mathbb{L}_\infty)$ are finitely generated over $\mathbb{Z}_p$.
(iii) The decomposition subgroups $D_v(\mathbb{L}_\infty/K) \subseteq \mathrm{Gal}(\mathbb{L}_\infty/K)$ are open for each $v \mid p$.
(iv) $X(E_1/\mathbb{L}_\infty)$ is a Λ_d-torsion module and $E_1[p^i] \cong E_2[p^i]$ for some integer $i > m_{0,1}$.

Then the following statements hold.

(1) $X(E_2/\mathbb{L}_\infty)$ is a Λ_d-torsion module with $m_{0,2} = m_{0,1}$. Moreover, $\widehat{l_{0,1}} \neq 0$ if and only if $\widehat{l_{0,2}} \neq 0$.
(2) $l_{0,2} = l_{0,1}$.

Let us comment on the additional hypotheses in Theorem 1.5.

- Condition (i) is mild as [36, Lemma 3.5] shows.
- Concerning condition (ii), we need the maximal pseudo-null submodules of the Pontryagin duals of the Selmer groups to be "not too large" in order to be able to apply results from [35]. In Section 9, we provide two explicit settings where condition (ii) is met.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

- The third hypothesis (iii) in Theorem 1.5 ensures that $\mathbb{L}_\infty$ contains only finitely many primes above p. In particular, if $K_\infty \subseteq \mathbb{L}_\infty$ denotes any $\mathbb{Z}_p$-extension of K, then no prime v of K above p splits completely in K_∞ (this is needed for Proposition 7.10). An example where (iii) holds is when K is an imaginary quadratic field (see [45, Lemma 3.1]). Also, (iii) is easily seen to hold if K has only one prime above p.

The above theorems are proven using an up-down approach: to show a relationship between generalized Iwasawa invariants of $X(E_1/\mathbb{L}_\infty)$ and $X(E_2/\mathbb{L}_\infty)$, we formulate using results of [35] an equivalent statement concerning Iwasawa invariants of $X(E_1/K_\infty)$ and $X(E_2/K_\infty)$ where K_∞/K are $\mathbb{Z}_p$-extensions inside $\mathbb{L}_\infty$. We then prove this latter statement using techniques similar to ones used in [20], [28], and [37].

Note that, unlike the former three papers, we do not assume that $E_j(K)[p] = 0$. A key result of Hachimori and Matsuno [23] describing the maximal finite submodule of the Pontryagin dual of $\mathrm{Sel}(E/K_\infty)$ where K_∞/K is a $\mathbb{Z}_p$-extension will allow us to work in the case $E_j(K)[p] \neq 0$.

Remark 1.6. *Assume that the elliptic curves E_1 and E_2 are defined over a subfield K' of K and the isomorphism $E_1[p^i] \cong E_2[p^i]$ in Theorems 1.4 and 1.5 is $\mathrm{Gal}(\bar{K}/K')$-equivariant. Then the proof of Lemma 3.5 reveals that we can replace the condition* (Δ) *by*

Condition (Δ') *: For every prime $\mathfrak{p}$ of K' above p, we have that the inertia subgroup of the extension $K'_\mathfrak{p}(\mu_p)/K'_\mathfrak{p}$ is nontrivial.*

Note that when $K' = \mathbb{Q}$ condition (Δ') *is true. In fact, condition* (Δ') *will be true as soon as p is unramified in K' or if K' is a normal extension of $\mathbb{Q}$ and $p-1$ does not divide the degree of the extension $K'/\mathbb{Q}$.*

Let us briefly summarize the structure of the paper. The article consists of nine sections, including this introduction. In Section 2, we introduce three kinds of Selmer groups which are used in the literature, and we compare these Selmer groups over (multiple) $\mathbb{Z}_p$-extensions of K. Although preliminary in nature, we believe that this overview on relations between the different kinds of Selmer groups is of independent interest. Moreover, we bound the ranks of the maximal finite Λ-submodules of Selmer groups over $\mathbb{Z}_p$-extensions by using the results of Hachimori–Matsuno mentioned above. In Section 3, we explore the property ($\star$) from Definition 1.3, and we prove several control theorems.

The Iwasawa μ- and λ-invariants of Selmer groups over $\mathbb{Z}_p$-extensions are studied in Section 4. These results form the basis of our up-down proof of Theorem 1.4, which is given in Section 5. In Section 6, we describe an alternative proof of Theorem 1.4 which is due to Lim (see [39]). Lim's proof is completely different from ours and relies on asymptotic growth formulas which are due to Cuoco, Monsky, and Perbet. It allows to compare Λ-ranks and μ-invariants of Selmer groups of congruent elliptic curves over (multiple) $\mathbb{Z}_p$-extensions. At the end of Section 6, we show how to derive results on (generalized) λ-invariants from Lim's approach. It turns out that this approach can deal with λ-invariants only under very restrictive assumptions. Therefore, we return to our up-down approach in Section 7, where we present a proof of Theorem 1.5, which works under less restrictive assumptions.

In Section 8, we study the $\mathfrak{M}_H(G)$-property (see also [36]). This notion goes back to work of Coates et al. [6, 9] on noncommutative Iwasawa theory. The validity of a suitable $\mathfrak{M}_H(G)$-property is essential even for the formulation of a main conjecture in noncommutative Iwasawa theory, since it segregates a natural subclass of Iwasawa modules with a sufficiently nice structure theory. Even in the commutative setting of $\mathbb{Z}_p^d$-extensions, there are not many known cases where the property holds, in particular outside of the cyclotomic $\mathbb{Z}_p$-extension. We show that under suitable hypotheses the $\mathfrak{M}_H(G)$-property holds for the Selmer groups of an elliptic curve E if and only if it holds for any elliptic curve E_2 which is congruent to E. We also prove that the $\mathfrak{M}_H(G)$-property holds for a dense subset of $\mathbb{Z}_p$-extensions inside many $\mathbb{Z}_p^d$-extensions $\mathbb{L}_\infty/K$; this result generalizes a result from [36] from dimension 2 to dimension d. In Section 9, we study the maximal pseudo-null submodules of Selmer groups over multiple $\mathbb{Z}_p$-extensions of K. Finally, we end the paper with a section on concrete numerical examples that illustrate Theorems 1.4 and 1.5.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

2. Comparing Selmer groups

In this section, we define various Selmer groups and prove results that compare these different groups. We recall the definition of the classical Selmer group and then define two other Selmer groups which we call the strict and Greenberg Selmer groups. The comparison theorems in this section will allow us to compare results formulated for these different Selmer groups. This is especially important for Theorems 1.4 and 1.5 which are formulated for the classical Selmer group. As it is easier to work with the Greenberg Selmer group rather than the classical Selmer group, we use in the proofs of these theorems our comparison result Corollary 2.4 to change the Selmer group.

In this section, we let E be *any* elliptic curve defined over K and only in this section we let S be *any* finite set of nonarchimedean primes of K containing S_p and all the primes where E has bad reduction. Let K_S be the maximal extension of K unramified outside S and the archimedean primes of K. Suppose now that F/K is a field extension with $K \subseteq F \subseteq K_S$. We let $G_S(F) = \mathrm{Gal}(K_S/F)$ and let S_F, $S_{F,p}$ be the sets of primes of F above those in S, S_p, respectively. For every prime $w \in S_F$, we define a subgroup $H^1_f(F_w, E[p^\infty])$ of $H^1(F_w, E[p^\infty])$ and let

$$H^1_s(F_w, E[p^\infty]) = H^1(F_w, E[p^\infty])/H^1_f(F_w, E[p^\infty]).$$

Define $\mathcal{L}(E/F) = \prod_{w \in S_F} H^1_f(F_w, E[p^\infty])$. The p^∞-Selmer group of E/F attached to this data is defined as

$$0 \longrightarrow \mathrm{Sel}(E/F, \mathcal{L}(E/F)) \longrightarrow H^1(G_S(F), E[p^\infty]) \longrightarrow \prod_{w \in S_F} H^1_s(F_w, E[p^\infty]).$$

We now list various local conditions.

(1) $H^1_{kum}(F_w, E[p^\infty]) = \mathrm{img}(E(F_w) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(F_w, E[p^\infty]))$
Note that because of Mattuck's theorem, we get that $H^1_f(F_w, E[p^\infty]) = 0$ for primes w not dividing p.

(2)
$$H^1_{str}(F_w, E[p^\infty]) = \begin{cases} \ker\left(H^1(F_w, E[p^\infty]) \longrightarrow H^1(F_w, \tilde{E}[p^\infty])\right) & \text{if } w \mid p, \\ 0 & \text{if } w \nmid p. \end{cases}$$
Here, $\tilde{E}$ is the reduced elliptic curve over the residue field.

(3)
$$H^1_{Gr}(F_w, E[p^\infty]) = \begin{cases} \ker\left(H^1(F_w, E[p^\infty]) \longrightarrow H^1(I_w, \tilde{E}[p^\infty])\right) & \text{if } w \mid p, \\ 0 & \text{if } w \nmid p. \end{cases}$$
Here, I_w is the inertia group.

Each of the above local conditions defines a Selmer group:

(1) If F/K is a finite extension, and when $H^1_f(F_w, E[p^\infty]) = H^1_{kum}(F_w, E[p^\infty])$ for all $w \in S_F$ then we denote $\mathrm{Sel}(E/F, \mathcal{L}(E/F))$ by $\mathrm{Sel}(E/F)$. This is the *classical Selmer group* of E/F. If F/K is an infinite extension, then when $H^1_f(F_w, E[p^\infty]) = H^1_{kum}(F_w, E[p^\infty])$ for all $w \in S_F$ we denote $\mathrm{Sel}(E/F, \mathcal{L}(E/F))$ by $\mathrm{Sel}_\infty(E/F)$. For any F/K (finite or infinite), we write $H^1_{kum,s}(F_w, E[p^\infty])$ for $H^1_s(F_w, E[p^\infty])$.

(2) If F/K is a finite extension, then when $H^1_f(F_w, E[p^\infty]) = H^1_{str}(F_w, E[p^\infty])$ for all $w \in S_F$ we denote $\mathrm{Sel}(E/F, \mathcal{L}(E/F))$ by $\mathrm{Sel}^{str}(E/F)$. We call this the *strict Selmer group*. If F/K is an infinite extension, then when $H^1_f(F_w, E[p^\infty]) = H^1_{str}(F_w, E[p^\infty])$ for all $w \in S_F$ we denote $\mathrm{Sel}(E/F, \mathcal{L}(E/F))$ by $\mathrm{Sel}^{str}_\infty(E/F)$. For any F/K (finite or infinite), we write $H^1_{str,s}(F_w, E[p^\infty])$ for $H^1_s(F_w, E[p^\infty])$.

(3) If F/K is a finite extension, then when $H^1_f(F_w, E[p^\infty]) = H^1_{Gr}(F_w, E[p^\infty])$ for all $w \in S_F$ we denote $\mathrm{Sel}(E/F, \mathcal{L}(E/F))$ by $\mathrm{Sel}^{Gr}(E/F)$. We call this the *Greenberg Selmer group* (see [15]). If F/K

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

is an infinite extension, then when $H^1_f(F_w, E[p^\infty]) = H^1_{Gr}(F_w, E[p^\infty])$ for all $w \in S_F$ we denote $\mathrm{Sel}(E/F, \mathcal{L}(E/F))$ by $\mathrm{Sel}^{Gr}_\infty(E/F)$. For any F/K (finite or infinite), we write $H^1_{Gr,s}(F_w, E[p^\infty])$ for $H^1_s(F_w, E[p^\infty])$.

Now let L/K be a p-adic Lie extension with $K \subseteq L \subset K_S$. We define

$$\mathrm{Sel}(E/L) = \varinjlim \mathrm{Sel}(E/F), \quad \mathrm{Sel}^{str}(E/L) = \varinjlim \mathrm{Sel}^{str}(E/F)$$

and

$$\mathrm{Sel}^{Gr}(E/L) = \varinjlim \mathrm{Sel}^{Gr}(E/F)$$

where the direct limits run over all finite extensions F of K contained in L with respect to restriction. We call these, respectively, the classical, strict, and Greenberg Selmer groups.

We denote the Pontryagin duals of $\mathrm{Sel}(E/L)$, $\mathrm{Sel}^{str}(E/L)$, and $\mathrm{Sel}^{Gr}(E/L)$ by $X(E/L)$, $X^{str}(E/L)$, and $X^{Gr}(E/L)$, respectively.

Suppose that F/K is a field extension with $K \subseteq F \subseteq K_S$. Sometimes, $H^1_f(F_w, E[p^\infty])$ for primes $w \nmid p$ is defined as:

$$H^1_{ur}(F_w, E[p^\infty]) = \ker\left(H^1(F_w, E[p^\infty]) \longrightarrow H^1(I_w, E[p^\infty])\right).$$

This is equal to $H^1(\mathrm{Gal}(\overline{F_w}/F_w)/I_w, E[p^\infty]^{I_w})$. If F/K is a $\mathbb{Z}_p^d$-extension and a prime v of K not dividing p does not split completely in F/K, then for any prime w of F above v the pro-p part of $\mathrm{Gal}(\overline{F_w}/F_w)/I_w$ is trivial. Therefore, in this case, we see that we get the same definition of the Selmer group of F/K if we choose $H^1_f(F_w, E[p^\infty])$ to be either zero or $H^1_{ur}(F_w, E[p^\infty])$.

For the rest of this section, we define Ω to be the set of finite extensions F of K inside $\mathbb{L}_\infty$ for a $\mathbb{Z}_p^d$-extension $\mathbb{L}_\infty$ of K. We will compare the three kinds of Selmer groups over $\mathbb{L}_\infty$. First, we have the following important observation.

Lemma 2.1. *We have equalities*

(a) $\mathrm{Sel}(E/\mathbb{L}_\infty) = \mathrm{Sel}_\infty(E/\mathbb{L}_\infty)$,
(b) $\mathrm{Sel}^{str}(E/\mathbb{L}_\infty) = \mathrm{Sel}^{str}_\infty(E/\mathbb{L}_\infty)$,
(c) $\mathrm{Sel}^{Gr}(E/\mathbb{L}_\infty) = \mathrm{Sel}^{Gr}_\infty(E/\mathbb{L}_\infty)$.

Moreover, each of these Selmer groups is independent of the set S.

Proof. We prove (a). The proof of (b) and (c) will be similar. To simplify the notation, we denote $\mathbb{L}_\infty$ by L. From the definitions, we have exact sequences

$$0 \longrightarrow \mathrm{Sel}_\infty(E/L) \longrightarrow H^1(G_S(L), E[p^\infty]) \longrightarrow \prod_{w \in S_L} H^1(L_w, E)[p^\infty],$$

$$0 \longrightarrow \mathrm{Sel}(E/L) \longrightarrow H^1(G_S(L), E[p^\infty]) \longrightarrow \bigoplus_{v \in S} \left(\varinjlim_{F \in \Omega} \bigoplus_{w|v} H^1(F_w, E)[p^\infty] \right),$$

where the direct limit in the last term in the second exact sequence runs over all finite extensions F/K inside L.

Define

$$X := \bigoplus_{v \in S} \left(\varinjlim_{F \in \Omega} \bigoplus_{w|v} H^1(F_w, E)[p^\infty] \right),$$

$$Y := \prod_{w \in S_L} H^1(L_w, E)[p^\infty].$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

To prove the lemma, it will be enough to exhibit an injection $\Xi{:}X \hookrightarrow Y$. To obtain such an injection, we need to show that for any $v \in S$, we have an injection $\Xi_v : X_v \hookrightarrow Y_v$, where $X_v := \varinjlim_{F\in\Omega} \bigoplus_{w|v} H^1(F_w, E)[p^\infty]$ and $Y_v := \prod_{w|v} H^1(L_w, E)[p^\infty]$.

For any $F \in \Omega$, the restriction maps induce a map $\theta_F : \bigoplus_{w|v} H^1(F_w, E)[p^\infty] \longrightarrow \prod_{w|v} H^1(L_w, E)[p^\infty]$. The maps $\{\theta_F\}_{F\in\Omega}$ are compatible under restriction and hence from the universal property of the direct limit we have a homomorphism $\Xi_v : X_v \longrightarrow Y_v$. We now show that Ξ_v is an injection.

Assume that $x \in \ker \Xi_v$. We have that for some $F \in \Omega$, $x = \alpha_F(x_F)$ where $x_F \in \bigoplus_{w|v} H^1(F_w, E)[p^\infty]$ and $\alpha_F : \bigoplus_{w|v} H^1(F_w, E)[p^\infty] \longrightarrow X_v$ is the map into the direct limit. Since $\Xi_v \circ \alpha_F = \theta_F$, we have that $\theta_F(x_F) = 0$.

Write $x_F = (z_w)$ where the component z_w is contained in $H^1(F_w, E)[p^\infty]$. Let w be a prime of F above v. Choose a prime w' of L above w. Since $\theta_F(x_F) = 0$, it follows that $\mathrm{res}_{L_{w'}}(z_w) = 0$, where

$$\mathrm{res}_{L_{w'}} : H^1(F_w, E)[p^\infty] \longrightarrow H^1(L_{w'}, E)[p^\infty]$$

is the restriction map. It is well known that we have $H^1(L_{w'}, E) = \varinjlim_{\tilde{F}\in\Omega} H^1(\tilde{F}_{w'}, E)$, where for $\tilde{F} \in \Omega$, $\tilde{F}_{w'}$ means the completion of $\tilde{F}$ at the prime of $\tilde{F}$ below w'. Hence, $H^1(L_{w'}, E)[p^\infty] = \varinjlim_{\tilde{F}\in\Omega} H^1(\tilde{F}_{w'}, E)[p^\infty]$. Therefore from this and the fact that $\mathrm{res}_{L_{w'}}(z_w) = 0$, we see that there exists $F^{(w)} \in \Omega$ that is Galois over F with $\mathrm{res}_{(F^{(w)})_{w'}}(z_w) = 0$, where $\mathrm{res}_{(F^{(w)})_{w'}} : H^1(F_w, E)[p^\infty] \longrightarrow H^1((F^{(w)})_{w'}, E)[p^\infty]$ is the restriction map.

Since $F^{(w)}$ is Galois over F, if $\tilde{w}$ is any prime of $F^{(w)}$ above w, then the completion $(F^{(w)})_{\tilde{w}}$ is equal to $(F^{(w)})_{w'}$. Therefore, for any prime $\tilde{w}$ of $F^{(w)}$ above w we have $\mathrm{res}_{(F^{(w)})_{\tilde{w}}}(z_w) = 0$.

Now let F' be the composite of the fields $F^{(w)}$ where w runs over all primes of F above v. Then we see that $\beta_{F,F'}(x_F) = 0$, where $\beta_{F,F'} : \bigoplus_{w|v} H^1(F_w, E)[p^\infty] \longrightarrow \bigoplus_{w|v} H^1(F'_w, E)[p^\infty]$ is the map coming from restriction in each component. Therefore, $x = \alpha_F(x_F) = 0$ and hence $\ker \Xi_v = 0$.

Finally, to prove that each of the Selmer groups in the statement of the lemma is independent of the set S, we only need to show that this result is true if $\mathbb{L}_\infty$ is replaced with $F \in \Omega$. To this end, let $F \in \Omega$ and let S be any finite set of nonarchimedean primes of K containing S_p and all the primes where E has bad reduction. By [44, Proposition I-6.5], we have an exact sequence

$$0 \longrightarrow H^1(G_S(F), E[p^\infty]) \longrightarrow H^1(F, E[p^\infty]) \longrightarrow \prod_{w\notin S_F} H^1(F_w, E)[p^\infty]. \tag{3}$$

We should note that loc. cit. assumes that S_F contains all archimedean primes of F. For any archimedean prime w of F, we have $H^1(F_w, E[p^\infty]) = 0$ because p is odd. Also recall from the beginning of this section that we defined K_S to be the maximal extension of K unramified outside S and the archimedean primes of K. Thus, we do in fact have an exact sequence (3).

Let $\bullet \in \{kum, str, Gr\}$. We now show that $\mathrm{Sel}^\bullet(E/F)$ is independent of the set S, where $\mathrm{Sel}^{kum}(E/F) = \mathrm{Sel}(E/F)$. For $\bullet = kum$, this is proven in [44, Corollary I-6.6]. We can easily now adapt the proof to also work for the strict and Greenberg Selmer groups. Consider the exact sequence

$$H^1(F, E[p^\infty]) \xrightarrow{\theta} \prod_{\text{all } w} H^1_{\bullet,s}(F_w, E[p^\infty]) \xrightarrow{\pi} \prod_{w\notin S_F} H^1_{\bullet,s}(F_w, E[p^\infty]). \tag{4}$$

In the above sequence, θ is the localization map and π is just the projection. This sequence of maps induces an exact sequence

$$0 \longrightarrow \ker\theta \longrightarrow \ker\pi\circ\theta \longrightarrow \ker\pi. \tag{5}$$

If $w \notin S_F$, then in particular w does not divide p. By Mattuck's theorem $E(F_w) \cong \mathbb{Z}_l^d \times T$, where l is the residue characteristic of F_w, $d = [F_w : \mathbb{Q}_l]$ and T is a finite group. Since $l \neq p$, we have $E(F_w) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ and so

$$H^1_{\bullet,s}(F_w, E[p^\infty]) = H^1(F_w, E[p^\infty]) = H^1(F_w, E)[p^\infty].$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Taking this into account, we get from (3) that $\ker \pi \circ \theta = H^1(G_S(F), E[p^\infty])$. Therefore, we get from (5) an exact sequence

$$0 \longrightarrow \ker \theta \longrightarrow H^1(G_S(F), E[p^\infty]) \longrightarrow \prod_{w \in S_F} H^1_{\bullet,s}(F_w, E[p^\infty]).$$

So $\ker \theta = \mathrm{Sel}^\bullet(E/F)$. Since $\ker \theta$ does not depend on the set S, the Selmer group $\mathrm{Sel}^\bullet(E/F)$ is independent of the set S. □

We will use the equalities in the previous lemma throughout the paper without reference. In what follows, let $\mathbb{L}_\infty/K$ be an arbitrary, but fixed $\mathbb{Z}_p^d$-extension.

Proposition 2.2. *We have an equality* $\mathrm{Sel}^{Gr}(E/\mathbb{L}_\infty) = \mathrm{Sel}^{str}(E/\mathbb{L}_\infty)$.

Proof. To prove the proposition, it will clearly suffice to show that for any $F \in \Omega$ we have $\mathrm{Sel}_p{}^{Gr}(E/F) = \mathrm{Sel}_p{}^{str}(E/F)$. Let $F \in \Omega$ and consider the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}^{str}(E/F) & \longrightarrow & H^1(G_S(F), E[p^\infty]) & \xrightarrow{\lambda_F} & \bigoplus_{w \in S_F} H^1_{str;s}(F_w, E[p^\infty]) \\
 & & \downarrow \iota & & \| & & \downarrow \alpha \\
0 & \longrightarrow & \mathrm{Sel}^{Gr}(E/F) & \longrightarrow & H^1(G_S(F), E[p^\infty]) & \longrightarrow & \bigoplus_{w \in S_F} H^1_{Gr,s}(F_w, E[p^\infty])
\end{array}$$

Applying the snake lemma to the above diagram, we get an exact sequence

$$0 \longrightarrow \mathrm{Sel}^{str}(E/F) \xrightarrow{\iota} \mathrm{Sel}^{Gr}(E/F) \longrightarrow \mathrm{im}\lambda_F \cap \ker \alpha \longrightarrow 0.$$

Therefore to prove the result, it will suffice to show that $\ker \alpha = 0$. It is easy to see that we have an injection $\ker \alpha \hookrightarrow \bigoplus_{w \in S_{F,p}} H^1(\mathfrak{h}_{F,w}, \tilde{E}[p^\infty])$, where $\mathfrak{h}_{F,w} = \mathrm{Gal}(\overline{F_w}/F_w)/I_w$ and I_w is the inertia subgroup.

As the residue field of F_w is finite, $\mathfrak{h}_{F,w}$ acts nontrivially on $\tilde{E}[p^\infty]$. Now,

$$H^1(\mathfrak{h}_{F,w}, \tilde{E}[p^\infty]) = \tilde{E}[p^\infty]/(g-1)\tilde{E}[p^\infty]$$

where g is a topological generator of $\mathfrak{h}_{F,w}$. Since $\tilde{E}[p^\infty]$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ and $\mathfrak{h}_{F,w}$ acts nontrivially on it, it follows that $\tilde{E}[p^\infty]/(g-1)\tilde{E}[p^\infty] = 0$. So, $H^1(\mathfrak{h}_{F,w}, \tilde{E}[p^\infty]) = 0$ as desired. □

Proposition 2.3. *The following assertions hold.*

(a) If F/K is a finite subextension of $\mathbb{L}_\infty/K$ and $w \in S_{F,p}$, we let k_{F_w} denote the residue field of F_w. We have an inclusion map $\iota : \mathrm{Sel}(E/\mathbb{L}_\infty) \longrightarrow \mathrm{Sel}^{str}(E/\mathbb{L}_\infty)$ and an embedding

$$\theta : \mathrm{coker}\iota \hookrightarrow \Big(\varprojlim_{F \in \Omega} \bigoplus_{w \in S_{F,p}} \tilde{E}(k_{F_w})[p^\infty] \Big)^\vee,$$

where the inverse limit is taken with respect to corestriction.

(b) If $X(E/\mathbb{L}_\infty)$ is Λ_d-torsion and $E(\mathbb{L}_\infty)[p^\infty]$ is finite, then θ is an isomorphism.

(c) If every prime in S_p ramifies in $\mathbb{L}_\infty/K$, then $\mathrm{Sel}(E/\mathbb{L}_\infty) = \mathrm{Sel}^{str}(E/\mathbb{L}_\infty)$.

(d) $X(E/\mathbb{L}_\infty)$ is a finitely generated Λ_d-torsion module if and only if $X^{str}(E/\mathbb{L}_\infty)$ is a finitely generated Λ_d-torsion module.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Proof. By the discussion in [7, pg. 152–153], we have for any finite extension F/K inside $\mathbb{L}_\infty$ and $w \in S_{F,p}$ that $H^1_{kum}(F_w, E[p^\infty]) \subseteq H^1_{str}(F_w, E[p^\infty])$. Therefore, we have an inclusion

$$\iota : \mathrm{Sel}(E/\mathbb{L}_\infty) \longrightarrow \mathrm{Sel}^{str}(E/\mathbb{L}_\infty).$$

Let S_∞ be the set of primes of $\mathbb{L}_\infty$ above those in S. We have the following commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}(E/\mathbb{L}_\infty) & \longrightarrow & H^1(G_S(\mathbb{L}_\infty), E[p^\infty]) & \xrightarrow{\lambda_\infty} & \varinjlim_{F\in\Omega} \bigoplus_{w\in S_F} H^1_{kum,s}(F_w, E[p^\infty]) \\
 & & \downarrow \iota & & \| & & \downarrow \alpha \\
0 & \longrightarrow & \mathrm{Sel}^{str}(E/\mathbb{L}_\infty) & \longrightarrow & H^1(G_S(\mathbb{L}_\infty), E[p^\infty]) & \longrightarrow & \varinjlim_{F\in\Omega} \bigoplus_{w\in S_F} H^1_{str,s}(F_w, E[p^\infty])
\end{array}$$

Applying the snake lemma to the above diagram, we get an exact sequence

$$0 \longrightarrow \mathrm{Sel}(E/\mathbb{L}_\infty) \xrightarrow{\iota} \mathrm{Sel}^{str}(E/\mathbb{L}_\infty) \longrightarrow \mathrm{img}\lambda_\infty \cap \ker\alpha \longrightarrow 0.$$

We have an isomorphism

$$\ker\alpha \cong \varinjlim_{F\in\Omega} \bigoplus_{w\in S_F} H^1_{str}(F_w, E[p^\infty])/H^1_{kum}(F_w, E[p^\infty]).$$

Let $F \in \Omega$ and let $w \in S_{F,p}$. Let $C_w = \mathcal{F}(\bar{\mathfrak{m}})[p^\infty]$ where $\bar{\mathfrak{m}}$ is the maximal ideal of $\overline{F_w}$ and $\mathcal{F}$ is the formal group of E. First, we note that Tate local duality [47, Theorem 7.2.6] together with the Weil pairing yields a non-degenerate pairing

$$\langle\ ,\ \rangle : H^2(F_w, T_p(C_w)) \times H^0(F_w, \tilde{E}[p^\infty]) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

where $T_p(C_w)$ is the p-adic Tate module of C_w. If F'_w/F_w is a finite extension, let

$$\mathrm{res} : H^2(F_w, T_p(C_w)) \longrightarrow H^2(F'_w, T_p(C_w))$$

be the restriction map and let $\mathrm{cor} : H^0(F'_w, \tilde{E}[p^\infty]) \longrightarrow H^0(F_w, \tilde{E}[p^\infty])$ be the corestriction (norm) map. For $a \in H^2(F_w, T_p(C_w))$ and $b \in H^0(F'_w, \tilde{E}[p^\infty])$, a property of Tate local duality gives $\langle \mathrm{res}a, b\rangle = \langle a, \mathrm{cor}b\rangle$. We have maps

$$\kappa_{F_w} : E(F_w) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(F_w, E[p^\infty]),$$

$$\lambda_{F_w} : H^1(F_w, C_w) \longrightarrow H^1(F_w, E[p^\infty]).$$

Taking into account [7, Proposition 4.5], the proof of [7, Proposition 4.6] shows that we have an isomorphism $\theta_{F_w} : \mathrm{img}\lambda_{F_w}/\mathrm{img}\kappa_{F_w} \xrightarrow{\sim} (\tilde{E}(k_{F_w})[p^\infty])^\vee$ where k_{F_w} is the residue field of F_w. Consider the exact sequence

$$0 \longrightarrow C_w \longrightarrow E[p^\infty] \longrightarrow \tilde{E}[p^\infty] \longrightarrow 0.$$

From this exact sequence, we see that $\mathrm{img}\lambda_{F_w} = H^1_{str}(F_w, E[p^\infty])$. Therefore, taking into account the property of Tate local duality above and the description of the map θ_{F_w}, we have an isomorphism

$$\varinjlim_{F\in\Omega} \bigoplus_{w\in S_{F,p}} \mathrm{img}\lambda_{F_w}/\mathrm{img}\kappa_{F_w} \cong \left(\varprojlim_{F\in\Omega} \bigoplus_{w\in S_{F,p}} \tilde{E}(k_{F_w})[p^\infty] \right)^\vee.$$

The direct limits are taken with respect to restriction and inverse limits are taken with respect to corestriction. This proves (a).

If $X(E/\mathbb{L}_\infty)$ is Λ_d-torsion and $E(\mathbb{L}_\infty)[p^\infty])$ is finite, then by [25, Theorem 7.2] the map λ_∞ in the commutative diagram above is surjective. Therefore by the proof of part (a), we see that θ is an isomorphism. This proves (b).

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

For part (c), we note that if L'_w/L_w is a finite totally ramified extension, then the norm map from $\tilde{E}(k_{L'_w})[p^\infty]$ to $\tilde{E}(k_{L_w})[p^\infty]$ is multiplication by $[L'_w : L_w]$. Therefore, if every prime in S_p ramifies in $\mathbb{L}_\infty/K$, we see from this that $(\varprojlim_{F\in\Omega} \bigoplus_{w\in S_{F,p}} \tilde{E}(k_{F_w})[p^\infty])^\vee = 0$ and so $\mathrm{Sel}(E/\mathbb{L}_\infty) = \mathrm{Sel}^{str}(E/\mathbb{L}_\infty)$. Alternatively, (c) follows from [7, Prop. 4.3].

From (a), we see that to prove (d), we only have to show that the Pontryagin dual of $A := \left(\varprojlim_{F\in\Omega} \bigoplus_{w\in S_{F,p}} \tilde{E}(k_{F_w})[p^\infty]\right)^\vee$ is a finitely generated Λ_d-torsion module. For $v \in S_p$, we let $B_v := \left(\varprojlim_{F\in\Omega} \bigoplus_{w|v} \tilde{E}(k_{F_w})[p^\infty]\right)^\vee$ where the direct sum ranges over all primes w of $F \in \Omega$ dividing v. To show that $A^\vee$ is a finitely generated torsion Λ_d-module, it suffices to show that for any $v \in S_p$ the Λ_d-module $(B_v)^\vee$ is finitely generated torsion. Let $v \in S_p$ and let $G = \mathrm{Gal}(\mathbb{L}_\infty/K)$. By Shapiro's lemma, we have $(B_v)^G \cong \left(\left(\varprojlim_{F\in\Omega} \tilde{E}(k_{F_w})[p^\infty]\right)^\vee\right)^{G_w}$ where w is some prime of $\mathbb{L}_\infty$ above v and G_w is the decomposition group. As $\varprojlim \tilde{E}(k_{F_w})[p^\infty]$ is a pro-p procyclic group, it is a quotient of $\mathbb{Z}_p$ (see [51, Proposition 2.7.1]). Therefore, $(B_v)^G$ is cofinitely generated over $\mathbb{Z}_p$, and so $(B_v)^\vee$ is a finitely generated Λ_d-module.

To prove that $(B_v)^\vee$ is a torsion Λ_d-module, we consider two cases. First assume that v splits completely in $\mathbb{L}_\infty/K$. Let w be a prime of $\mathbb{L}_\infty$ above v. Then $\varprojlim \tilde{E}(k_{F_w})[p^\infty] = \tilde{E}(k_{K_v})[p^\infty]$ is finite. Therefore, some power of p annihilates B_v whence $(B_v)^\vee$ is a torsion Λ_d-module.

Now assume that v does not split completely in $\mathbb{L}_\infty/K$. Choose some $\mathbb{Z}_p$-extension K_∞/K inside $\mathbb{L}_\infty$ where v does not split completely and let $H = \mathrm{Gal}(\mathbb{L}_\infty/K_\infty)$. Let T be the set of primes of K_∞ above v. Then by Shapiro's lemma it follows that $(B_v)^H \cong \left(\left(\varprojlim_{F\in\Omega} \bigoplus_{w\in T} \tilde{E}(k_{F_w})[p^\infty]\right)^\vee\right)^{H_w}$ where for each $w \in T$ we have also written w for a fixed prime of $\mathbb{L}_\infty$ and H_w is the decomposition group. Since the set T is finite, we see that $(B_v)^H$ is cofinitely generated over $\mathbb{Z}_p$. Therefore, $(B_v)^\vee$ is finitely generated over $\mathbb{Z}_p[[H]]$ whence it is a torsion Λ_d-module. □

Recall the notion of $\mathcal{E}_p$ from Definition 1.2. From Propositions 2.2 and 2.3, we get

Corollary 2.4. *Assume that $\mathcal{E}_p \neq \emptyset$. Then*

$$\mathrm{Sel}(E/\mathbb{L}_\infty) = \mathrm{Sel}^{str}(E/\mathbb{L}_\infty) = \mathrm{Sel}^{Gr}(E/\mathbb{L}_\infty).$$

Definition 2.5. *For an abelian group G, we define its p-rank as*

$$r_p(G) = \dim_{\mathbb{F}_p}(G[p]).$$

Under certain conditions, we will need to bound the p-rank of the maximal finite Λ-submodule of $X^{Gr}(E/K_\infty)$ as K_∞ runs over the set $\mathcal{E}$. To achieve this, we use the result of Hachimori–Matsuno [23] to bound the order of the maximal finite submodule of $X(E/K_\infty)$. First, we need

Lemma 2.6. *Let $K_\infty \in \mathcal{E}$. We write $\Gamma = \mathrm{Gal}(K_\infty/K)$, and we let $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$ for each $n \in \mathbb{N}$. Let $s_n : \mathrm{Sel}(E/K_n) \longrightarrow \mathrm{Sel}(E/K_\infty)^{\Gamma_n}$ be the map induced by restriction. Then $\ker s_n$ is finite with $r_p(\ker s_n) \leq 2$, and the order of $\ker s_n$ is bounded as n varies.*

Proof. For any n, consider the restriction map

$$g_n : H^1(G_S(K_n), E[p^\infty]) \longrightarrow H^1(G_S(K_\infty), E[p^\infty])^{\Gamma_n}.$$

Since $\ker s_n$ injects into $\ker g_n$, it will suffice to prove the desired result for $\ker g_n$ instead. We have $\ker g_n = H^1(\Gamma_n, E(K_\infty)[p^\infty])$. Let $W = E(K_\infty)[p^\infty]$. If γ is a topological generator of $\mathrm{Gal}(K_\infty/K) = \Gamma$, then $\ker g_n = W/(\gamma^{p^n} - 1)W$. The kernel of $\gamma^{p^n} - 1$ acting on W is $E(K_n)[p^\infty]$ which is finite.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Let W_{div} be the maximal divisible subgroup of W. Since W_{div} has finite $\mathbb{Z}_p$-corank and the kernel of $\gamma^{p^n} - 1$ acting on W is finite, it follows that $(\gamma^{p^n} - 1)W_{\text{div}} = W_{\text{div}}$. Therefore, we see that we have a surjection $W/W_{\text{div}} \twoheadrightarrow \ker g_n$. This shows that $|\ker g_n|$ is bounded by $[W : W_{\text{div}}]$ and also that

$$r_p(\ker g_n) \leq r_p(W/W_{\text{div}}) \leq 2. \qquad \square$$

Definition 2.7. *If $K_\infty \in \mathcal{E}$, we denote the maximal finite Λ-submodule of $X(E/K_\infty)$ (resp. $X^{Gr}(E/K_\infty)$) by $\mathfrak{X}(E/K_\infty)$ (resp. $\mathfrak{X}^{Gr}(E/K_\infty)$).*

Now, we have the following important theorem

Theorem 2.8 (Hachimori–Matsuno [23]). *Suppose that $K_\infty \in \mathcal{E}$ and that $X(E/K_\infty)$ is Λ-torsion. Then $\mathfrak{X}(E/K_\infty)$ is isomorphic to $\varprojlim \ker s_n$ where $s_n : \text{Sel}(E/K_n) \longrightarrow \text{Sel}(E/K_\infty)^{\Gamma_n}$ and the inverse limit is taken with respect to the corestriction maps.*

From Theorem 2.8 and Lemma 2.6, we have

Proposition 2.9. *For all $K_\infty \in \mathcal{E}$ with $X(E/K_\infty)$ Λ-torsion, we have $r_p(\mathfrak{X}(E/K_\infty)) \leq 2$.*

Proof. Let $K_\infty \in \mathcal{E}$ with $X(E/K_\infty)$ Λ-torsion. Let

$$s_n : \text{Sel}(E/K_n) \longrightarrow \text{Sel}(E/K_\infty)^{\Gamma_n}$$

and let $A_n := \ker s_n$. From Lemma 2.6, we know that A_n is finite with bounded order as n varies. For any n, consider the exact sequence $A_n \xrightarrow{\times p} A_n \longrightarrow A_n/p \longrightarrow 0$. Since A_n/p is finite, it follows by taking inverse limits with respect to corestriction that we have an exact sequence (see [51, Lemma 1.1.5])

$$\varprojlim A_n \xrightarrow{\times p} \varprojlim A_n \longrightarrow \varprojlim (A_n/p) \longrightarrow 0.$$

Taking Theorem 2.8 into account, the above exact sequence implies

$$\mathfrak{X}(E/K_\infty)/p \cong (\varprojlim A_n)/p \cong \varprojlim (A_n/p).$$

By Lemma 2.6, for any n, we have $\dim_{\mathbb{F}_p}(A_n/p) \leq 2$. From this, it follows that the inverse system coming from the groups A_n/p is Mittag-Leffler. For any $i \in \mathbb{N}$ let $B_i \subseteq A_i/p$ be the stable image of $\overline{\text{cor}}(A_j/p)$ for $j \geq i$ where $\overline{\text{cor}}$ is the map induced by corestriction. Then $\varprojlim (A_n/p) = \varprojlim B_n$. By the choice of the groups B_i, the inverse system coming from these groups has surjective maps. As each B_i is finite, therefore for some $N \geq 0$ we have for $j \geq i \geq N$ that the map $\overline{\text{cor}} : B_j \longrightarrow B_i$ is an isomorphism. Then $\varprojlim B_n \cong B_N$. Whence we have

$$\dim_{\mathbb{F}_p}(\varprojlim B_n) = \dim_{\mathbb{F}_p}(B_N) \leq \dim_{\mathbb{F}_p}(A_N/p) \leq 2.$$

This completes the proof. $\square$

Proposition 2.10. *Assume that $E(\mathbb{L}_\infty)[p^\infty]$ is finite and that the decomposition subgroups $D_v(\mathbb{L}_\infty/K) \subseteq \text{Gal}(\mathbb{L}_\infty/K)$ are open for each $v \mid p$. Then there exists a constant $C^{Gr} \geq 0$ such that for all $K_\infty \in \mathcal{E}$ with $X^{Gr}(E/K_\infty)$ Λ-torsion we have $r_p(\mathfrak{X}^{Gr}(E/K_\infty)) \leq C^{Gr}$.*

Proof. Let t be the number of primes of $\mathbb{L}_\infty$ above p. We claim that $C^{Gr} = t + 2$ has the required property. Let $K_\infty \in \mathcal{E}$ be such that $X^{Gr}(E/K_\infty)$ is Λ-torsion. Propositions 2.2 and 2.3 hold for any $\mathbb{Z}_p^d$-extension $\mathbb{L}_\infty/K$. Applying them to the $\mathbb{Z}_p$-extension K_∞/K, we see that $X(E/K_\infty)$ is Λ-torsion. Therefore, by Proposition 2.9 $r_p(\mathfrak{X}(E/K_\infty)) \leq 2$.

By Propositions 2.2 and 2.3, we have a surjection

$$\Psi : X^{Gr}(E/K_\infty) \twoheadrightarrow X(E/K_\infty).$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Therefore, we have an exact sequence

$$0 \longrightarrow \mathfrak{X}^{Gr}(E/K_\infty) \cap \ker \Psi \longrightarrow \mathfrak{X}^{Gr}(E/K_\infty) \longrightarrow \mathfrak{X}(E/K_\infty) \longrightarrow 0.$$

From this exact sequence and the fact that $r_p(\mathfrak{X}(E/K_\infty)) \leq 2$, we see that to show that $r_p(\mathfrak{X}^{Gr}(E/K_\infty)) \leq t+2$ it will suffice to show that $r_p(\ker \Psi) \leq t$.

With the notation of Proposition 2.3 let

$$A := \left(\varprojlim_{F \in \Omega} \bigoplus_{w \in S_{F,p}} \tilde{E}(k_{F_w})[p^\infty] \right)^\vee .$$

It is easy to see that $\dim_{\mathbb{F}_p}(A/p) \leq t$. This fact together with Propositions 2.2 and 2.3 implies that $r_p(\ker \Psi) \leq t$. This completes the proof. □

Remark 2.11. *The main tool needed to prove Theorem 2.8 of Hachimori–Matsuno is the Cassels–Tate pairing for the classical Selmer group:*

$$\mathrm{Sel}(E/K_n) \times \mathrm{Sel}(E/K_n) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

Here K_n is any tower field of our $\mathbb{Z}_p$-extension K_∞/K. In Li Guo's paper [21], a slightly modified version of $\mathrm{Sel}^{str}(E/K_n)$ is defined which we denote by $\mathrm{Sel}^{str*}(E/K_n)$. loc. cit. defines a pairing:

$$\mathrm{Sel}^{str*}(E/K_n) \times \mathrm{Sel}^{str*}(E/K_n) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

With this pairing, one can prove the analog of the Hachimori–Matsuno result for $\varinjlim \mathrm{Sel}^{str*}(E/K_n)$. We need to impose some conditions in order to get $\varinjlim \mathrm{Sel}^{str*}(E/K_n) = \mathrm{Sel}^{str}(E/K_\infty)$. Therefore to avoid additional hypotheses, we have proven Proposition 2.10 using Propositions 2.9, 2.2 and 2.3.

3. Results on $\mathrm{Sel}^{Gr}(E/K_\infty)$ for $K_\infty \in \mathcal{E}$

In this section, we prove some important results on $\mathrm{Sel}_p{}^{Gr}(E/K_\infty)$ for $K_\infty \in \mathcal{E}$. Let E be either E_1 or E_2. Recall from the introduction that S is a finite set of nonarchimedean primes of K containing S_p and all the primes where either E_1 or E_2 has bad reduction. Suppose now that F is a field with $K \subseteq F \subseteq K_S$.

For a prime $v \in S \setminus S_p$, we define

$$\mathcal{H}_v(E/F) = \prod_{w|v} H^1(F_w, E[p^\infty])$$

where the sum is over all primes w dividing v.

Proposition 3.1. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Assume that $v \notin S_p$ does not split completely in K_∞/K. Then $\mathcal{H}_v(E/K_\infty)^\vee$ is a finitely generated free $\mathbb{Z}_p$-module with $\mathrm{rank}_{\mathbb{Z}_p}(\mathcal{H}_v(E/K_\infty)^\vee) \leq 2n$ where n is the number of primes of K_∞ above v.*

Proof. Let w be a prime of K_∞ above v. First, we show that $H^1(K_{\infty,w}, E[p^\infty])$ is divisible. Since v does not split completely in K_∞/K, it follows from [47, Theorem 7.1.8(i)] that $cd_p(K_{\infty,w}) \leq 1$. The exact sequence $0 \longrightarrow E[p] \longrightarrow E[p^\infty] \xrightarrow{\times p} E[p^\infty] \longrightarrow 0$ induces an exact sequence

$$H^1(K_{\infty,w}, E[p^\infty]) \xrightarrow{\times p} H^1(K_{\infty,w}, E[p^\infty]) \longrightarrow H^2(K_{\infty,w}, E[p]).$$

The last term is zero because $cd_p(K_{\infty,w}) \leq 1$ whence $H^1(K_{\infty,w}, E[p^\infty])$ is divisible.

Let $B = \mathrm{Hom}_{\mathbb{Z}_p}(T_p(E[p^\infty]), \mu_{p^\infty})$ where $T_p(E[p^\infty])$ is the p-adic Tate module of $E[p^\infty]$ and μ_{p^∞} is the group of p-power roots of unity. By [15, Proposition 2], $H^1(K_{\infty,w}, E[p^\infty])$ is cofinitely generated over $\mathbb{Z}_p$ with $\mathrm{corank}_{\mathbb{Z}_p}(H^1(K_{\infty,w}, E[p^\infty])) = \mathrm{corank}_{\mathbb{Z}_p}(H^0(K_{\infty,w}, B))$. By the Weil pairing $B \cong E[p^\infty]$ and therefore $\mathrm{corank}_{\mathbb{Z}_p}(H^1(K_{\infty,w}, E[p^\infty])) = \mathrm{corank}_{\mathbb{Z}_p}(E(K_{\infty,w})[p^\infty])$. This completes the proof. □

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Proposition 3.2. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Let $v \notin S_p$. Then the following two assertions hold true.*

(i) If E has additive reduction at v and $p \geq 5$, then $\mathcal{H}_v(E/K_\infty) = 0$.
(ii) If E has multiplicative reduction at v, $p \nmid c_v$ and $p \nmid \#k_v^\times$ where k_v is the residue field of K_v, then $\mathcal{H}_v(E/K_\infty) = 0$.

Proof. Let w be a prime of K_∞ above v. If v does not split completely in K_∞/K, then $K_{\infty,w}/K_v$ is a $\mathbb{Z}_p$-extension. Let $\Gamma_w = \mathrm{Gal}(K_{\infty,w}/K_v)$. Then $cd_p(\Gamma_w) = 1$ and so we get a surjection

$$H^1(K_v, E[p^\infty]) \twoheadrightarrow H^1(K_{\infty,w}, E[p^\infty])^{\Gamma_w}.$$

Since Γ_w is pro-p, we see that to show that $H^1(K_{\infty,w}, E[p^\infty]) = 0$, it will suffice to show that $H^1(K_v, E[p^\infty]) = 0$. If v splits completely in K_∞/K, then $H^1(K_{\infty,w}, E[p^\infty]) = H^1(K_v, E[p^\infty])$. Therefore, we see that in either case that we must show that $H^1(K_v, E[p^\infty]) = 0$.

By Mattuck's Theorem, we have that $E(K_v) \cong \mathbb{Z}_l^d \times T$, where l is the residue characteristic of K_v, $d = [K_v : \mathbb{Q}_l]$ and T is a finite group. Since $l \neq p$, we have $E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ and so $H^1(K_v, E[p^\infty]) = H^1(K_v, E)[p^\infty]$. By Tate duality for abelian varieties over local fields [44, Corollary I-3.4], we have an isomorphism $H^1(K_v, E)^\vee \cong E(K_v)$. Therefore, $(H^1(K_v, E)[p^\infty])^\vee \cong \varprojlim E(K_v)/p^n E(K_v)$. Since $E(K_v) \cong \mathbb{Z}_l^d \times T$ and $l \neq p$, we have that $\varprojlim E(K_v)/p^n E(K_v)$ is just the (finite) p-primary subgroup of $E(K_v)$. It follows from the previous facts that $H^1(K_v, E[p^\infty])$ is isomorphic to $E(K_v)[p^\infty]$ and so we only need to show that $E(K_v)[p^\infty] = 0$.

Assume that E has additive reduction at v and p and $p \geq 5$. Let $E_0(K_v)$ be the group of points of $E(K_v)$ of nonsingular reduction. Since $p \geq 5$, by [57, pg. 448] the cardinality of $E(K_v)/E_0(K_v)$ is prime to p. Therefore, $E(K_v)[p^\infty] = E_0(K_v)[p^\infty]$. Let $\hat{E}$ be the formal group of E/K_v and $\mathfrak{m}_v$ the maximal ideal of O_v (the ring of integers of K_v). Since $v \nmid p$, $\hat{E}(\mathfrak{m}_v)$ has no elements of order p and so $E(K_v)[p^\infty] = E_0(K_v)[p^\infty]$ injects into the set $\tilde{E}_{ns}(k_v)$ of nonsingular points of the reduction of E modulo the residue field k_v. But as E has additive reduction at v we have $\tilde{E}_{ns}(k_v) \cong k_v$. Since k_v has no points of order p (because $v \nmid p$), we see that $E(K_v)[p^\infty] = 0$. This proves (i).

Now assume that E has multiplicative reduction at v, $p \nmid c_v$ and $p \nmid \#k_v^\times$. Since $p \nmid c_v$, $\#E(K_v)/E_0(K_v)$ is prime to p and so $E(K_v)[p^\infty] = E_0(K_v)[p^\infty]$. As above we have that $E(K_v)[p^\infty] = E_0(K_v)[p^\infty]$ injects into $\tilde{E}_{ns}(k_v)$. As E has multiplicative reduction at v, $\tilde{E}_{ns}(k_v) \cong k_v^\times$. Since $p \nmid \#k_v^\times$ by assumption, we can conclude that $E(K_v)[p^\infty] = 0$. This proves (ii). □

Let K_∞/K be a $\mathbb{Z}_p$-extension. Let S_{K_∞} (resp. $S_{K_{\infty,p}}$) be the sets of primes of K_∞ above those in S (resp. S_p). We now define the "non-primitive" Greenberg Selmer group as

$$0 \longrightarrow \mathrm{Sel}^{Gr(p)}(E/K_\infty) \longrightarrow H^1(G_S(K_\infty), E[p^\infty]) \longrightarrow \prod_{w \in S_{K_{\infty,p}}} H^1_{Gr,s}(K_{\infty,w}, E[p^\infty]). \tag{6}$$

We will denote the Pontryagin dual of $\mathrm{Sel}^{Gr(p)}(E/K_\infty)$ by $X^{Gr(p)}(E/K_\infty)$. We now define the reduced Greenberg Selmer groups and reduced non-primitive Greenberg Selmer groups. To define these, we first define the reduced local conditions. For $i \in \mathbb{N}$, we define

$$H^1_{Gr}(K_{\infty,w}, E[p^i]) = \begin{cases} \ker\left(H^1(K_{\infty,w}, E[p^i]) \longrightarrow H^1(I_w, \tilde{E}[p^i])\right) & \text{if } w \mid p, \\ 0 & \text{if } w \nmid p. \end{cases}$$

For any prime w of K_∞, we define

$$H^1_{Gr,s}(K_{\infty,w}, E[p^i]) = H^1(K_{\infty,w}, E[p^i])/H^1_{Gr}(K_{\infty,w}, E[p^i]).$$

We define

$$0 \longrightarrow \mathrm{Sel}^{Gr}(E[p^i]/K_\infty) \longrightarrow H^1(G_S(K_\infty), E[p^i]) \longrightarrow \prod_{w \in S_{K_\infty}} H^1_{Gr,s}(K_{\infty,w}, E[p^i]),$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

$$0 \longrightarrow \mathrm{Sel}^{Gr(p)}(E[p^i]/K_\infty) \longrightarrow H^1(G_S(K_\infty), E[p^i]) \longrightarrow \prod_{w \in S_{K_\infty,p}} H^1_{Gr,s}(K_{\infty,w}, E[p^i]).$$

Recall from Definition 2.5 that for an abelian group G, we define its p-rank as $r_p(G) = \dim_{\mathbb{F}_p}(G[p])$. We have the following result.

Proposition 3.3. *For any $K_\infty \in \mathcal{E}_p$ and each $i \in \mathbb{N}$, the natural map*

$$s_i : \mathrm{Sel}^{Gr(p)}(E[p^i]/K_\infty) \longrightarrow \mathrm{Sel}^{Gr(p)}(E/K_\infty)[p^i]$$

is surjective with finite kernel satisfying $r_p(\ker s_i) \leq 2$ and $|\ker(s_i)| \leq p^{2i}$.

Proof. Consider the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}^{Gr(p)}(E/K_\infty)[p^i] & \longrightarrow & H^1(G_S(K_\infty), E[p^\infty])[p^i] & \longrightarrow & \prod_{w \in S_{K_\infty,p}} H^1_{Gr,s}(K_{\infty,w}, E[p^\infty])[p^i] \\
 & & \uparrow{\scriptstyle s_i} & & \uparrow{\scriptstyle g_i} & & \uparrow{\scriptstyle h_i} \\
0 & \longrightarrow & \mathrm{Sel}^{Gr(p)}(E[p^i]/K_\infty) & \longrightarrow & H^1(G_S(K_\infty), E[p^i]) & \longrightarrow & \prod_{w \in S_{K_\infty,p}} H^1_{Gr,s}(K_{\infty,w}, E[p^i])
\end{array}$$

The map g_i is surjective with $\ker g_i = E(K_\infty)[p^\infty]/p^i$, whence $r_p(\ker g_i) \leq 2$. It follows from this and the snake lemma that the desired result will follow if we can show that the map h_i is injective. This in turn will follow if we can show that the map $h_{w,i} : H^1(I_w, \tilde{E}[p^i]) \longrightarrow H^1(I_w, \tilde{E}[p^\infty])[p^i]$ is injective where w is a prime of K_∞ above p. But I_w acts trivially on $\tilde{E}$, so

$$\ker h_{w,i} = H^0(I_w, \tilde{E}[p^\infty])/p^i = \tilde{E}[p^\infty]/p^i = 0.$$

This completes the proof. □

Remark 3.4. *The proof of the above lemma shows that s_i is an isomorphism if $E(K_\infty)[p^\infty] = 0$.*

Lemma 3.5. *For any $K_\infty \in \mathcal{E}_p$ and every $i \in \mathbb{N}$, $i > 0$, the isomorphism $E_1[p^i] \cong E_2[p^i]$ of Galois modules induces an isomorphism*

$$\mathrm{Sel}^{Gr(p)}(E_1[p^i]/K_\infty) \cong \mathrm{Sel}^{Gr(p)}(E_2[p^i]/K_\infty).$$

Proof. The isomorphism $\Phi : E_1[p^i] \cong E_2[p^i]$ induces an isomorphism

$$H^1(G_S(K_\infty), E_1[p^i]) \cong H^1(G_S(K_\infty), E_2[p^i]).$$

Let v be a prime of K above p. We want to show that Φ induces an isomorphism $\Phi_v : \tilde{E}_1[p^i] \cong \tilde{E}_2[p^i]$. We now show that condition (Δ) in the introduction implies that such a map Φ_v can be induced from Φ. Let $G_{K_v} = \mathrm{Gal}(\bar{K}_v/K_v)$ and let I_v be the inertia subgroup.

Let $C_v = \mathcal{F}(\bar{\mathfrak{m}})$ where $\bar{\mathfrak{m}}$ is the maximal ideal of $\bar{K}_v$ and $\mathcal{F}$ is the formal group of E_1. We similarly define D_v using the formal group of E_2. Then we have exact sequences

$$0 \longrightarrow C_v[p^n] \longrightarrow E_1[p^n] \longrightarrow \tilde{E}_1[p^n] \longrightarrow 0,$$

$$0 \longrightarrow D_v[p^n] \longrightarrow E_2[p^n] \longrightarrow \tilde{E}_2[p^n] \longrightarrow 0.$$

From the exact sequences above, we see that to prove that Φ_v can be induced from Φ we need to show that $\Phi(C_v[p^n]) = D_v[p^n]$. To show that, we use a similar argument to that of Greenberg and Vatsal, see [20, p. 26]. Let μ_{p^n} be the group of p^n-th roots of unity in $\bar{K}_v$. It will suffice to prove that $C_v[p^n]$ is the unique subgroup of $E_1[p^n]$ that is isomorphic to μ_{p^n} as an I_v-module and similarly for $E_2[p^n]$. Note that as E_1 and E_2 have good ordinary reduction at v; therefore as $\mathbb{Z}/p^n\mathbb{Z}$-modules, we have $\tilde{E}_1[p^n] \cong \tilde{E}_2[p^n] \cong \mathbb{Z}/p^n\mathbb{Z}$. As I_v acts trivially on $\tilde{E}_1[p^n]$, we see by the Weil pairing that I_v acts on $C_v[p^n]$ by the p^n-cyclotomic character χ, that is, $C_v[p^n] \cong \mu_{p^n}$ as an I_v-module. Now we show that $C_v[p^n]$ is the unique subgroup with this property.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

CLAIM: I_v acts nontrivially on any nontrivial quotient of μ_{p^n}. Assume that the claim is not true. Any nontrivial quotient of μ_{p^n} is of the form μ_{p^n}/μ_{p^k} where $k < n$. Let $\sigma \in I_v$ and let ζ be a primitive p^n-th root of unity. Then $\sigma(\zeta)\mu_{p^k} = \sigma(\zeta\mu_{p^k}) = \zeta\mu_{p^k}$, that is $\sigma(\zeta) = \zeta\alpha$ where $\alpha \in \mu_{p^k}$. Since $\alpha = \zeta^c$ for some integer c divisible by p^{n-k}, we have that $\sigma(\zeta) = \zeta^{1+c}$ for such an integer c. Then $\sigma(\zeta^{p^{n-1}}) = (\zeta^{p^{n-1}})^{1+c} = \zeta^{p^{n-1}}$ since cp^{n-1} is divisible by p^n. Thus, $\sigma(\mu_p) = \mu_p$. This holds for all $\sigma \in I_v$. Therefore, $(\mu_p)^{I_v} = \mu_p$. This contradicts (Δ) and so we see that the claim is true.

Now suppose that $U \neq C_v[p^n]$ is a subgroup of $E_1[p^n]$ that is isomorphic to μ_{p^n} as an I_v-module. Consider the quotient $U/(U \cap C_v[p^n])$. Since $U \neq C_v[p^n]$, this is a nontrivial quotient of U and so by the above claim I_v acts nontrivially on this quotient. But we have a $(\mathbb{Z}/p^n\mathbb{Z})[I_v]$-injection

$$U/(U \cap C_v[p^n]) \hookrightarrow \tilde{E}_1[p^n].$$

Since I_v acts trivially on $\tilde{E}_1[p^n]$, this is a contradiction. Therefore, we see that $U = C_v[p^n]$, that is, $C_v[p^n]$ is the unique subgroup of $E_1[p^n]$ that is isomorphic to μ_{p^n} as an I_v-module. Thus, Φ induces an isomorphism Φ_v.

It follows from this that for any $w \in S_p$, we have an isomorphism

$$H^1_{Gr,s}(K_{\infty,w}, E_1[p^i]) \cong H^1_{Gr,s}(K_{\infty,w}, E_2[p^i]).$$

The lemma follows from these observations. □

We end this section with the following control theorem (where as usual we assume that $d \geq 2$). Let E be either E_1 or E_2. Let S be the set of primes of K which lie above p or where E has bad reduction.

Proposition 3.6. *Let $K_\infty \in \mathcal{E}$. Consider the dual of the restriction map*

$$f^\vee : X^{Gr}(E/\mathbb{L}_\infty)_{\mathrm{Gal}(\mathbb{L}_\infty/K_\infty)} \longrightarrow X^{Gr}(E/K_\infty).$$

We have

(a) $\mathrm{coker} f^\vee$ *is a finitely generated $\mathbb{Z}_p$-module with* $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{coker}\, f^\vee) \leq (d-1)$.
(b) Let $m_p = \sum_{v|p} m_v$ where the sum runs over the primes of K above p and m_v is defined to be zero if v splits completely in K_∞ and equal to the number of primes of K_∞ above v otherwise. Then $\ker f^\vee$ *is a finitely generated torsion Λ-module with* $\lambda(\ker f^\vee) \leq (d-1)m_p + (d-1)(d-2)/2$.

Proof. Taking into account Proposition 2.2, this proposition can be proven in an identical way to [35, Lemma 3.11]. □

Corollary 3.7. *Let $K_\infty \in \mathcal{E}$, then the following assertions hold.*

(a) $\mathrm{rank}_\Lambda(X^{Gr}(E/K_\infty)) = \mathrm{rank}_\Lambda(X^{Gr}(E/\mathbb{L}_\infty)_{\mathrm{Gal}(\mathbb{L}_\infty/K_\infty)})$.
(b) Assume that

(1) no prime in S_p splits completely in K_∞/K,
(2) $\mathrm{rank}_\Lambda(X^{Gr}(E/K_\infty)) = \mathrm{rank}_\Lambda(X^{Gr}(E/\mathbb{L}_\infty)_{\mathrm{Gal}(\mathbb{L}_\infty/K_\infty)}) = 0$.

Furthermore, assume either of the following conditions is true

(i) No prime in $S \setminus S_p$ splits completely in K_∞/K
(ii) E satisfies $(\star)$ from the introduction for all $v \in S$

Then $\mu(X^{Gr}(E/K_\infty)) = \mu(X^{Gr}(E/\mathbb{L}_\infty)_{\mathrm{Gal}(\mathbb{L}_\infty/K_\infty)})$.
(c) If no prime in S_p splits completely in K_∞/K, then there exists a neighbourhood $\mathcal{E}(K_\infty, n)$ such that $|\lambda(X^{Gr}(E/K'_\infty)) - \lambda(X^{Gr}(E/\mathbb{L}_\infty)_{\mathrm{Gal}(\mathbb{L}_\infty/K'_\infty)})|$ is bounded as K'_∞ runs over the elements of $\mathcal{E}(K_\infty, n)$ for which

$$\mathrm{rank}_\Lambda(X^{Gr}(E/K'_\infty)) = \mathrm{rank}_\Lambda(X^{Gr}(E/\mathbb{L}_\infty)_{\mathrm{Gal}(\mathbb{L}_\infty/K'_\infty)}) = 0.$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Proof. Statement (a) follows directly from Proposition 3.6. Now assume that both $X^{Gr}(E/K_\infty)$ and $X^{Gr}(E/\mathbb{L}_\infty)_{\mathrm{Gal}(\mathbb{L}_\infty/K_\infty)}$ are Λ-torsion. Also assume that no prime in S_p splits completely in K_∞/K. By Lemma 2.1, we may assume that S is precisely the set of primes of K above p and where E has bad reduction. If E satisfies ($\star$) for all $v \in S$, then by Proposition 3.2, for any prime of K_∞ lying over a prime of $S \setminus S_p$ we have $H^1(K_{\infty,w}, E[p^\infty]) = 0$. From this and the proof of Proposition 3.6, we have that under either condition (i) or (ii) both $\mu(\ker f^\vee) = 0$ and $\mu(\mathrm{coker} f^\vee) = 0$. This proves (b). We can prove part (c) in an identical way to [35, Corollary 3.12(b)]. □

4. Congruent elliptic curves and $\mathbb{Z}_p$-extensions

In this section, we collect some results about relationships between Iwasawa invariants of Pontryagin duals of Selmer groups of congruent elliptic curves over $\mathbb{Z}_p$-extensions. Via the up-down approach described in the introduction, we will in the next sections use these results to prove our main theorems.

We need the following auxiliary result, which is due to Lim.

Lemma 4.1 (Lim [39], Lemma 2.4.1). *Let M be a finitely generated Λ-module. Suppose that there is a Λ-module homomorphism*

$$\varphi\colon M[p^\infty] \longrightarrow \bigoplus_{j=1}^{s} \Lambda/(p^{m_j}) \tag{7}$$

with pseudo-null (i.e. finite) kernel and cokernel. Then we have

$$\mu(M/p^i) = i \cdot \mathrm{rank}_\Lambda(M) + \sum_{j=1}^{s} \min(i, m_j).$$

for every $i \in \mathbb{N}$, $i \geq 1$.

Note that the module $\bigoplus_{j=1}^{s} \Lambda/(p^{m_j})$ is an elementary Λ-module attached to $M[p^\infty]$, as in the exact sequence (2).

Definition 4.2. *Let M be a finitely generated Λ-module, and consider a pseudo-isomorphism φ as in equation (7). Then we define $e(M)$ to be the maximum of the exponents m_j, $1 \leq j \leq s$.*

The following theorem illustrates relationships between μ-invariants of Pontryagin duals of Selmer groups of congruent elliptic curves. Recall Definitions 1.2 and 1.3 from the introduction.

Theorem 4.3. *Assume that either $K_\infty \in \mathcal{E}_{ns}$ or E_1 and E_2 satisfy condition ($\star$) for all $v \in S$.*

(a) Suppose that $E_1[p^i] \cong E_2[p^i]$ as Galois modules, where i is larger than both $e(X^{Gr}(E_1/K_\infty))$ and $e(X^{Gr}(E_2/K_\infty))$. Then

$$\mathrm{rank}_\Lambda(X^{Gr}(E_1/K_\infty)) = \mathrm{rank}_\Lambda(X^{Gr}(E_2/K_\infty))$$

and

$$\mu(X^{Gr}(E_1/K_\infty)) = \mu(X^{Gr}(E_2/K_\infty)).$$

In fact, the two Λ-modules $X^{Gr}(E_1/K_\infty)[p^\infty]$ and $X^{Gr}(E_2/K_\infty)[p^\infty]$ are pseudo-isomorphic.

(b) Now suppose that $\mathrm{rank}_\Lambda(X^{Gr}(E_1/K_\infty)) \leq \mathrm{rank}_\Lambda(X^{Gr}(E_2/K_\infty))$ and that $E_1[p^i] \cong E_2[p^i]$ for some $i > e(X^{Gr}(E_1/K_\infty))$. Then the Λ-ranks are equal, and the p-primary torsion submodules of $X^{Gr}(E_1/K_\infty)$ and $X^{Gr}(E_2/K_\infty)$ are pseudo-isomorphic as Λ-modules.

(c) If $E_1[p] \cong E_2[p]$, then $\mathrm{Sel}^{Gr}(E_1/K_\infty)$ is Λ-cotorsion with $\mu = 0$ if and only if $\mathrm{Sel}^{Gr}(E_2/K_\infty)$ is Λ-cotorsion with $\mu = 0$.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Proof. The following proof uses ideas from the proof of [39, Theorem 4.2.1]. But note that Lim's result was proven only for torsion Iwasawa modules.

For both $j = 1$ and $j = 2$, we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}^{Gr}(E_j/K_\infty) \longrightarrow \mathrm{Sel}^{Gr(p)}(E_j/K_\infty) \longrightarrow \prod_{v \in S \setminus S_p} \mathcal{H}_v(E_j/K_\infty).$$

If $K_\infty \in \mathcal{E}_{ns}$, then by Proposition 3.1 we see that $\bigoplus_{v \in S \setminus S_p} \mathcal{H}_v(E_j/K_\infty)$ is a cotorsion Λ-module with $\mu = 0$ for both $j = 1, 2$. By Lemma 2.1 in the exact sequence above, we may assume for $j = 1, 2$ that S is precisely the set of primes of K which lie above p or where E_j has bad reduction. If both E_1 and E_2 satisfy condition $(\star)$ for all $v \in S$, then by Proposition 3.2 $\bigoplus_{v \in S \setminus S_p} \mathcal{H}_v(E_j/K_\infty) = 0$, $j = 1, 2$. Taking Pontryagin duals in the above exact sequence, we may conclude that in either case we have

$$\mathrm{rank}_\Lambda(X^{Gr}(E_j/K_\infty)) = \mathrm{rank}_\Lambda(X^{Gr(p)}(E_j/K_\infty))$$

and

$$\mu(X^{Gr}(E_j/K_\infty)) = \mu(X^{Gr(p)}(E_j/K_\infty))$$

for both $j = 1$ and $j = 2$. In fact, the p-torsion submodules are pseudo-isomorphic, that is,

$$e(X^{Gr}(E_j/K_\infty)) = e(X^{Gr(p)}(E_j/K_\infty))$$

for both j. Moreover, for every $k \in \mathbb{N}$ we have an exact sequence

$$\prod_{v \in S \setminus S_p} \mathcal{H}_v(E_j/K_\infty)^\vee / p^k \longrightarrow X^{Gr(p)}/p^k \longrightarrow X^{Gr}/p^k \longrightarrow 0,$$

where the first term is finite for each k.

Suppose first that $E_1[p^i] \cong E_2[p^i]$ for some $i > 1$. Then Lemma 3.5 implies

$$\mathrm{Sel}^{Gr(p)}(E_1[p^i]/K_\infty) \cong \mathrm{Sel}^{Gr(p)}(E_2[p^i]/K_\infty).$$

From Proposition 3.3, we have for $j = 1, 2$ that the natural map

$$\mathrm{Sel}^{Gr(p)}(E_j[p^i]/K_\infty) \longrightarrow \mathrm{Sel}^{Gr(p)}(E_j/K_\infty)[p^i]$$

is a surjection with finite kernel. Combining the two previous facts and taking Pontryagin duals, we obtain that we have a pseudo-isomorphism of Λ-modules

$$X^{Gr(p)}(E_1/K_\infty)/p^i \sim X^{Gr(p)}(E_2/K_\infty)/p^i.$$

In particular, the μ-invariants of these two quotient modules are equal. Note that we also have $E_1[p^{i-1}] \cong E_2[p^{i-1}]$, and therefore we also have an equality of μ-invariants

$$\mu(X^{Gr(p)}(E_1/K_\infty)/p^{i-1}) = \mu(X^{Gr(p)}(E_2/K_\infty)/p^{i-1}).$$

As we have seen in the first part of the proof, this implies that we have an analogous equation for X^{Gr} instead of $X^{Gr(p)}$. Now we apply Lemma 4.1, both with i and $i-1$, and obtain that

$$\begin{aligned} i \cdot r_1 + \mu(X^{Gr}(E_1/K_\infty)) &= i \cdot r_2 + \mu(X^{Gr}(E_2/K_\infty)), \\ (i-1) \cdot r_1 + \mu(X^{Gr}(E_1/K_\infty)) &= (i-1) \cdot r_2 + \mu(X^{Gr}(E_2/K_\infty)), \end{aligned}$$

where we let $r_1 = \mathrm{rank}_\Lambda(X^{Gr}(E_1/K_\infty))$ and $r_2 = \mathrm{rank}_\Lambda(X^{Gr}(E_2/K_\infty))$ for brevity. Here, we use the fact that $i-1$ is greater than or equal to the maximum of both $e(X^{Gr(p)}(E_j/K_\infty))$, $j \in \{1, 2\}$. Subtracting the two equations, we obtain that the two Λ-ranks are equal, and then the first equation concludes the proof of the first part of (a). In order to obtain the last part, we just note that our assumptions imply that $E_1[p^k] \cong E_2[p^k]$ for each $k \leq i$. Writing down the corresponding equations from Lemma 4.1 and comparing the coefficients $\min(k, m_j)$ for the two Λ-modules, starting from $k = i-1$ and going down to $k = 1$, we can finish the proof of (a) via an induction.

Now suppose that we are the setting of (b). Write down the equation from Lemma 4.1 for each integer $k \leq i$. Recall that $i - 1 \geq e(X^{Gr}(E_1/K_\infty))$. Comparing the equations for $k = i$ and $k = i-1$, we

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

may conclude that

$$\mu(X^{Gr}(E_1/K_\infty)) = \mu(X^{Gr}(E_1/K_\infty)/p^i) = \mu(X^{Gr}(E_1/K_\infty)/p^{i-1})$$

equals both

$$i \cdot (r_2 - r_1) + \mu(X^{Gr}(E_2/K_\infty)/p^i)$$

and

$$(i-1) \cdot (r_2 - r_1) + \mu(X^{Gr}(E_2/K_\infty)/p^{i-1}).$$

Letting $r := r_2 - r_1$ for brevity, we obtain that

$$ir + \mu(X^{Gr}(E_2/K_\infty)/p^i) = (i-1)r + \mu(X^{Gr}(E_2/K_\infty)/p^{i-1}).$$

Since it is obvious that the first (respectively, the second) summand on the left-hand side of this equation is greater than or equal to the first (respectively, the second) summand on the right-hand side (here we use the assumption that $r \geq 0$), we conclude that we must have

$$ir = (i-1)r, \quad \mu(X^{Gr}(E_2/K_\infty/p^i)) = \mu(X^{Gr}(E_2/K_\infty)/p^{i-1}).$$

This proves that $e(X^{Gr}(E_2/K_\infty)) \leq i-1$, and that $r = 0$, that is, $\operatorname{rank}_\Lambda(X^{Gr}(E_1/K_\infty)) = \operatorname{rank}_\Lambda(X^{Gr}(E_2/K_\infty))$. Now we proceed iteratively, as in the proof of (a), decreasing the value of k step by step.

Finally, we prove the last assertion of the theorem. From the structure theorem of finitely generated Λ-modules, it is easy to see that

$$\begin{aligned} &\operatorname{Sel}^{Gr(p)}(E_i/K_\infty) \text{ is } \Lambda\text{-cotorsion with } \mu = 0 \\ \iff &\operatorname{Sel}^{Gr(p)}(E_i/K_\infty)[p] \text{ is finite.} \end{aligned}$$

From Proposition 3.3 and Lemma 3.5 it follows that, since $E_1[p] \cong E_2[p]$, $\operatorname{Sel}^{Gr(p)}(E_1/K_\infty)[p]$ is finite if and only if $\operatorname{Sel}^{Gr(p)}(E_2/K_\infty)[p]$ is finite. Part (c) of the theorem follows by combining these results. □

Definition 4.4. *If $K_\infty \in \mathcal{E}$, we denote the maximal finite Λ-submodule of $X^{Gr(p)}(E_j/K_\infty)$ by $\mathfrak{X}^{Gr(p)}(E/K_\infty)$.*

Proposition 4.5. *Let E be either E_1 or E_2. Assume the following:*

(1) $E(\mathbb{L}_\infty)[p^\infty]$ is finite
(2) The decomposition subgroups $D_v(\mathbb{L}_\infty/K) \subseteq \operatorname{Gal}(\mathbb{L}_\infty/K)$ are open for each $v \mid p$
(3) E satisfies ($\star$) from Definition 1.3 for all $v \in S$

Then there exists a constant $C^{Gr} \geq 0$ such that for all $K_\infty \in \mathcal{E}$ with $X^{Gr}(E/K_\infty)$ Λ-torsion we have $r_p(\mathfrak{X}^{Gr(p)}(E/K_\infty)) \leq C^{Gr}$.

Proof. Let $K_\infty \in \mathcal{E}$ with $X^{Gr}(E/K_\infty)$ Λ-torsion. We have an exact sequence

$$\prod_{v \in S \setminus S_p} \mathcal{H}_v(E/K_\infty)^\vee \longrightarrow X^{Gr(p)}(E/K_\infty) \longrightarrow X^{Gr}(E/K_\infty) \longrightarrow 0.$$

By Lemma 2.1, we may assume that S is precisely the set of primes of K above p or where E has bad reduction. By Proposition 3.2, the first term in the above sequence is trivial. Therefore, the desired result follows from Proposition 2.10. □

In order to be able to compare λ-invariants, we need

Lemma 4.6. *Assume that both E_1 and E_2 satisfy condition ($\star$) for all $v \in S$. Then for any $K_\infty \in \mathcal{E}$, we have $\lambda(X^{Gr}(E_j/\tilde{K}_\infty)) = \lambda(X^{Gr(p)}(E_j/\tilde{K}_\infty))$.*

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Proof. We have an exact sequence

$$\prod_{v\in S\setminus S_p} \mathcal{H}_v(E/K_\infty)^\vee \longrightarrow X^{Gr(p)}(E/K_\infty) \longrightarrow X^{Gr}(E/K_\infty) \longrightarrow 0.$$

By Lemma 2.1, we may assume that S is precisely the set of primes of K above p or where E has bad reduction. By Proposition 3.2, the first term in the above sequence is trivial. The lemma follows. □

Greenberg [14] introduced the following topology on $\mathcal{E}$. For $L \in \mathcal{E}$ and n a positive integer, we define $\mathcal{E}(L,n) := \{L' \in \mathcal{E} \mid [L' \cap L : K] \geq p^n\}$. This means that $\mathcal{E}(L,n)$ consists of all $\mathbb{Z}_p$-extensions of K which coincide with L at least up to the n-th layer. Taking $\mathcal{E}(L,n)$ as a base of neighborhoods of L gives us a topology on $\mathcal{E}$.

Lemma 4.7. *Assume the following*

(1) $E_1(\mathbb{L}_\infty)[p^\infty]$ *and* $E_2(\mathbb{L}_\infty)[p^\infty]$ *are finite,*
(2) the decomposition subgroups $D_v(\mathbb{L}_\infty/K) \subseteq \mathrm{Gal}(\mathbb{L}_\infty/K)$ *are open for each* $v \mid p$*,*
(3) E_1 *and* E_2 *satisfy* $(\star)$ *for all* $v \in S$*.*
Suppose that K_∞ *is a* $\mathbb{Z}_p$*-extension of* K *such that*
(4) $X^{Gr}(E_1/K_\infty)$ *is* Λ*-torsion.*
Assume that
(5) $E_1[p^i] \cong E_2[p^i]$ *for some integer* i *such that* $i > \mu(X^{Gr}(E_1/K_\infty))$*. Then* $X^{Gr}(E_2/K_\infty)$ *is* Λ*-torsion and*

$$|\lambda(X^{Gr}(E_1/K_\infty)) - \lambda(X^{Gr}(E_2/K_\infty))| \leq 2i + C^{Gr},$$

where C^{Gr} *denotes the constant from Proposition 4.5.*

Proof. In view of our hypotheses, it follows from Theorem 4.3(b) that $X^{Gr}(E_2/K_\infty)$ is Λ-torsion with $\mu(X^{Gr}(E_2/K_\infty)) = \mu(X^{Gr}(E_1/K_\infty))$.

Now fix K_∞. For both $j=1$ and $j=2$, we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E_j[p^{i-1}] & \longrightarrow & E_j[p^\infty] & \xrightarrow{\times p^{i-1}} & E_j[p^\infty] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \iota_j} & & \downarrow & & \downarrow{\scriptstyle \times p} & & \\
0 & \longrightarrow & E_j[p^i] & \longrightarrow & E_j[p^\infty] & \xrightarrow{\times p^i} & E_j[p^\infty] & \longrightarrow & 0.
\end{array}$$

In the above diagram, the left vertical map is inclusion and the middle vertical map is the identity map. This commutative diagram implies that we have another commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B_{i-1} & \longrightarrow & \mathrm{Sel}^{Gr(p)}(E_j[p^{i-1}]/K_\infty) & \longrightarrow & \mathrm{Sel}^{Gr(p)}(E_j/K_\infty)[p^{i-1}] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \iota_{j*}} & & \downarrow & & \\
0 & \longrightarrow & B_i & \longrightarrow & \mathrm{Sel}^{Gr(p)}(E_j[p^i]/K_\infty) & \longrightarrow & \mathrm{Sel}^{Gr(p)}(E_j/K_\infty)[p^i] & \longrightarrow & 0.
\end{array}$$

By Proposition 3.3, the rows are exact with $\#B_k \leq p^{2k}$ for both $k=i$ and $k=i-1$. Taking Pontryagin duals and using the snake lemma, the above commutative diagram induces a map $\theta_j\colon p^{i-1}X^{Gr(p)}(E_j/K_\infty)/p^i \longrightarrow \ker \widehat{\iota_{j*}}$ where $\widehat{\iota_{j*}}$ is the dual map to ι_{j*}. The map θ_j is injective with $\#\mathrm{coker}\theta_j \leq p^{2i}$.

Now Lemma 3.5 implies that $\ker \widehat{\iota_{1*}} \cong \ker \widehat{\iota_{2*}}$. Since p^{i-1} annihilates the 'μ-parts' of both $X^{Gr(p)}(E_j/K_\infty)$, $j=1,2$, it is easy to see that $p^{i-1}X^{Gr(p)}(E_j/K_\infty)/p^i$ are finite for $j=1,2$. From these two

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

facts and the above, we have

$$\begin{aligned}\#p^{i-1}X^{Gr(p)}(E_1/K_\infty)/p^i \cdot \#\mathrm{coker}\theta_1 &= \#\ker \widehat{\iota_{1*}} \\ &= \#\ker \widehat{\iota_{2*}} \\ &= \#p^{i-1}X^{Gr(p)}(E_2/K_\infty)/p^i \cdot \#\mathrm{coker}\theta_2.\end{aligned}$$

Therefore, we may conclude that

$$|v_p(|p^{i-1}X^{Gr(p)}(E_1/K_\infty)/p^i|) - v_p(|p^{i-1}X^{Gr(p)}(E_2/K_\infty)/p^i|)|$$

equals

$$|v_p(|\mathrm{coker}\theta_1|) - v_p(|\mathrm{coker}\theta_2|)|,$$

and therefore it is bounded by $2i$.

Recall that $\mathfrak{X}^{Gr(p)}(E_j/K_\infty) \subseteq X^{Gr(p)}(E_j/K_\infty)$ denotes the maximal finite Λ-submodule, $j = 1, 2$. Let C^{Gr} be the integer in Proposition 4.5. By Proposition 4.5 $r_p(\mathfrak{X}^{Gr(p)}(E_j/K_\infty)) \leq C^{Gr}$ for each $j = 1, 2$.

Using that p^{i-1} annihilates the 'μ-parts' of both $X^{Gr(p)}(E_j/K_\infty)$, $j = 1, 2$, we will now show by using [33, Lemma 3.8] that the cardinality of $p^{i-1}X^{Gr(p)}(E_j/K_\infty)/p^i$ differs from $p^{\lambda(X^{Gr(p)}(E_j/K_\infty))}$ by at most $p^{r_p(\mathfrak{X}^{Gr(p)}(E_j/K_\infty))}$, $j = 1, 2$. Then it will follow from the above that the difference between the λ-invariants of these two Λ-modules is bounded by $2i + C^{Gr}$, and the assertion of the lemma follows from Lemma 4.6.

In order to prove the above claim, we fix j and abbreviate $X^{Gr(p)}(E_j/K_\infty)$ to X. Let $Y = p^{i-1}X$. Then Y is a finitely generated and torsion Λ-module, and it follows from the choice of i that $\mu(Y) = 0$. We let $\mathfrak{X} \subseteq X$ and $\mathcal{Y} \subseteq Y$ be the maximal finite Λ-submodules, and we fix an elementary Λ-module E_Y attached to Y.

Then we have an exact sequence

$$0 \longrightarrow \mathcal{Y} \longrightarrow Y \longrightarrow \tilde{E}_Y \longrightarrow 0,$$

where $\tilde{E}_Y \subseteq E_Y$ is a submodule of finite index. For any abelian group A, we define $\mathrm{rank}_p(A) = v_p(|A/pA|)$, provided this number is finite. Since $\mu(Y) = 0$, multiplication by p is injective on $\tilde{E}_Y \subseteq E_Y$ and we have an equality

$$\mathrm{rank}_p(Y) = \mathrm{rank}_p(\mathcal{Y}) + \mathrm{rank}_p(\tilde{E}_Y)$$

of p-ranks. Since p does not divide the characteristic power series f_Y of Y, it follows from [31, Proposition 3.4(i) and (iv)] that $\mathrm{rank}_p(\tilde{E}_Y) = \mathrm{rank}_p(E_Y)$, and the latter is just $\lambda(E_Y) = \lambda(Y) = \lambda(X)$ because f_Y is a distinguished polynomial. On the other hand, since $\mathcal{Y} \subseteq \mathfrak{X}$, we have $\mathrm{rank}_p(\mathcal{Y}) \leq \mathrm{rank}_p(\mathfrak{X})$. This proves the above claim. □

5. Proof of the first main theorem

In this section, we prove Theorem 1.4. First, we need the following

Lemma 5.1. *Assume that $\mathcal{E}_{ns} \neq \emptyset$. For $j = 1, 2$ $X^{Gr}(E_j/\mathbb{L}_\infty)$ is a torsion Λ_d-module with $m_0(X^{Gr}(E_j/\mathbb{L}_\infty)) = \alpha$ if and only if there exist a finite number of $\mathbb{Z}_p^{d-1}$-extensions of K contained in $\mathbb{L}_\infty$ such that for all $\tilde{K}_\infty \in \mathcal{E}$ that are not contained in these extensions we have that $X^{Gr}(E_j/\tilde{K}_\infty)$ is Λ-torsion with $\mu(X^{Gr}(E_j/\tilde{K}_\infty)) = \alpha$.*

Proof. Let $j \in \{1, 2\}$. For brevity, we let $X = X^{Gr}(E_j/\mathbb{L}_\infty)$. We have the following facts:

(a) If X is Λ_d-torsion, then for any $\tilde{K}_\infty \in \mathcal{E}$ and $\tilde{H} = \mathrm{Gal}(\mathbb{L}_\infty/\tilde{K}_\infty)$ it follows from [46, Theorem 3.2] that $X_{\tilde{H}}$ is a torsion Λ-module with μ-invariant equal to $m_0(X)$ as long as $\tilde{K}_\infty$ is not contained in a fixed finite number of $\mathbb{Z}_p^{d-1}$-extensions of K contained in $\mathbb{L}_\infty$.

(b) Let $\tilde{K}_\infty \in \mathcal{E}$ and $\tilde{H} = \mathrm{Gal}(\mathbb{L}_\infty/\tilde{K}_\infty)$. From [40, Lemma 4.7], it follows that if $X_{\tilde{H}}$ is Λ-torsion, then X is Λ_d-torsion.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

(c) Let $\tilde{K}_\infty \in \mathcal{E}$ and $\tilde{H} = \mathrm{Gal}(\mathbb{L}_\infty/\tilde{K}_\infty)$. Corollary 3.7 implies that

(i) $\mathrm{rank}_\Lambda(X_{\tilde{H}}) = \mathrm{rank}_\Lambda(X^{Gr}(E/\tilde{K}_\infty))$,
(ii) $\mu(X_{\tilde{H}}) = \mu(X^{Gr}(E/\tilde{K}_\infty))$ if there does not exist a prime in S which splits completely in $\tilde{K}_\infty/K$.

The condition in (c)-(ii) above means that it will suffice if $\tilde{K}_\infty$ is not contained in the decomposition field of any of the primes $v \in S$. Since $\mathcal{E}_{ns} \neq \emptyset$, the decomposition subgroup $D_v(\mathbb{L}_\infty/K) \subseteq \mathrm{Gal}(\mathbb{L}_\infty/K)$ has $\mathbb{Z}_p$-rank at least one for each $v \in S$. Therefore, condition (c)-(ii) excludes the $\mathbb{Z}_p$-extensions which are contained in a finite set of $\mathbb{Z}_p^{d-1}$-extensions inside $\mathbb{L}_\infty$. The statement of the lemma easily follows from this and the facts (a), (b), and (c) above. □

We can now prove the first main result, namely Theorem 1.4 from the introduction.

Proof of Theorem 1.4. By Propositions 2.2 and 2.3, it suffices to prove the theorem with $X(E_j/\mathbb{L}_\infty)$ replaced with $X^{Gr}(E_j/\mathbb{L}_\infty)$ for $j = 1, 2$. Assume that $X^{Gr}(E_1/\mathbb{L}_\infty)$ is a torsion Λ_d-module with $E_1[p^i] \cong E_2[p^i]$ for some integer $i > m_{0,1}$. By Lemma 5.1 for all $\tilde{K}_\infty \in \mathcal{E}$ that are not contained in a fixed finite number of $\mathbb{Z}_p^{d-1}$-extensions of K contained in $\mathbb{L}_\infty$, we have that $X^{Gr}(E_1/\tilde{K}_\infty)$ is Λ-torsion with $\mu(X^{Gr}(E_1/\tilde{K}_\infty)) = m_{0,1}$. Note that $\mu(X^{Gr}(E_1/K_\infty)) \geq e(X^{Gr}(E_1/K_\infty))$ for any $K_\infty \in \mathcal{E}$. Therefore, we see from Theorem 4.3(b) that for all $\tilde{K}_\infty \in \mathcal{E}$ that are not contained in a fixed finite number of $\mathbb{Z}_p^{d-1}$-extensions of K contained in $\mathbb{L}_\infty$ we have that $X^{Gr}(E_2/\tilde{K}_\infty)$ is Λ-torsion with $\mu(X^{Gr}(E_2/\tilde{K}_\infty)) = m_{0,1}$. Then by Lemma 5.1, $X^{Gr}(E_2/\mathbb{L}_\infty)$ is a torsion Λ_d-module with $m_{0,2} = m_{0,1}$. □

6. Via Lim's approach

In [39], Lim gave a proof of Theorem 1.4 in more generality, using a completely different approach. We will now describe this approach briefly. Then we strengthen Lim's approach in order to compare also l_0-invariants of Selmer groups. It will turn out that in order to compare l_0-invariants via Lim's approach, a strong additional hypothesis is needed (see Theorem 6.15 below). Our up-down approach seems more suitable for handling l_0-invariants, since it allows us to prove Theorem 1.5 which holds under milder assumptions. We will follow that approach in Section 7.

In this section, we will work with $X^{str}(E/\mathbb{L}_\infty)$. By Proposition 2.2, our results apply to $X^{Gr}(E/\mathbb{L}_\infty)$ and under suitable assumptions (see Proposition 2.3) our results also apply to $X(E/\mathbb{L}_\infty)$.

Let $X = X^{str}(E_1/\mathbb{L}_\infty)$ and $X' = X^{str}(E_2/\mathbb{L}_\infty)$, and write $G = \mathrm{Gal}(\mathbb{L}_\infty/K) \cong \mathbb{Z}_p^d$. Then $\mathbb{L}_\infty = \bigcup_n \mathbb{L}_n$, where each number field $\mathbb{L}_n = \mathbb{L}_\infty^{G_n}$, $G_n = G^{p^n}$, satisfies $\mathrm{Gal}(\mathbb{L}_n/K) \cong (\mathbb{Z}/p^n\mathbb{Z})^d$. On any finite level n, we write $X_n = X^{str}(E_1/\mathbb{L}_n)$ and $X'_n = X^{str}(E_2/\mathbb{L}_n)$ for brevity.

The strategy is as follows. We encode the information about the m_0-invariants into asymptotic growth formulas for the orders of the quotients X_{G_n} and X'_{G_n}, moding out the submodules of elements which are multiples of p^k for a sufficiently large k (it will be important that k is larger than $m_0(X)$). In fact, the m_0-invariants and the Λ_d-ranks give rise to the leading terms in these asymptotic formulas. Via a control theorem, the quotients X_{G_n}/p^k and X'_{G_n}/p^k are related to analogous quotients of the Pontryagin duals of the strict Selmer groups $X^{str}(E_1/\mathbb{L}_n)$ and $X^{str}(E_2/\mathbb{L}_n)$. Via a result similar to Proposition 3.3 (see Lemma 6.4), we can relate these quotients to the Pontryagin duals of residual Selmer groups $\mathrm{Sel}^{str}(E_j[p^k]/\mathbb{L}_n)$, $j = 1, 2$, which are defined as the classical strict Selmer groups in Section 2, but with $E_j[p^\infty]$ replaced by $E_j[p^k]$. If $E_1[p^k] \cong E_2[p^k]$ as Galois modules, then the cardinalities of the two latter groups are equal (this will follow from a result analogous to Lemma 3.5). All in all we obtain that $|X_{G_n}/p^k|$ and $|X'_{G_n}/p^k|$ are equal up to a certain error term which does not affect the leading terms in the above growth formulas, therefore matching up the rank and m_0-invariant of X and X'.

We will now make this more precise. For the first step, we first choose $k = n$ in the above explanation; this will be eventually larger than the m_0-invariant of both X and X'. We start with three auxiliary lemmas.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Lemma 6.1. *Let M be a finitely generated Λ_d-module, and let $r = \operatorname{rank}_{\Lambda_d}(M)$. Then*

$$|v_p(|M_{G_n}/p^n|) - \left(r \cdot np^{dn} + m_0(M) \cdot p^{dn}\right)| = O(np^{(d-1)n}).$$

Proof. See [50, Théorème 2.1 (ii)]. □

Let $E_M = \bigoplus_{i=1}^{s} \Lambda_d/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda_d/(h_j^{n_j})$ be an elementary Λ_d-module attached to M. Then $m_0(M) = \sum_i m_i$ by the definitions. Now let $k \in \mathbb{N}$ be arbitrary, but fixed. Then we define a truncated m_0-invariant by

$$m_0^{(k)}(M) := \sum_{i=1}^{s} \min(k, m_i).$$

Note: If M is Λ_d-torsion, then $m_0^{(k)}(M) = m_0(M/p^k)$ for each $k \in \mathbb{N}$.

Corollary 6.2. *Let M be as in Lemma 6.1, and let $k \in \mathbb{N}$ be arbitrary but fixed. Suppose that M is Λ_d-torsion. Then*

$$|v_p(|M_{G_n}/p^k|) - m_0^{(k)}(M)p^{dn}| = O(np^{(d-1)n}).$$

Proof. We apply Lemma 6.1 to the module M/p^k, noting that

$$M_{G_n}/p^k = (M/p^k)_{G_n}/p^n$$

for each $n \geq k$. □

The next result which we need is a control theorem that was proved by Lim. Recall that $X = X^{str}(E_1/\mathbb{L}_\infty)$. For each n, we let $X_n = X^{str}(E_1/\mathbb{L}_n)$ for brevity.

Lemma 6.3. *Suppose that no prime in S is completely split in $\mathbb{L}_\infty$, and fix some integer k. Then*

$$|v_p(|X_{G_n}/p^k|) - v_p(|X_n/p^k|)| = O(p^{n(d-1)})$$

and

$$|v_p(|X_{G_n}/p^n|) - v_p(|X_n/p^n|)| = O(np^{n(d-1)}).$$

A similar result holds for $X' = X(E_2/\mathbb{L}_\infty)$.

Proof. It has been shown in the proof of [39, Proposition 4.1.3] on page 1174 of loc. cit. that the kernels and cokernels of the maps

$$t_{n,k} \colon X_{G_n}/p^k \longrightarrow X_n/p^k$$

are finite abelian p-groups and that the p-ranks of these groups are in $O(p^{n(d-1)})$ where the implicit constant does not depend on n or k. Here, we mean by the p-rank of a finite abelian p-group A the dimension of A/p over the field $\mathbb{F}_p$ with p elements, as in Definition 2.5.

This immediately gives the first claim (for fixed k). In order to obtain the second claim, we let $k = n$ (recall that the p-ranks of the kernels and cokernels are bounded independently in k). □

Let $X^{str}(E_j[p^k]/\mathbb{L}_n)$ be the Pontryagin dual of $\mathrm{Sel}^{str}(E_j[p^k]/\mathbb{L}_n)$. We also need the following lemma.

Lemma 6.4. *Suppose that no prime in S is completely split in the $\mathbb{Z}_p^d$-extension $\mathbb{L}_\infty/K$, and fix some integer k. Then the number of primes above some $v \in S$ in $\mathbb{L}_n$ is $O(p^{n(d-1)})$,*

$$|v_p(|X_n/p^k|) - v_p(|X^{str}(E_1[p^k]/\mathbb{L}_n)|)| = O(p^{(d-1)n})$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

and

$$|v_p(|X_n/p^n|) - v_p(|X^{str}(E_1[p^n]/\mathbb{L}_n)|)| = O(np^{(d-1)n}).$$

A similar result holds for $X' = X^{str}(E_2/\mathbb{L}_\infty)$.

Proof. Again, we refer the reader to the proof of [39, Proposition 4.1.3] on page 1174 of loc. cit. □

In order to obtain a better error term, we will use the following variant of that lemma.

Lemma 6.5. *Let* $\mathbb{L}_\infty/K$ *be a* $\mathbb{Z}_p^d$*-extension, and suppose that the following hypotheses hold.*

(i) E_1 *satisfies condition* $(\star)$ *from the introduction for all* $v \in S$.
(ii) The decomposition subgroups $D_v(\mathbb{L}_\infty/K) \subseteq \mathrm{Gal}(\mathbb{L}_\infty/K)$ *have* $\mathbb{Z}_p$*-ranks at least two for each* $v \in S_p$.

Then the natural map

$$s_n : X_n/p^n \longrightarrow X^{str}(E_1[p^n]/\mathbb{L}_n)$$

has finite kernel and cokernel, and the p-valuation of the order of the kernel and cokernel of s_n *is in* $O(np^{(d-2)n})$.

A similar result holds for $X' = X^{str}(E_2/\mathbb{L}_\infty)$.

Proof. By Lemma 2.1, we may assume that S is precisely the set of primes of K which lie above p or where E has bad reduction. Let S_n be the set of primes of $\mathbb{L}_n$ above those in S and let $S_{p,n}$ be the primes of $\mathbb{L}_n$ above p. Consider the maps

$$\theta_n : \bigoplus_{w \in S_{p,n}} H^1(\mathbb{L}_{n,w}, \tilde{E}[p^n]) \longrightarrow \bigoplus_{w \in S_{p,n}} H^1(\mathbb{L}_{n,w}, \tilde{E}[p^\infty])[p^n],$$

$$\psi_n : \bigoplus_{w \in S_n \setminus S_{p,n}} H^1(\mathbb{L}_{n,w}, E[p^n]) \longrightarrow \bigoplus_{w \in S_n \setminus S_{p,n}} H^1(\mathbb{L}_{n,w}, E[p^\infty])[p^n].$$

As in the proof of [39, Proposition 4.1.3], we see that to prove the lemma we must show that $v_p(|\ker \theta_n|) = O(np^{(d-2)n})$ and $v_p(|\ker \psi_n|) = O(np^{(d-2)n})$. Condition (ii) implies that the number of primes of $\mathbb{L}_n$ above any prime in S_p is $O(p^{(d-2)n})$. Then as is the proof of loc. cit., this immediately proves that $v_p(|\ker \theta_n|) = O(np^{(d-2)n})$.

We now turn to $\ker \psi_n$. We now show that condition (i) of the lemma implies that $H^1(\mathbb{L}_{n,w}, E[p^n]) = 0$ for all $n \geq 0$ and $w \in S_n \setminus S_{p,n}$. This implies that $\ker \psi_n = 0$. Let $n \geq 0$ and $w \in S_n \setminus S_{p,n}$. Then we have an exact sequence

$$0 \longrightarrow E(\mathbb{L}_{n,w})/p^n \longrightarrow H^1(\mathbb{L}_{n,w}, E[p^n]) \longrightarrow H^1(\mathbb{L}_{n,w}, E)[p^n] \longrightarrow 0.$$

By Mattuck's Theorem, we have that $E(\mathbb{L}_{n,w}) \cong \mathbb{Z}_l^d \times T$, where l is the residue characteristic of $\mathbb{L}_{n,w}$, $d = [\mathbb{L}_{n,w} : \mathbb{Q}_l]$ and T is a finite group. Since $l \neq p$, we have $E(\mathbb{L}_{n,w})/p^n \cong E(\mathbb{L}_{n,w})[p^n]$. By Tate duality for abelian varieties over local fields (see [44, Corollary I-3.4]), we have an isomorphism $H^1(\mathbb{L}_{n,w}, E)^\vee \cong E(\mathbb{L}_{n,w})$. Therefore, $(H^1(\mathbb{L}_{n,w}, E)[p^n])^\vee \cong E(\mathbb{L}_{n,w})/p^n$. So as above we have $H^1(\mathbb{L}_{n,w}, E)[p^n] \cong (H^1(\mathbb{L}_{n,w}, E)[p^n])^\vee \cong E(\mathbb{L}_{n,w})[p^n]$. Combining the two previous facts with the exact sequence above, we see that $|H^1(\mathbb{L}_{n,w}, E[p^n])| = |E(\mathbb{L}_{n,w})[p^n]|^2$.

The proof of Proposition 3.2 shows that condition (i) implies that $E(K_v)[p^\infty] = 0$ where v is the prime of K below w. So $(E(\mathbb{L}_{n,w})[p^\infty])^{\mathrm{Gal}(\mathbb{L}_{n,w}/K_v)} = E(K_v)[p^\infty] = 0$. Therefore, $E(\mathbb{L}_{n,w})[p^\infty] = 0$ whence by the result above $H^1(\mathbb{L}_{n,w}, E[p^n]) = 0$. This completes the proof. □

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Now suppose that $E_1[p^n] \cong E_2[p^n]$ for all $n \in \mathbb{N}$ (we will relax drastically this assumption below). Then it follows from Lemmas 6.1, 6.3, and 6.4 that

$$| \left(rnp^{dn} + m_0(X)p^{dn}\right) - \left(r'np^{dn} + m_0(X')p^{dn}\right) | = O(np^{n(d-1)}).$$

Here, we let $r = \operatorname{rank}_{\Lambda_d}(X)$ and $r' = \operatorname{rank}_{\Lambda_d}(X')$. This immediately implies that $r = r'$, and that $m_0(X) = m_0(X')$.

Now we improve on the above approach. First, we want to get rid of the assumption that $E_1[p^n] \cong E_2[p^n]$ for *all* n. Second, we would like to say something about l_0-invariants.

To the first aim, we suppose from now on that X and X' are both torsion Λ_d-modules. Instead of choosing $k = n$ in the above quotients, we let k vary from 1 to $m_0(X) + 1$ (it suffices to replace $m_0(X)$ by the exponent $e(X)$ of X, see below). Using Corollary 6.2 and the first formulas in Lemmas 6.3 and 6.4, we obtain that for each such k we have

$$\left|\left(m_0^{(k)}(X)p^{dn}\right) - \left(m_0^{(k)}(X')p^{dn}\right)\right| = O(p^{n(d-1)}).$$

Now suppose that $E_1[p^i] \cong E_2[p^i]$ for some $i > e(X)$ (here $e(X)$ means the maximum of the exponents m_i in the elementary Λ_d-module attached to M, as in Definition 4.2). Then $m_0^{(k)}(X) = m_0^{(k)}(X')$ for each $k \leq e(X) + 1$. In particular,

$$m_0^{(e(X)+1)}(X') = m_0^{(e(X)+1)}(X) = m_0^{(e(X))}(X) = m_0^{(e(X))}(X').$$

This shows that $m_0(X') = m_0(X)$ and that in fact the p-torsion submodules of the elementary Λ_d-modules attached to X and X' are isomorphic, that is, $X[p^\infty]$ is pseudo-isomorphic to $X'[p^\infty]$. We summarize this result as

Theorem 6.6 (Lim). *Let $\mathbb{L}_\infty/K$ be a $\mathbb{Z}_p^d$-extension such that no prime in S is totally split in $\mathbb{L}_\infty$. Suppose that $X = X^{str}(E_1/\mathbb{L}_\infty)$ and $X' = X^{str}(E_2/\mathbb{L}_\infty)$ are both Λ_d-torsion modules, and that $E_1[p^i] \cong E_2[p^i]$ for some $i > e(X)$.*

Then there exists a pseudo-isomorphism

$$X[p^\infty] \sim X'[p^\infty],$$

and in particular we have $m_0(X) = m_0(X')$.

In order to reach the second aim formulated above, we first have to formulate more precise asymptotic growth formulas. We will use a formula which has been obtained by the first-named author and Katharina Müller in [34], generalizing work of Cuoco and Monsky from [11]. In order to formulate the result, we have to introduce some notation from [11].

In the asymptotic formula which we will use, the coinvariant modules X_{G_n} are replaced by certain smaller quotients, which are a bit involved to introduce. For the convenience of the reader, we provide a definition from scratch. Recall that Λ_d has been identified with $\mathbb{Z}_p[[T_1, \ldots, T_d]]$ by mapping a set of topological generators $\gamma_1, \ldots, \gamma_d$ of $G \cong \mathbb{Z}_p^d$ to the elements $T_1 + 1, \ldots, T_d + 1$. For any element $\sigma \in G \setminus G^p$, we can introduce a variable $S = \sigma - 1$ in Λ_d. We consider the polynomials

$$\omega_0(S) := S, \quad \omega_n(S) := (S+1)^{p^n} - 1, \ n \geq 1, \quad \nu_n(S) := \frac{\omega_{n+1}(S)}{\omega_n(S)},$$

where n is any natural number. Moreover, we also let, for two natural numbers $n \geq m$,

$$\nu_{n,m}(S) := \frac{\omega_n(S)}{\omega_m(S)} = \nu_{n-1}(S) \cdot \nu_{n-2}(S) \cdot \ldots \cdot \nu_m(S).$$

Following [11, Definitions 4.1 and 4.6], we define

Definition 6.7. *Let M be a finitely generated torsion Λ_d-module. A structure $\mathcal{S}$ on M consists of an integer $\nu \geq 0$ and a finite set of tuples (σ_i, M_i), where $\sigma_i \in G \setminus G^p$ and $M_i \subseteq M$ is a submodule for each i.*

For each $n \in \mathbb{N}$ let $I_n \subseteq \Lambda_d$ be the ideal generated by $\omega_n(T_1), \ldots, \omega_n(T_d)$.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Given a structure $\mathcal{S}$ on M, we define $J_n = J_n(\mathcal{S})$ to be the submodule of M generated by $I_n \cdot M$ and $\sum_i \nu_{n,\nu}(S_i) \cdot M_i$, where the sum runs over all pairs (σ_i, M_i) in $\mathcal{S}$ and $S_i = \sigma_i - 1$ for each i.

A structure $\mathcal{S}$ is called admissible on M if

$$\operatorname{rank}_{\mathbb{Z}_p}(M/J_n) = O(p^{(d-2)n}).$$

Remark 6.8. *The quotients M_{G_n} of coinvariants considered in the asymptotic formula in Lemma 6.1 correspond to the quotients M/I_n, since I_n is just the augmentation ideal of the subgroup $G_n = G^{p^n} \subseteq G$ in Λ_d. Therefore, these quotients correspond to the 'empty structure' on M, that is, $J_n = I_n \cdot M$ and there are no additional submodules M_i of M. Unfortunately, this structure is not always admissible in the above sense.*

Suppose now that we are given a finitely generated and torsion Λ_d-module M. Let us briefly describe how one can come up with an admissible structure on M.

Let E_M be an elementary torsion Λ_d-module attached to M. As in the introduction, we write

$$E_M = \bigoplus_{i=1}^{s} \Lambda_d/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda_d/(h_j^{n_j}),$$

where the power series $h_1, \ldots, h_t$ are irreducible and coprime with p. Recall that the characteristic power series f_M of M is just the same as $p^{m_0(M)} \cdot \prod_{j=1}^{t} h_j^{n_j}$. It follows from [11, Theorem 3.13] that the empty structure (see also Remark 6.8) is admissible on M as long as no irreducible element h_j is a *special prime* element. By this, Cuoco and Monsky mean the following:

Definition 6.9. *A prime element $h \in \Lambda_d = \mathbb{Z}_p[[G]]$ is called special if there exists some $\sigma \in G \setminus G^p$ such that for $S = \sigma - 1$ we have either*

(1) $h = S$ or
(2) $h = \nu_r(S)$ for some $r \in \mathbb{N}$.

It remains to define an admissible structure on M if some of the irreducible elements h_j dividing the characteristic power series f_M of M are special. Suppose first that $M = E_M = \Lambda_d/(h^n)$ for some special prime h. We let σ be the corresponding group element, and we define $\mathcal{S}$ to be the one element structure $(\nu, \{(\sigma, M)\})$, where $\nu = 0$ in case (1) and $\nu = r$ in case (2). In other words, we define

$$J_n = I_n \cdot M + \nu_{n,\nu}(S) \cdot M,$$

where the choice of ν depends on the type of the special prime h, as described above. It is easy to see that $\operatorname{rank}_{\mathbb{Z}_p}(M/J_n) = O(p^{(d-2)n})$ with that choice of $\mathcal{S}$, that is, this structure is admissible on $M = \Lambda_d/(h^n)$.

Now suppose that $M = E_M = \bigoplus_{i=1}^{s} \Lambda_d/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda_d/(h_j^{n_j})$. In this case, we let (without loss of generality) $M_1, \ldots, M_c$ be the cyclic submodules $\Lambda_d/(h_i^{n_i})$ such that $h_1, \ldots, h_c$ are special. For each such i, let $S_i = \sigma_i - 1$ be the corresponding variable and choose $r_i = 0$ or $r_i = r$ depending on whether we have a first case special prime or a second case special prime, and let $\hat{r} = \max(r_1, \ldots, r_c)$. Note that $\hat{r}$ is the smallest number such that $\nu_{\hat{r}}(S_i)$ is coprime with each $h_i \in \mathbb{Z}_p[S_i]$. This is what makes the following structure admissible: We take

$$\mathcal{S} = (\hat{r}, \{(\sigma_1, M_1), (\sigma_2, M_2), \ldots, (\sigma_c, M_c)\}), \tag{8}$$

where $M_i = \Lambda_d/(h_i^{n_i})$, respectively.

If M is not an elementary Λ_d-module, then we proceed via a 'dirty trick', by applying the following result of Cuoco and Monsky (see [11, Theorem 4.12]).

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Proposition 6.10. *Let M and M' be two pseudo-isomorphic torsion Λ_d-modules, and let $\mathcal{S}$ and $\mathcal{S}'$ be any admissible structures on M and M', with attached quotients M/J_n and M'/J'_n. Then*

$$|v_p(|(M/J_n)[p^\infty]|) - v_p(|(M'/J'_n)[p^\infty]|)| = O(p^{(d-1)n}).$$

Since we will be interested in the growth of the orders of our quotients only up to an error of $O(p^{(d-1)n})$ (see also Lemma 6.12 below), we can now proceed as follows: If M is not elementary, then we just replace M by E_M and choose the admissible structure on E_M which has been defined above. It follows from the above proposition that it suffices to study the growth of $v_p(|E_M/J_n|)$ for this particular structure. In other words, we do not have to think too much about a particular choice of admissible structure on M if M is not elementary.

The following result of Cuoco and Monsky will allow us to simplify the definition of the structure as given in (8).

Proposition 6.11. *Let $\mathcal{S}$ be an admissible structure on M, and let $J_n(\mathcal{S}) \subseteq M$ be the corresponding submodules used in the quotients. Let $\mathcal{S}'$ be the new structure which is obtained from $\mathcal{S}$ by replacing M_1 by M, and let $J'_n := J_n(\mathcal{S}')$ be the corresponding submodules. Then $\mathcal{S}'$ is also admissible, and*

$$|v_p(|(M/J_n)[p^\infty]|) - v_p(|(M/J'_n)[p^\infty]|)| = O(p^{(d-1)n}).$$

Proof. It is obvious that $\mathcal{S}'$ is again admissible, since we are making the quotients M/J_n even smaller. Now apply [11, Lemma 4.9]. □

Applying this proposition iteratively, we can replace the structure $\mathcal{S}$ from (8) by the easier structure

$$S' = (\hat{r}, \{(\sigma_1, M), (\sigma_2, M), \ldots, (\sigma_c, M)\}),$$

which we will denote by $\mathcal{S}$ again in what follows. Note that the quotients M/J_n with respect to this structure are just $M/(\mathcal{I}_n \cdot M)$, where

$$\mathcal{I}_n = \mathcal{I}_n(\mathcal{S}) = I_n + (\nu_{n,\hat{r}}(S_1), \ldots, \nu_{n,\hat{r}}(S_c)). \tag{9}$$

Now we turn to the study of l_0-invariants. We can formulate the following asymptotic formula from [34].

Lemma 6.12. *Let M be a finitely generated and torsion Λ_d-module, and consider the quotients M/J_n attached to an admissible structure $\mathcal{S}$ on M, as described above. Then*

$$\left|v_p(|M/J_n/p^n|) - \left(m_0(M) \cdot p^{dn} + l_0(M) \cdot np^{(d-1)n}\right)\right| = O(p^{(d-1)n}).$$

Proof. It follows from [34, Lemma 5.12] that

$$\left|v_p(|(M/J_n)[p^\infty]/p^n|) - \left(m_0(M) \cdot p^{dn} + l_0(M) \cdot np^{(d-1)n}\right)\right| = O(p^{(d-1)n}).$$

Since $\mathcal{S}$ is admissible, we have $\operatorname{rank}_{\mathbb{Z}_p}(M/J_n) = O(p^{(d-2)n})$, and therefore we may replace $(M/J_n)[p^\infty]$ by M/J_n in the above asymptotic formula. □

The last ingredient which will be needed is the following control theorem. By an identical proof to [34, Theorem 6.8], we have

Proposition 6.13. *Let $\mathbb{L}_\infty/K$ be a $\mathbb{Z}_p^d$-extension with intermediate number fields $\mathbb{L}_n$ as above, let E be an elliptic curve with good ordinary reduction at p and suppose that no prime of S splits completely in $\mathbb{L}_\infty$. Then the kernels and the cokernels of the natural maps*

$$s_n \colon X_{G_n} \longrightarrow X_n$$

are finite. Moreover, the p-valuations of the orders of the kernels and cokernels are in $O(p^{(d-1)n})$.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Corollary 6.14. *In the setting of the previous proposition, let $\mathcal{S}$ be an admissible structure on $X = X^{str}(E/\mathbb{L}_\infty)$, with corresponding quotients $X/\mathcal{I}_n$, where the ideals $\mathcal{I}_n \subseteq \Lambda_d$ are defined as in (9). Then the kernels and cokernels of the induced maps*

$$t_n : X/\mathcal{I}_n \longrightarrow X_n/\mathcal{I}_n$$

are finite, and the p-valuations of their orders are in $O(p^{(d-1)n})$.

Note that $I_n \subseteq \mathcal{I}_n$ operates trivially on $X_n = X^{str}(E/\mathbb{L}_n)$, that is,

$$X/\mathcal{I}_n = X_n/(\nu_{n,\hat{r}}(S_1), \ldots, \nu_{n,\hat{r}}(S_c)).$$

Proof. Consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_n \cdot X_{G_n} & \longrightarrow & X_{G_n} & \longrightarrow & X_{G_n}/I_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle r_n} & & \downarrow{\scriptstyle s_n} & & \downarrow{\scriptstyle t_n} & & \\ 0 & \longrightarrow & I_n \cdot X_n & \longrightarrow & X_n & \longrightarrow & X_n/I_n & \longrightarrow & 0 \end{array}$$

Let t be the number of generators of $\mathcal{I}_n$ (note that each of these ideals has the same number of generators). Then it follows from the snake lemma that

$$|\mathrm{coker}(t_n)| \leq |\mathrm{coker}(s_n)|$$

and

$$|\ker(t_n)| \leq |\ker(s_n)| \cdot |\mathrm{coker}(r_n)|.$$

Since $\mathrm{coker}(r_n) = \mathcal{I}_n \cdot \mathrm{coker}(s_n)$, we may conclude that

$$|\ker(t_n)| \leq |\ker(s_n)| \cdot |\mathrm{coker}(s_n)|^t.$$

Therefore, the statement of the corollary follows from Proposition 6.13. □

Now assume that the hypotheses (*i*) and (*ii*) from Lemma 6.5 are satisfied. Then Lemma 6.5 implies that

$$|v_p(|X_n/p^n|) - v_p(|X^{str}(E_1[p^n]/\mathbb{L}_n)|)| = O(np^{(d-2)n}). \tag{10}$$

If we assume that $E_1[p^n] \cong E_2[p^n]$ for each $n \in \mathbb{N}$ (here we will not be able to relax this assumption), then we may conclude as in Lemma 3.5 that

$$X^{str}(E_1[p^n]/\mathbb{L}_n) \cong X^{str}(E_2[p^n]/\mathbb{L}_n). \tag{11}$$

Choose a structure $\mathcal{S}$ which is admissible on both X and X'. Then we may use the same arguments as in the proof of Corollary 6.14 to derive from (10) and (11) that

$$\left|v_p(|(X_n/J_n)/p^n|) - v_p(|(X'_n/J_n)/p^n|)\right| = O(np^{(d-2)n}).$$

Then it follows from Lemma 6.12 and Corollary 6.14 that

$$\left|\left(m_0(X)p^{dn} + l_0(X)np^{(d-1)n}\right) - \left(m_0(X')p^{dn} + l_0(X')np^{(d-1)n}\right)\right| = O(p^{(d-1)n}).$$

This (together with Theorem 6.6) proves the following

Theorem 6.15. *Let $\mathbb{L}_\infty/K$ be a $\mathbb{Z}_p^d$-extension such that no prime of S splits completely in $\mathbb{L}_\infty$. We assume that the following hypotheses are satisfied.*

(a) $E_1[p^n] \cong E_2[p^n]$ *for every* $n \in \mathbb{N}$.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

(b) E_1 and E_2 satisfy condition $(\star)$ from the introduction for all $v \in S$.
(c) The decomposition subgroups $D_v(\mathbb{L}_\infty/K) \subseteq \mathrm{Gal}(\mathbb{L}_\infty/K)$ have $\mathbb{Z}_p$-ranks at least two for each $v \in S_p$.

Then

$$\mathrm{rank}_{\Lambda_d}(X) = \mathrm{rank}_{\Lambda_d}(X').$$

If these ranks are equal to 0, then

(i) $m_0(X) = m_0(X')$ and
(ii) $l_0(X) = l_0(X')$.

Remark 6.16. *Hypothesis (a) in Theorem 6.15 implies that the p-adic Tate modules of $E_1[p^\infty]$ and $E_2[p^\infty]$ are isomorphic. Indeed, letting C_n be the set of G_K-isomorphisms between $E_1[p^n]$ and $E_2[p^n]$, $n \in \mathbb{N}$, the assumption implies that each C_n is non-empty. Moreover, each C_n is finite because $E_1[p^n]$ is finite. It follows from [51, Proposition 1.1.4] that the inverse limit $C = \varprojlim_n C_n$, taken with regard to the restriction maps, is non-empty. Any element in C gives an isomorphism between the Tate modules.*

By results of Faltings on the Tate conjecture, it follows that there exists an isogeny of degree prime to p between E_1 and E_2.[1] But then the Iwasawa modules X and X' are isomorphic. Therefore, the conclusion of the theorem is not interesting under assumption (a).

7. Proof of the second main theorem

In this section, we will apply the up-down approach from the proof of Theorem 1.4 to the investigation of l_0-invariants. This will enable us to prove the second main result (Theorem 1.5) without assuming the strong hypothesis (a) from Theorem 6.15. Note that this comes at the price of the additional hypotheses (i) and (ii) in Theorem 1.5. These two assumptions, however, are natural and mild, as we pointed out in Section 1. On the other hand, we have seen in Remark 6.16 that the conclusion of the theorem is not interesting under hypothesis (a). As this is the best result that we can prove via Lim's approach, we apply the up-down approach instead in the current section.

In what follows, we will work with Greenberg Selmer groups.

Let $K_\infty \in \mathcal{E}$ be arbitrary, but fixed. The canonical restriction map $\mathrm{Gal}(\mathbb{L}_\infty/K) \twoheadrightarrow \mathrm{Gal}(K_\infty/K)$ induces a surjective homomorphism

$$\pi : \Lambda_d \cong \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}_\infty/K)]] \longrightarrow \Lambda \cong \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]].$$

We write the characteristic power series $f_1, f_2 \in \Lambda_d$ of $X^{Gr}(E_1/\mathbb{L}_\infty)$ and $X^{Gr}(E_2/\mathbb{L}_\infty)$ as

$$f_1 = p^{m_{0,1}} \cdot g_1, \quad f_2 = p^{m_{0,2}} \cdot g_2.$$

Then we have the following auxiliary result which will be one of the main ingredients in the proof of Theorem 1.5.

Lemma 7.1. *In the above setting, suppose that $\pi(g_1) \not\equiv 0 \pmod p$. Then there exists a Greenberg neighborhood $U = \mathcal{E}(K_\infty, n)$ such that for any $\tilde{K}_\infty \in U$ we have $\tilde{\pi}(g_1) \not\equiv 0 \pmod p$ where*

$$\tilde{\pi} : \Lambda_d \cong \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}_\infty/K)]] \longrightarrow \Lambda \cong \mathbb{Z}_p[[\mathrm{Gal}(\tilde{K}_\infty/K)]]$$

is the surjective homomorphism induced by the canonical restriction map $\mathrm{Gal}(\mathbb{L}_\infty/K) \twoheadrightarrow \mathrm{Gal}(\tilde{K}_\infty/K)$.

Proof. We can choose the variables $T_1, T_2, \ldots, T_d$ of Λ_d such that the map π is given by

$$\pi(T_1) = \pi(T_2) = \cdots = \pi(T_{d-1}) = 0, \quad \pi(T_d) = T \in \Lambda = \mathbb{Z}_p[[T]]$$

[1] The authors are grateful to the editor for pointing out this connection.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

(this choice of variables corresponds to a choice $\gamma_1, \gamma_2, \ldots, \gamma_d$ of topological generators of G such that $\mathrm{Gal}(\mathbb{L}_\infty/K_\infty) = \langle \gamma_1, \gamma_2, \ldots, \gamma_{d-1} \rangle$, and $T_i = \gamma_i - 1$ for each i). Since $\pi(g_1) \not\equiv 0 \pmod{p}$, the image $\pi(g_1) \in \Lambda$ is associated with a distinguished polynomial of degree, say, r by the Weierstraß Preparation Theorem. Now choose $U = \mathcal{E}(K_\infty, 2s)$, where s is large enough such that $p^s > r$. Then the proof of [3, Proposition 1.1] implies that

$$\tilde{\pi}(g_1) \equiv \pi(g_1) \mod (p^s, T^{p^s})$$

for every $\tilde{K}_\infty \in U$. In particular, $\tilde{\pi}(g_1) \not\equiv 0 \pmod{p}$ (in fact, $\tilde{\pi}(g_1)$ is also associated with a distinguished polynomial of degree r). □

Proposition 7.9 is a key result that allows us to use the up-down approach to prove Theorem 1.5. In order to prove this key result, we make use of the following auxiliary lemma. We start with a finitely generated torsion Λ_d-module M. Consider a presentation

$$\Lambda_d^g \xrightarrow{A} \Lambda_d^l \longrightarrow M \longrightarrow 0$$

of the Λ_d-module M. Since M is torsion, we know that $l \leq g$. Recall that the *Fitting ideal* of M over Λ_d is generated by the $l \times l$-minors of the matrix $A = (a_{ij})$, and that this ideal does not depend on the chosen presentation of M.

Lemma 7.2. *Let M be a torsion Λ_d-module with characteristic power series f, and let $f_1, \ldots, f_k$ be any set of generators of the Fitting ideal of M.*

(1) Then $f = \gcd(f_1, \ldots, f_k)$.
(2) Let $\pi : \Lambda_d \longrightarrow \Lambda$ be a surjective ring homomorphism, and suppose that $M_\pi := M/(\ker(\pi) \cdot M)$ is a torsion $\Lambda = \Lambda_d/\ker(\pi)$-module. Then the characteristic power series $f_\pi \in \Lambda$ of M_π satisfies

$$f_\pi = \gcd(\pi(f_1), \ldots, \pi(f_k)).$$

Proof. Since $\pi : \Lambda_d \longrightarrow \Lambda$ is surjective, the Λ-module M_π has a presentation

$$\Lambda^g \xrightarrow{\pi(A)} \Lambda^l \longrightarrow M_\pi \longrightarrow 0, \tag{12}$$

where we denote by $\pi(A)$ the matrix with entries $(\pi(a_{ij}))_{i,j}$ in Λ.

In order to prove assertion (1), we let $h \in \Lambda_d$ be any irreducible element (e.g. $h = p$) and consider the prime ideal $\mathfrak{p} = (h)$ in Λ_d. The localization $(\Lambda_d)_\mathfrak{p}$ of Λ_d at $\mathfrak{p}$ is a discrete valuation ring with maximal ideal $\mathfrak{p}$. Since M is a torsion Λ_d-module, we can attach to it an elementary torsion Λ_d-module and a short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow \bigoplus_{i=1}^{s} \Lambda_d/(p^{n_i}) \oplus \bigoplus_{j=1}^{t} \Lambda_d/(h_j(T)^{l_j}) \longrightarrow M_2 \longrightarrow 0,$$

where M_1 and M_2 are pseudo-null. The localized sequence remains exact, and $(M_1)_\mathfrak{p} = (M_2)_\mathfrak{p} = \{0\}$ (Indeed, since the M_i are pseudo-null, we can choose an element a in Λ_d which is coprime with h and annihilates both M_1 and M_2. But a becomes a unit in the localization $(\Lambda_d)_\mathfrak{p}$.). Therefore,

$$M_\mathfrak{p} \cong \bigoplus_{i=1}^{s} (\Lambda_d)_\mathfrak{p}/(p^{n_i}) \oplus \bigoplus_{j=1}^{t} (\Lambda_d)_\mathfrak{p}/(h_j(T)^{l_j}).$$

Note that $(\Lambda_d)_\mathfrak{p}/(\lambda) = \{0\}$ for each $\lambda \in \Lambda_d$ which is coprime with h. Therefore, $M_\mathfrak{p}$ is of the form

$$M_\mathfrak{p} \cong \bigoplus_{i=1}^{k} (\Lambda_d)_\mathfrak{p}/(h^{e_i})$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

(this sum might be empty, i.e. $k = 0$ is possible). In other words, the powers h^{e_i} are the principal divisors of $M_{\mathfrak{p}}$ as a module over the principal ideal domain $(\Lambda_d)_{\mathfrak{p}}$. □

Now we apply the following auxiliary result (see [4, Theorem 2.9.6]):

Lemma 7.3. *Let N denote a finitely generated torsion module over a principal ideal domain R, with matrix of relations B, and suppose that we are given a presentation*

$$R^g \xrightarrow{B} R^l \longrightarrow N \longrightarrow 0.$$

Then the product of the l principal divisors of N is equal to the greatest common divisor of the $l \times l$-minors of B.

We apply this lemma to the presentation

$$(\Lambda_d)_{\mathfrak{p}}^g \longrightarrow (\Lambda_d)_{\mathfrak{p}}^l \longrightarrow M_{\mathfrak{p}} \longrightarrow 0,$$

with matrix of relations A (viewed as a matrix with entries in the larger ring $(\Lambda_d)_{\mathfrak{p}}$). We may deduce that $e := \sum_{i=1}^{k} e_i$ is the exact exponent of the largest power of h which divides the greatest common divisor of the $l \times l$-minors of A. Since these minors generate the Fitting ideal of M, this also means that h^e is the exact power of h which divides the gcd of the generators $f_1, \ldots, f_k$ chosen above. Note that h^e is also the exact power of h which divides the characteristic power series f of M. Since h was arbitrary, this proves assertion (1).

In order to prove assertion (2), we start from the presentation (12) with the matrix $\pi(A)$. Now we proceed as above: Choose any irreducible element $h \in \Lambda$, and localize at $\mathfrak{p} = (h)$. Then we get

$$(M_\pi)_{\mathfrak{p}} \cong \bigoplus_{i=1}^{k} \Lambda_{\mathfrak{p}}/(h^{e_i})$$

for suitable $e_i \in \mathbb{N}$, and the powers h^{e_i} are the principal divisors of $(M_\pi)_{\mathfrak{p}}$ over $\Lambda_{\mathfrak{p}}$. An application of Lemma 7.3 then proves assertion (2).

We prove a corollary which will be used below.

Corollary 7.4. *Let M be a finitely generated torsion Λ_d-module, with characteristic power series f, and write $f = p^{m_0(M)} \cdot g$ as usual. Let $\pi : \Lambda_d \longrightarrow \Lambda$ be a surjective ring homomorphism, and write $M_\pi = M/(\ker(\pi) \cdot M)$ (this is a finitely generated Λ-module).*

If $d > 2$, then we assume that the maximal pseudo-null Λ_d-submodule M° of M is finitely generated over $\mathbb{Z}_p$. Then the following statements hold.

(a) If $\pi(f) \neq 0$, then M_π is a torsion Λ-module.
(b) Suppose that M_π is a torsion Λ-module. Then $\mu(M_\pi) = m_0(M)$ if and only if $\pi(g) \not\equiv 0 \pmod{p}$.

Proof. Let E_M be an elementary Λ_d-module attached to M, and consider an exact sequence

$$0 \longrightarrow M^\circ \longrightarrow M \longrightarrow E_M \longrightarrow P \longrightarrow 0,$$

where P is a pseudo-null Λ_d-module. This sequence shows that

$$\mathrm{Ann}(M^\circ) \cdot \mathrm{Ann}(E_M) \subseteq \mathrm{Ann}(M),$$

where we denote by $\mathrm{Ann}(Y)$ the annihilator ideal of any finitely generated Λ_d-module Y.

Now our assumption on M° implies that there exists an element $H \in \mathrm{Ann}(M^\circ)$ such that

$$\pi(H) \not\equiv 0 \pmod{p},$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

so in particular $\pi(H) \neq 0$ (cf. the proof of [35, Theorem 3.22]). Therefore, $\pi(H) \cdot \pi(f)$ yields a nonzero element in

$$\pi(\mathrm{Ann}(M)) \subseteq \mathrm{Ann}(M_\pi).$$

Choosing an elementary Λ-module E_π of M_π, the natural inclusion map $E_\pi \hookrightarrow M_\pi$ induces an inclusion

$$\mathrm{Ann}(M_\pi) \hookrightarrow \mathrm{Ann}(E_\pi) = (f_\pi),$$

where we denote by f_π the characteristic power series of M_π and E_π. Since $\pi(f)\pi(H) \neq 0$, we may conclude that $f_\pi \neq 0$, that is, M_π is a torsion Λ-module.

Now we turn to the proof of statement (b). Choose generators $f_1, \ldots, f_k$ of the Fitting ideal of M. We know from Lemma 7.2 that

$$\pi(f) = \pi(\gcd(f_1, \ldots, f_k)) \;\Big|\; \gcd(\pi(f_1), \ldots, \pi(f_k)) = f_\pi.$$

On the other hand, the first part of the proof shows that $f_\pi \mid (\pi(f) \cdot \pi(H))$. Summarizing, the chain of divisibilities

$$\pi(f) \;\Big|\; f_\pi \;\Big|\; (\pi(f)\pi(H))$$

shows that $\mu(M_\pi) > m_0$ if and only if $\pi(g)$ is divisible by p (recall that $\pi(H) \not\equiv 0 \pmod{p}$). □

Now we turn to the study of l_0-invariants and move on towards our key proposition. Let $X = X^{Gr}(E/\mathbb{L}_\infty)$ for some elliptic curve E which is defined over K and has good ordinary reduction at all primes of K above p. Let $f = p^{m_0(X)} \cdot g$ be the characteristic power series of X. If $l_0(g) > 0$, then there exists some element $\gamma \in \mathrm{Gal}(\mathbb{L}_\infty/K)$ which is not a p-th power, and such that the coset of $T := \gamma - 1$ in $\Omega_d = \Lambda_d/p$ divides the coset of g. If $\pi : \Lambda_d \longrightarrow \Lambda$ maps T to 0, then $\pi(g) \equiv 0 \pmod{p}$. For brevity, we introduce the following notion.

Definition 7.5. *Recall that $\mathcal{E}_p \cap \mathcal{E}_{ns}$ denotes the set of all $\mathbb{Z}_p$-subextensions $K_\infty \subseteq \mathbb{L}_\infty$ of K such that each prime above p ramifies in K_∞ and no prime of S splits completely in K_∞. We let $\mathcal{E}_\mu = \mathcal{E}_\mu(X)$ denote the subset of $\mathcal{E}_p \cap \mathcal{E}_{ns}$ which consists exactly of the $\mathbb{Z}_p$-extensions K_∞/K satisfying that $X^{Gr}(E/K_\infty)$ is Λ-torsion and*

$$\mu(X^{Gr}(E/K_\infty)) = m_0(X).$$

Remark 7.6. *Let $K_\infty \in \mathcal{E}$, let $\pi : \Lambda_d \longrightarrow \Lambda$ be the canonical surjection induced by the restriction map*

$$\mathrm{Gal}(\mathbb{L}_\infty/K) \longrightarrow \mathrm{Gal}(K_\infty/K),$$

and write $X_\pi = X/(\ker(\pi) \cdot X)$ as usual. We assume that $X^{Gr}(E/K_\infty)$ is a torsion Λ-module. In view of Corollary 3.7, this means that X_π is also Λ-torsion and that we have

$$\mu(X_\pi) = \mu(X^{Gr}(E/K_\infty))$$

as soon as $K_\infty \in \mathcal{E}_{ns}$. Therefore, any such K_∞ is contained in $\mathcal{E}_\mu$ if and only if

$$\mu(X_\pi) = m_0(X).$$

In fact, since $\pi(f)$ divides the characteristic power series of X_π in view of Lemma 7.2, we have that $\mu(X_\pi) \geq m_0(X)$ for any $\mathbb{Z}_p$-extension K_∞ such that X_π is Λ-torsion. Moreover, equality in this equation can hold only if

$$\pi(g) \not\equiv 0 \pmod{p}.$$

In general, the latter condition is not sufficient for ensuring $\mu(X_\pi) = m_0(X)$. We have shown in Corollary 7.4 above that it is also sufficient if hypothesis (ii) from Theorem 1.5 is satisfied.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Proposition 7.7. *Suppose that $\mathcal{E}_p$ and $\mathcal{E}_{ns}$ are non-empty and that $X = X^{Gr}(E/\mathbb{L}_\infty)$ is Λ_d-torsion. Then the subset $\mathcal{E}_\mu \subseteq \mathcal{E}$ is open and dense.*

Proof. First note that $\mathcal{E}_p \cap \mathcal{E}_{ns} \subseteq \mathcal{E}$ is an open subset with respect to Greenberg's topology. Indeed, suppose that $K_\infty \in \mathcal{E}_p \cap \mathcal{E}_{ns}$. Let $m \in \mathbb{N}$ be large enough such that

(i) each prime of K above p ramifies in the m-th layer K_m of K_∞, and
(ii) no prime in S splits completely in K_m/K.

Then it is easy to see that $\mathcal{E}(K_\infty, m) \subseteq \mathcal{E}_p \cap \mathcal{E}_{ns}$.

Now fix $K_\infty \in \mathcal{E}_\mu$, with homomorphism π. In particular, we have that $E(K_\infty)[p^\infty]$ is finite (see [17, Prop. 3.2(ii)]). Then taking into account Propositions 2.2 and 2.3(c), it follows from [32, Theorem 4.11] that there exists a neighborhood $\mathcal{E}(K_\infty, n)$ which is contained in $\mathcal{E}_p \cap \mathcal{E}_{ns}$ such that for each $\tilde{K}_\infty \in \mathcal{E}(K_\infty, n)$, with homomorphism $\tilde{\pi}$, we have that $X^{Gr}(E/\tilde{K}_\infty)$ is Λ-torsion and

$$\mu(X_{\tilde{\pi}}) = \mu(X^{Gr}(E/\tilde{K}_\infty)) \leq \mu(X^{Gr}(E/K_\infty)) = \mu(X_\pi) = m_0(X).$$

Since it is a general fact that $\mu(X_{\tilde{\pi}}) \geq m_0(X)$ (see also Remark 7.6), we may conclude that

$$\tilde{K}_\infty \in \mathcal{E}_\mu$$

for each $\tilde{K}_\infty \in \mathcal{E}(K_\infty, n)$, that is, $\mathcal{E}_\mu$ is open with respect to Greenberg's topology.

Let us now prove denseness. We will apply the following

Lemma 7.8. *Let $\mathcal{E}$ be the set of $\mathbb{Z}_p$-extensions of K which are contained in some fixed $\mathbb{Z}_p^d$-extension $\mathbb{L}_\infty/K$. Suppose we are given finitely many $\mathbb{Z}_p^{d-1}$-subextensions $\mathbb{L}^{(1)}, \ldots, \mathbb{L}^{(r)} \subseteq \mathbb{L}_\infty$ of K. Let $\tilde{\mathcal{E}} \subseteq \mathcal{E}$ denote the subset of $\mathbb{Z}_p$-extensions of K which are not contained in any of the $\mathbb{L}^{(i)}$.*

Then each Greenberg open neighborhood $U = \mathcal{E}(K_\infty, n)$, $K_\infty \in \mathcal{E}$, and $n \in \mathbb{N}$, contains an element of $\tilde{\mathcal{E}}$, that is, $\tilde{\mathcal{E}} \subseteq \mathcal{E}$ lies dense with respect to Greenberg's topology.

Proof. Let $K_\infty \in \mathcal{E}$, $n \in \mathbb{N}$ be arbitrary. First assume that K_∞ itself is contained in $\tilde{\mathcal{E}}$. Then we choose $n \in \mathbb{N}$ large enough to ensure that the n-th layer K_n of K_∞ is not contained in $\mathbb{L}^{(i)}$ for any i, and we let $U = \mathcal{E}(K_\infty, n)$. In this case, we actually have $\mathcal{E}(K_\infty, n) \subseteq \tilde{\mathcal{E}}$.

Now suppose that $K_\infty \notin \tilde{\mathcal{E}}$. Then K_∞ is contained in at least one of the $\mathbb{Z}_p^{d-1}$-extensions $\mathbb{L}^{(1)}, \ldots, \mathbb{L}^{(r)}$ of K.

Choose any $F \in \tilde{\mathcal{E}}$, and consider the $\mathbb{Z}_p^2$-extension $K_\infty \cdot F$ of K (note that $K_\infty \neq F$ since we assumed that $K_\infty \notin \tilde{\mathcal{E}}$). Then $F \cap \mathbb{L}^{(i)}$ is a finite extension of K for each $i \in \{1, \ldots, r\}$. Therefore, $K_\infty \cdot F$ contains at most r different $\mathbb{Z}_p$-extensions of K which are *not* contained in $\tilde{\mathcal{E}}$: Indeed, if $M^{(1)}, \ldots, M^{(r+1)} \subseteq K_\infty F$ are not contained in $\tilde{\mathcal{E}}$, then there exist numbers $i \neq j \in \{1, \ldots, r+1\}$ and $s \in \{1, \ldots, r\}$ such that both $M^{(i)}$ and $M^{(j)}$ are contained in $\mathbb{L}^{(s)}$. But then $M^{(i)} \cdot M^{(j)} \subseteq \mathbb{L}^{(s)}$. Since we necessarily have $M^{(i)} \cdot M^{(j)} = K_\infty \cdot F$, this contradicts the fact that $(F \cap \mathbb{L}^{(s)})/K$ is finite.

Since $K_\infty F \cap \mathcal{E}(K_\infty, n)$ is infinite for each $n \in \mathbb{N}$, this concludes the proof of Lemma 7.8. □

This also concludes the proof of Proposition 7.7. Indeed, since $\mathcal{E}_p$ and $\mathcal{E}_{ns}$ are non-empty, we know that each $\mathbb{Z}_p$-extension which is not contained in $\mathcal{E}_p \cap \mathcal{E}_{ns}$ is contained in a finite set of $\mathbb{Z}_p^{d-1}$-extensions (or smaller multiple $\mathbb{Z}_p$-extensions of K), namely, the inertia and decomposition subfields of $\mathbb{L}_\infty$ of the primes above p (respectively, the primes in S). Since X is Λ_d-torsion, we know from Lemma 5.1 that $X^{Gr}(E/K_\infty)$ is Λ-torsion and that $\mu(X^{Gr}(E/K_\infty)) = m_0(X)$ for all $\mathbb{Z}_p$-extensions K_∞ of K outside of a certain finite number of $\mathbb{Z}_p^{d-1}$-extensions of K. Therefore, we can consider $\tilde{\mathcal{E}} = \mathcal{E}_\mu(X)$ in Lemma 7.8. □

Now we can prove our key auxiliary result. Recall that we write the characteristic power series of X as $f = p^{m_0(X)} \cdot g$.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Proposition 7.9. *Let $X = X^{Gr}(E/\mathbb{L}_\infty)$, let $\gamma \in \mathrm{Gal}(\mathbb{L}_\infty/K)$ be an element which is not a p-th power, and set $T = \gamma - 1$. We let $M = \mathbb{L}_\infty^{\langle T+1\rangle}$, and we suppose that $\overline{T}^e \mid \overline{g}$ for some $e \in \mathbb{N}$ (note that $e = 0$ is possible – in that case assertion (a) below is empty).*

(a) Let $K_\infty \subseteq M$ be any $\mathbb{Z}_p$-extension of K contained in $\mathcal{E}_{ns}$. Then there exists a constant C such that for $n \gg 0$

$$\lambda(X^{Gr}(E/\tilde{K}_\infty)) \geq e \cdot p^n - C$$

for each $\tilde{K}_\infty \in \mathcal{E}(K_\infty, n)$ which is contained in $\mathcal{E}_\mu$.

(b) If $d > 2$, then we assume that

- *$X = X^{Gr}(E/\mathbb{L}_\infty)$ is Λ_d-torsion,*
- *the maximal pseudo-null submodule of X is finitely generated over $\mathbb{Z}_p$,*
- *$\mathcal{E}_p \cap \mathcal{E}_{ns} \subseteq \mathcal{E}$ is non-empty, and*
- *$\overline{T}^{e+1} \nmid \overline{g}$.*

Then there exists a $\mathbb{Z}_p^2$-extension N of K and a $\mathbb{Z}_p$-extension $K_\infty \in \mathcal{E}_\mu$ such that $K_\infty \subseteq N \cap M$ and there exists a constant C' such that for $n \gg 0$

$$\lambda(X^{Gr}(E/\tilde{K}_\infty)) \leq e \cdot p^n + C'$$

for each $\tilde{K}_\infty \in \mathcal{E}(K_\infty, n) \setminus \mathcal{E}(K_\infty, n+1)$ which is a subextension of N and contained in $\mathcal{E}_\mu$. In particular, if $\overline{T}$ does not divide $\overline{g}$, that is, $e = 0$, then for $n \gg 0$

$$\lambda(X^{Gr}(E/\tilde{K}_\infty)) = O(1).$$

Proof. Let $K_\infty \subseteq M$ be any $\mathbb{Z}_p$-extension of K contained in $\mathcal{E}_{ns}$, say, $K_\infty = \mathbb{L}_\infty^{\langle T+1, T_2+1, \ldots, T_{d-1}+1\rangle}$ for suitable variables $T_2, \ldots, T_{d-1}$, and write $T_i + 1 = \gamma_i$ for each i (in other words, $\gamma, \gamma_2, \ldots, \gamma_{d-1}$ are topological generators of $\mathrm{Gal}(\mathbb{L}_\infty/K_\infty)$). Let $\pi : \Lambda_d \longrightarrow \Lambda$ be the canonical epimorphism corresponding to K_∞. For the proof of (a), we will assume that $e \geq 1$. Since $\overline{T}^e \mid \overline{g}$ by assumption, we know that

$$\pi(g) \equiv 0 \pmod{p}.$$

Let now $\tilde{K}_\infty \in \mathcal{E}(K_\infty, n)$ be arbitrary, and choose topological generators $\tilde{\gamma}_1, \ldots, \tilde{\gamma}_{d-1}$ of $\mathrm{Gal}(\mathbb{L}_\infty/\tilde{K}_\infty)$. We let $\tilde{\pi}$ denote the corresponding surjection onto Λ, that is, $\tilde{\pi}(\tilde{\gamma}_i) = 1$ for each i. Suppose that $\tilde{\gamma}_d$ denotes a topological generator of $\mathrm{Gal}(\tilde{K}_\infty/K)$. Let $\tilde{K}_n \subseteq \tilde{K}_\infty$ be the unique intermediate field of degree p^n over K. Since

$$K_\infty \cap \tilde{K}_\infty \supseteq \tilde{K}_n = \mathbb{L}_\infty^{\langle \tilde{\gamma}_1, \tilde{\gamma}_2, \ldots, \tilde{\gamma}_{d-1}, \tilde{\gamma}_d^{p^n}\rangle},$$

we may conclude that $\gamma, \gamma_2, \ldots, \gamma_{d-1} \in \langle \tilde{\gamma}_1, \tilde{\gamma}_2, \ldots, \tilde{\gamma}_{d-1}, \tilde{\gamma}_d^{p^n}\rangle$. Since $\tilde{\pi}(\tilde{\gamma}_i) = 1$ for each i, it follows that $\tilde{\pi}(\gamma) \in \mathrm{Gal}(\tilde{K}_\infty/K)^{p^n}$ and

$$\tilde{\pi}(\gamma_i) \in \mathrm{Gal}(\tilde{K}_\infty/K)^{p^n}$$

for $i \in \{2, \ldots, d-1\}$. Writing $\mathbb{Z}_p[[\mathrm{Gal}(\tilde{K}_\infty/K)]] = \mathbb{Z}_p[[S]]$, we may conclude that the reduced degree of $\tilde{\pi}(T)$ (i.e. the degree of an element in its coset in the quotient ring $\Omega = \Lambda/(p)$) is at least p^n if $\tilde{\pi}(T) \not\equiv 0 \pmod{p}$, and the same holds for the reduced degree of $\tilde{\pi}(T_i)$ for each i.

Recall that $\overline{T}^e \mid \overline{g}$. Therefore, the above means that either $\tilde{\pi}(g) \equiv 0 \pmod{p}$ or the reduced degree of $\tilde{\pi}(g)$ is at least $e \cdot p^n$.

Now suppose that $\tilde{K}_\infty \in \mathcal{E}_\mu$. Then we know (see Remark 7.6) that $\tilde{\pi}(g)$ is not divisible by p. This means that $\tilde{\pi}(g) \in \Lambda$ is associated with a distinguished polynomial of degree at least $e \cdot p^n$.

Choose generators $f_1, \ldots, f_k$ of the Fitting ideal of X. Then it follows from Lemma 7.2 that

$$\tilde{\pi}(f) = \tilde{\pi}(\gcd(f_1, \ldots, f_k)) \;\Big|\; \gcd(\tilde{\pi}(f_1), \ldots, \tilde{\pi}(f_k)) = f_{\tilde{\pi}}, \tag{13}$$

where we denote by $f_{\tilde{\pi}} \in \Lambda$ the characteristic power series of $X_{\tilde{\pi}} = X/(\ker(\tilde{\pi} \cdot X))$. It follows from the above that $\tilde{\pi}(f) = p^{m_0(X)} \cdot \tilde{\pi}(g)$ is a multiple of a distinguished polynomial of degree at least $e \cdot p^n$. In

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

view of Corollary 3.7, we know that for $n \gg 0$

$$|\lambda(X_{\tilde{\pi}}) - \lambda(X^{Gr}(E/\tilde{K}_\infty))|$$

is bounded on $\mathcal{E}(K_\infty, n)$. Therefore, assertion (a) of the proposition follows.

Now we turn to the proof of assertion (b). We decompose the coset $\overline{g}$ of g in $\Omega_d = \Lambda_d/p$ into a product of irreducible factors:

$$\overline{g} = \overline{T}^e \cdot \overline{g_2}^{e_2} \cdot \ldots \cdot \overline{g_t}^{e_t},$$

where the $\overline{g_i}$ are not divisible by $\overline{T}$, and pairwise coprime in Ω_d. Let $s \leq t$ be such that, without loss of generality, $\overline{T}, \overline{g_2}, \ldots, \overline{g_s}$ are the factors of $\overline{g}$ which contribute to $l_0(X)$. Choose lifts g_i of $\overline{g_i}$ in Λ_d. Our aim is to choose a $\mathbb{Z}_p$-extension $K_\infty \subseteq M$ of K such that the homomorphism $\pi : \Lambda_d \longrightarrow \Lambda$ which corresponds to K_∞ maps each g_i, $2 \leq i \leq t$, to an element of Λ which is not divisible by p (and in particular will be nonzero).

Since X is Λ_d-torsion and $\mathcal{E}_p \cap \mathcal{E}_{ns} \neq \emptyset$ by assumption, it follows from Proposition 7.7 that $\mathcal{E}_\mu \subseteq \mathcal{E}$ is a dense subset so in particular, $\mathcal{E}_\mu \neq \emptyset$. Choose $K_\infty \in \mathcal{E}_\mu$. Then $\pi(g) \not\equiv 0 \pmod{p}$ (see Remark 7.6). Therefore, $\pi(g_i) \not\equiv 0 \pmod{p}$ for each i. This means that for each i the power series $\pi(g_i)$ is associated with a distinguished polynomial.

Let d denote the degree of the distinguished polynomial associated with $\pi(g_2^{e_2} \cdot \ldots \cdot g_t^{e_t})$, and choose n large enough such that $p^{(n-1)/2} > d$. Since $\mathcal{E}_\mu \subseteq \mathcal{E}$ is open by Proposition 7.7, we may assume that $\mathcal{E}(K_\infty, n) \subseteq \mathcal{E}_\mu$. Let $\tilde{K}_\infty \in \mathcal{E}(K_\infty, n)$ be an arbitrary element, and let $\tilde{\pi}$ be the corresponding homomorphism. Write $n = 2m$ if n is even, and $n = 2m + 1$ if n is odd. Then in both cases $\mathcal{E}(K_\infty, n) \subseteq \mathcal{E}(K_\infty, 2m)$ and $p^m > d$. Therefore, as in the proof of Lemma 7.1,

$$\deg\left(\tilde{\pi}\left(g_2^{e_2} \cdot \ldots \cdot g_t^{e_t}\right)\right) = \deg\left(\pi\left(g_2^{e_2} \cdot \ldots \cdot g_t^{e_t}\right)\right) = d$$

does not depend on the choice of $\tilde{K}_\infty$. This shows that the contribution of the divisors $\overline{g_i}$ of $\overline{g}$ to the degree of the distinguished polynomial attached to $\tilde{\pi}(g)$ is bounded as $\tilde{K}_\infty$ runs over the elements in $\mathcal{E}(K_\infty, n)$.

As in the proof of (a), we let $\gamma, \gamma_2, \ldots, \gamma_{d-1}$ denote a set of topological generators of $\mathrm{Gal}(\mathbb{L}_\infty/K_\infty)$. Now let $N = \mathbb{L}_\infty^{\langle \gamma_2, \ldots, \gamma_{d-1} \rangle}$ and suppose that $\tilde{K}_\infty \in \mathcal{E}(K_\infty, n) \setminus \mathcal{E}(K_\infty, n+1)$. Let $\tilde{\gamma}_1, \ldots, \tilde{\gamma}_{d-1}$ denote a set of topological generators of $\mathrm{Gal}(\mathbb{L}_\infty/\tilde{K}_\infty)$. In fact, we will assume from now on that $\tilde{\gamma}_i = \gamma_i$ for each $i \in \{2, \ldots, d-1\}$. Note this just means that we are restricting to $\mathbb{Z}_p$-extensions $\tilde{K}_\infty$ of K which are contained in N, as in the statement of the proposition.

Moreover, we denote by $\tilde{\gamma}_d$ a topological generator of $\mathrm{Gal}(\tilde{K}_\infty/K)$. Then, as in the proof of (a), $\gamma = T + 1$ can be written in the form

$$\tilde{\gamma}_1^{a_1} \cdot \ldots \cdot \tilde{\gamma}_{d-1}^{a_{d-1}} \cdot \tilde{\gamma}_d^{a_d}, \tag{14}$$

where $a_1, \ldots, a_d \in \mathbb{Z}_p$ and a_d is divisible by p^e. Since $\tilde{K}_\infty \notin \mathcal{E}(K_\infty, n+1)$, we know that at least one of the topological generators $\gamma, \gamma_2, \ldots, \gamma_{d-1}$ of $\mathrm{Gal}(\mathbb{L}_\infty/K_\infty)$ is not contained in $\langle \tilde{\gamma}_1, \tilde{\gamma}_2, \ldots, \tilde{\gamma}_{d-1}, \tilde{\gamma}_d^{p^{n+1}} \rangle$. Since $\tilde{K}_\infty \subseteq N$ by assumption, we may conclude that the exponent a_d from (14) is not divisible by p^{n+1}. In fact, the topological generator $\tilde{\gamma}_d$ of $\mathrm{Gal}(\tilde{K}_\infty/K)$ can be chosen such that $a_d = p^n$. Therefore,

$$\deg\left(\tilde{\pi}(T^e)\right) = e \cdot p^n.$$

Summarizing, we have shown that

$$\deg\left(\tilde{\pi}(g)\right) = e \cdot p^n + O(1)$$

on $\mathcal{E}(K_\infty, n) \setminus \mathcal{E}(K_\infty, n+1)$. Since the maximal pseudo-null submodule X° of X is finitely generated as a $\mathbb{Z}_p$-module in view of our hypotheses, we may, as in the proof of Corollary 7.4, choose an element $H \in \mathrm{Ann}(X^\circ)$ such that $\pi(H) \not\equiv 0 \pmod{p}$. Then $\deg\left(\tilde{\pi}(H)\right) = O(1)$ on $\mathcal{E}(K_\infty, n)$ by the same argument as for $g_2^{e_2} \cdot \ldots \cdot g_t^{e_t}$ above (it might be necessary to increase n appropriately). Moreover,

$$\tilde{\pi}(f) \mid f_{\tilde{\pi}} \mid \tilde{\pi}(f)\tilde{\pi}(H)$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

for each $\tilde{K}_\infty \in \mathcal{E}(K_\infty, n)$, as in the proof of Corollary 7.4 (here $f_{\tilde{\pi}}$ denotes the characteristic power series of $X_{\tilde{\pi}}$, as in the proof of (a)). We may thus conclude that

$$\lambda(X_{\tilde{\pi}}) = e \cdot p^n + O(1).$$

In view of Corollary 3.7, we know that for $n \gg 0$

$$|\lambda(X_{\tilde{\pi}}) - \lambda(X^{Gr}(E/\tilde{K}_\infty))|$$

is bounded on $\mathcal{E}(K_\infty, n)$. Therefore,

$$\lambda(X^{Gr}(E/\tilde{K}_\infty)) = e \cdot p^n + O(1).$$

□

The following result is the last auxiliary result which will be used in the proof of Theorem 1.5.

Proposition 7.10. *Let E be E_1 or E_2. If $d > 2$, suppose that the maximal pseudo-null submodule of $X = X^{Gr}(E/\mathbb{L}_\infty)$ is finitely generated over $\mathbb{Z}_p$. Let $K_\infty \in \mathcal{E}$. Assume that no prime in S_p splits completely in K_∞/K and that $X^{Gr}(E/K_\infty)$ is Λ-torsion.*

We write the characteristic power series of X as $f = p^{m_0(X)} \cdot g$. Then the following are equivalent:

(1) $\pi(g) \not\equiv 0 \pmod{p}$, where π corresponds to K_∞.
(2) $\lambda(X^{Gr}(E/\tilde{K}_\infty))$ is bounded as $\tilde{K}_\infty$ runs over the elements in a sufficiently small neighborhood of K_∞.

Proof. [35, Lemma 3.21] proves the analogous statement for the classical Selmer group. Using Corollary 3.7, the proof of [35, Lemma 3.21] can be formulated for the Greenberg Selmer group in an identical way. Taking this into account, we see that the equivalence in the statement of the proposition will follow if we show the existence of the element $H \in \Lambda_d$ in loc. cit. As the maximal pseudo-null submodule of $X^{Gr}(E/\mathbb{L}_\infty)$ is finitely generated over $\mathbb{Z}_p$, its annihilator ideal is not contained in any prime ideal of height at most $d-1$. Therefore, from the proof of [35, Theorem 3.22] such an element $H \in \Lambda_d$ exists. □

Now, we can finally prove Theorem 1.5.

Proof of Theorem 1.5. Assume that all the hypotheses of Theorem 1.5 are satisfied. By Propositions 2.2 and 2.3, it suffices to prove the theorem with $X(E_j/\mathbb{L}_\infty)$ replaced by $X^{Gr}(E_j/\mathbb{L}_\infty)$ for $j = 1, 2$.

Suppose that $X(E_1/\mathbb{L}_\infty)$ is a Λ_d-torsion module and $E_1[p^i] \cong E_2[p^i]$ for some integer $i > m_{0,1}$. From Theorem 1.4, we get that $X(E_2/\mathbb{L}_\infty)$ is a Λ_d-torsion module with $m_{0,2} = m_{0,1}$.

In order to conclude the proof of assertion (1), we assume that $\widehat{l_{0,1}} = 0$. Then for every $K_\infty \in \mathcal{E}$, we have that $\pi(g_1) \not\equiv 0 \pmod{p}$, where π corresponds to K_∞. From Corollaries 7.4 and 3.7, we get that $X^{Gr}(E_1/K_\infty)$ is Λ-torsion. Note that in view of hypothesis (ii) and (iii) from Theorem 1.5, we can apply Proposition 7.10 to each $K_\infty \in \mathcal{E}$. Therefore from Proposition 7.10, $\lambda(X^{Gr}(E_1/\tilde{K}_\infty))$ is bounded as $\tilde{K}_\infty$ runs over the elements in a sufficiently small neighborhood V of $\tilde{K}_\infty$. Since $\pi(g_1) \not\equiv 0 \pmod{p}$ for every π, it follows from Corollaries 7.4 and 3.7 that $X^{Gr}(E_1/\tilde{K}_\infty)$ is Λ-torsion with $\mu(X^{Gr}(E_1/\tilde{K}_\infty)) = \alpha$ for all $\tilde{K}_\infty \in V$.

By Lemma 4.7, the differences $|\lambda(X^{Gr}(E_1/\tilde{K}_\infty)) - \lambda(X^{Gr}(E_2/\tilde{K}_\infty))|$ are bounded on V. Therefore, $\lambda(X^{Gr}(E_2/\tilde{K}_\infty))$ is bounded as $\tilde{K}_\infty$ runs over the elements of V. So by Proposition 7.10, $\pi(g_2) \not\equiv 0 \pmod{p}$. Since K_∞ was arbitrary, we have thus shown that $\widehat{l_{0,2}} = 0$. The proof in the reverse direction is the same. This proves (1).

Now we prove assertion (2) of the theorem. We show that $l_{0,2} \leq l_{0,1}$ (the reverse inequality will follow from a symmetric argument). To this purpose, suppose that $\overline{T}^e \mid \overline{g}$ but $\overline{T}^{e+1} \nmid \overline{g}$ for some variable T (here $g_1 = g(X^{Gr}(E_1/\mathbb{L}_\infty))$, as in the first part of the proof). Note that we allow $e = 0$ here. Let K_∞ be any $\mathbb{Z}_p$-extension of K contained in $\mathcal{E}_\mu$ as in Proposition 7.9(b). Then we can choose a sequence of $\mathbb{Z}_p$-extensions

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

$\tilde{K}_\infty^{(n)}$ of K such that

$$\lambda(X^{Gr}(E/\tilde{K}_\infty^{(n)})) \leq e \cdot p^n + C' \tag{15}$$

and $\tilde{K}_\infty^{(n)} \in \mathcal{E}(K_\infty, n) \setminus \mathcal{E}(K_\infty, n+1)$ for each $n \in \mathbb{N}$ and some fixed constant C'. As in the first part of the proof, the differences $|\lambda(X^{Gr}(E_1/\tilde{K}_\infty^{(n)})) - \lambda(X^{Gr}(E_2/\tilde{K}_\infty^{(n)}))|$ are bounded for these $\tilde{K}_\infty^{(n)} \in \mathcal{E}_\mu$.

Now suppose that $\overline{g_2}$, $g_2 = g(X^{Gr}(E_2/\mathbb{L}_\infty))$, is divisible by a higher power of $\overline{T}$. Then Proposition 7.9(a) implies that for $m \gg 0$

$$\lambda(X^{Gr}(E_2/\tilde{K}_\infty^{(m)})) \geq (e+1) \cdot p^m$$

for each $\tilde{K}_\infty^{(m)} \in \mathcal{E}(K_\infty, m)$ which is contained in $\mathcal{E}_\mu$. For any m which is strictly larger than n and the sum of the constant C' from equation (15) and the constant bounding the above difference of λ-invariants, this yields a contradiction.

Since $T = \gamma - 1$ and $e \in \mathbb{N}$ had been chosen arbitrarily, this shows that indeed $l_{0,2} \leq l_{0,1}$. □

8. The $\mathfrak{M}_H(G)$-property

Finally, we mention an application to the $\mathfrak{M}_H(G)$-*property*. This property, motivated by the $\mathfrak{M}_H(G)$-*conjecture* (see [9]), has been studied before in [36]. We adapt the following notation from [36] to our purposes.

Definition 8.1. *We let $\mathcal{H} \subseteq \mathcal{E}$ denote the subset of $\mathbb{Z}_p$-extensions $L \subseteq \mathbb{L}_\infty$ which satisfy the following hypotheses:*

(a) $L \in \mathcal{E}_p \cap \mathcal{E}_{ns}$, that is, each prime of K above p ramifies in L, and no prime in S splits completely in L/K,
(b) $X(E_1/L)$ and $X(E_2/L)$ are both Λ-torsion.

Definition 8.2. *Let $L \in \mathcal{H}$, and write $G = \mathrm{Gal}(\mathbb{L}_\infty/K)$ and $H = \mathrm{Gal}(\mathbb{L}_\infty/L)$. Then $H \cong \mathbb{Z}_p^{d-1}$, and we say that the $\mathfrak{M}_H(G)$-property holds for $X(E_i/\mathbb{L}_\infty)$ if the quotient*

$$X_f(E_i/\mathbb{L}_\infty) := X(E_i/\mathbb{L}_\infty)/X(E_i/\mathbb{L}_\infty)[p^\infty]$$

is finitely generated as a $\mathbb{Z}_p[[H]]$-module.

Before stating the main results in this section, we need two lemmas.

Lemma 8.3. *Let $i \in \{1, 2\}$, $E = E_i$, $g = g_i$, and $K_\infty \in \mathcal{H}$. Suppose that we have $\pi(g) \not\equiv 0 \pmod{p}$, where π corresponds to K_∞ as in the beginning of Section 7. Furthermore, if $d > 2$, suppose that the maximal pseudo-null submodule of $X(E/\mathbb{L}_\infty)$ is finitely generated over $\mathbb{Z}_p$.*

Let $H = \mathrm{Gal}(\mathbb{L}_\infty/K_\infty)$. Then $X_f(E/\mathbb{L}_\infty)$ is finitely generated as a $\mathbb{Z}_p[[H]] \cong \Lambda_{d-1}$-module.

Proof. For simplicity, we denote $X_f(E/\mathbb{L}_\infty)$ by X_f. We have an exact sequence

$$0 \longrightarrow A \longrightarrow X_f \longrightarrow E$$

where A is a pseudo-null Λ_d-module and E is an elementary Λ_d-module. Assume that $\pi(g) \not\equiv 0 \pmod{p}$.

If $d = 2$, then as A is pseudo-null it has Krull dimension at most one. Multiplication by p is injective on X_f by definition. Therefore, A/p has Krull dimension zero by [1, Corollary 11.9], that is, A/p is finite whence A is a finitely generated $\mathbb{Z}_p$-module.

Since $X(E/\mathbb{L}_\infty)[p^\infty] = X(E/\mathbb{L}_\infty)[p^n]$ for some $n \in \mathbb{N}$, we have an isomorphism

$$X_f \cong p^n \cdot X(E/\mathbb{L}_\infty) \subseteq X(E/\mathbb{L}_\infty).$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

Therefore, if $d > 2$, the maximal pseudo-null Λ_d-submodule of X_f is finitely generated as a $\mathbb{Z}_p$-module by assumption. Since this former statement is also true for $d = 2$ by the above, we see from the above exact sequence that X_f will be finitely generated over $\mathbb{Z}_p[[H]]$ if we can show that E is finitely generated over $\mathbb{Z}_p[[H]]$.

To this end, we first note that E_H is a finitely generated torsion $\mathbb{Z}_p[[\Gamma]] \cong \Lambda$-module, where $\Gamma = \mathrm{Gal}(K_\infty/K)$. To see this, we first remark that since characteristic power series are multiplicative in exact sequences (this can be shown by localizations at height one primes ideals of Λ_d), the characteristic power series of X_f (and hence E) is g. The assumption $\pi(g) \not\equiv 0 \pmod p$ certainly implies that $\pi(g) \neq 0$. As g annihilates E, we see that E_H is a finitely generated torsion Λ-module.

Now we claim that $\mu(E_H) = 0$. This can be seen from the following sequence of equivalences. Assume that $E = \bigoplus_{j=1}^{t} \Lambda_d/(h_j^{n_j})$ so that $g = \prod h_j^{n_j}$. Let $\Omega_d := \Lambda_d/p$ be the 'mod p' Iwasawa algebra. We have

$$\begin{aligned}
&\mu(E_H) = 0\\
\iff &\mu((\Lambda_d/(h_j^{n_j}))_H) = 0 \text{ for } j = 1, \ldots, t\\
\iff &(\Omega_d)_H/(\pi(\overline{h_j}^{n_j})) \text{ is finite for } j = 1, \ldots, t\\
\iff &\pi(h_j^{n_j}) \not\equiv 0 \pmod p \text{ for } j = 1, \ldots, t\\
\iff &\pi(g) \not\equiv 0 \pmod p.
\end{aligned}$$

Therefore, we see that $\mu(E_H) = 0$. So, E_H is a finitely generated torsion Λ-module with $\mu = 0$. Therefore, E_H is finitely generated over $\mathbb{Z}_p$. This proves the lemma. □

Lemma 8.4. *Let E be E_1 or E_2, $K_\infty \in \mathcal{H}$ and $H = \mathrm{Gal}(\mathbb{L}_\infty/K_\infty)$. Assume that $X_f(E/\mathbb{L}_\infty)$ is finitely generated over $\mathbb{Z}_p[[H]]$ and that $E(\mathbb{L}_\infty)[p^\infty]$ is finite. Then $\mu(X(E/K_\infty)) = m_0(X(E/\mathbb{L}_\infty))$.*

Proof. Since $X_f(E/\mathbb{L}_\infty)$ is finitely generated over $\mathbb{Z}_p[[H]]$, it is easy to see that $X(E/\mathbb{L}_\infty)$ is Λ-torsion. Since $X(E/\mathbb{L}_\infty)$ is Λ_d-torsion and $E(\mathbb{L}_\infty)[p^\infty]$ is finite, it follows from [25, Theorem 7.2] that $H^2(G_S(\mathbb{L}_\infty), E[p^\infty]) = 0$ and that the map

$$H^1(G_S(\mathbb{L}_\infty), E[p^\infty]) \longrightarrow \bigoplus_{v \in S} J_v(E/\mathbb{L}_\infty)$$

is surjective. Here, $J_v(E/\mathbb{L}_\infty) = \varinjlim \bigoplus_{w|v} H^1(F_w, E)[p^\infty]$ where the direct limit runs over the finite extensions F of K contained in $\mathbb{L}_\infty$.

Consider the map

$$s_{K_\infty} : X(E/\mathbb{L}_\infty)_H \longrightarrow X(E/K_\infty)$$

whose dual is induced by restriction. Since $K_\infty \in \mathcal{H} \subseteq \mathcal{E}_p \cap \mathcal{E}_{ns}$, it follows from [35, Lemma 3.14, Corollary 3.15] that $\ker s_{K_\infty}$ and $\mathrm{coker} s_{K_\infty}$ are finitely generated torsion Λ-modules with $\mu = 0$ and therefore are finitely generated over $\mathbb{Z}_p$.

The previous results mentioned allow us to use Lim's result [38, Proposition 4.7]:

$$m_0(X(E/\mathbb{L}_\infty)) = \mu(X(E/K_\infty)) + \sum_{i=0}^{d-2} (-1)^{i+1} \mu(H_i(H, X_f(E/\mathbb{L}_\infty))). \tag{16}$$

Note that Lim proved this result when K_∞ is the cyclotomic $\mathbb{Z}_p$-extension of K. The same proof works for arbitrary $K_\infty \in \mathcal{H}$ because as mentioned above $\ker s_{K_\infty}$ and $\mathrm{coker} s_{K_\infty}$ are finitely generated over $\mathbb{Z}_p$.

By assumption, $X(E/\mathbb{L}_\infty)_f$ is finitely generated over $\Lambda(H) = \mathbb{Z}_p[[H]]$. Therefore for any $i \geq 0$, we have that $H_i(H, X_f(E/\mathbb{L}_\infty))$ is finitely generated over $\mathbb{Z}_p$ (see the proof of [26, Theorem 1.1]). So from (16), we have $\mu(X(E/K_\infty)) = m_0(X(E/\mathbb{L}_\infty))$. This completes the proof. □

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

The following criterion for the $\mathfrak{M}_H(G)$-property generalizes part of the main result from [36] from the setting of $\mathbb{Z}_p^2$-extensions to $\mathbb{Z}_p^d$-extensions, $d \geq 2$.

Lemma 8.5. *Let E be an elliptic curve defined over K, with good ordinary reduction at p. Let $\mathbb{L}_\infty/K$ be a $\mathbb{Z}_p^d$-extension such that $E(\mathbb{L}_\infty)[p^\infty]$ is finite. If $d > 2$, then we moreover assume that the maximal pseudo-null Λ_d-submodule of $X(E/\mathbb{L}_\infty)$ is finitely generated over $\mathbb{Z}_p$.*

Write the characteristic power series of $X(E/\mathbb{L}_\infty)$ as $f = p^{m_0(X(E/\mathbb{L}_\infty))}g$. Let $K_\infty \in \mathcal{H}$, $H = \mathrm{Gal}(\mathbb{L}_\infty/K_\infty)$ and let

$$\pi : \Lambda_d \twoheadrightarrow \Lambda = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$$

be the canonical surjection.

Then the following conditions are equivalent.

(a) $X(E/\mathbb{L}_\infty)$ has the $\mathfrak{M}_H(G)$-property.
(b) $\mu(X(E/K_\infty)) = m_0(X(E/\mathbb{L}_\infty))$.
(c) $\pi(g) \not\equiv 0 \pmod{p}$.

Proof. $(a) \Longrightarrow (b)$: Lemma 8.4.

$(b) \Longrightarrow (c)$: Let $X = X(E/\mathbb{L}_\infty)$ for brevity, and write $X_\pi = X/\ker(\pi)$. Since $K_\infty \in \mathcal{H}$, we have that X_π is torsion as a Λ-module. Therefore, we can apply Corollary 7.4(b) to X and X_π.

Suppose now that $\pi(g) \equiv 0 \pmod{p}$. Then $\mu(X_H) > m_0(X)$ by Corollary 7.4(b). But since $K_\infty \in \mathcal{H}$ and therefore no prime in S is totally split in K_∞/K, it follows from [35, Corollary 3.15(b)] that $\mu(X_H) = \mu(X(E/K_\infty))$.

$(c) \Longrightarrow (a)$: This follows from Lemma 8.3. □

Corollary 8.6. *In the setting of the previous lemma suppose that the equivalent conditions hold for some $K_\infty \in \mathcal{H}$. Then there exists a Greenberg neighborhood U of K_∞ such that the conditions are satisfied for each $\tilde{K}_\infty \in U$.*

Proof. We have seen in Lemma 7.1 that the validity of condition (c) from Lemma 8.5 implies that this condition is true for each $\tilde{K}_\infty$ in a certain neighborhood U of K_∞. Note that Lemma 7.1 has been proven for Greenberg Selmer groups. However, since $K_\infty \in \mathcal{H} \subseteq \mathcal{E}_p \cap \mathcal{E}_{ns}$, it follows from Proposition 2.2 and 2.3(c) that U can be chosen small enough to ensure that $X^{Gr}(E/\tilde{K}_\infty) = X(E/\tilde{K}_\infty)$ for each $\tilde{K}_\infty \in U$. □

We can now prove the main result of this section. One should compare this result to results of Lim (see [39, Proposition 5.1.3] and the main result from [41]), which need additional hypotheses. Moreover, our approach will also yield Corollary 8.8.

Theorem 8.7. *Let $\mathbb{L}_\infty/K$ be a $\mathbb{Z}_p^d$-extension, and let $K_\infty \in \mathcal{H}$. Write $H = \mathrm{Gal}(\mathbb{L}_\infty/K_\infty)$. We assume that*

(i) both $E_1(\mathbb{L}_\infty)[p^\infty]$ and $E_2(\mathbb{L}_\infty)[p^\infty]$ are finite,
(ii) $E_1[p^i] \cong E_2[p^i]$ as Galois modules, where $i > m_{0,1} = m_0(X(E_1/\mathbb{L}_\infty))$.

If $d > 2$, then we moreover assume that the maximal pseudo-null Λ_d-submodules of $X(E_1/\mathbb{L}_\infty)$ and $X(E_2/\mathbb{L}_\infty)$ are finitely generated $\mathbb{Z}_p$-modules.

If the $\mathfrak{M}_H(G)$-property holds for E_1, then it also holds for E_2.

Proof. Let $K_\infty = \mathbb{L}_\infty^H$. First, since $K_\infty \in \mathcal{H}$ by assumption and thus $X(E_i/K_\infty)$ are Λ-torsion, $i = 1, 2$, it follows from [35, Lemma 3.17] that both $X(E_i/\mathbb{L}_\infty)$, $i = 1, 2$, are finitely generated and Λ_d-torsion. Moreover, since $H \in \mathcal{H}$, it follows from [32, Theorem 4.11] that we can choose a neighbourhood U of

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

K_∞ such that $X(E_i/\tilde{K}_\infty)$ is Λ-torsion for both $i = 1, 2$, and

$$\mu(X(E_1/\tilde{K}_\infty)) \le \mu(X(E_1/K_\infty)), \quad \mu(X(E_2/\tilde{K}_\infty)) \le \mu(X(E_2/K_\infty))$$

hold for each $\tilde{K}_\infty \in U$. In addition, we may assume that $U \subseteq \mathcal{E}_p \cap \mathcal{E}_{ns}$ (indeed, it suffices if $U = \mathcal{E}(K_\infty, n)$ has been chosen small enough such that each prime of K above p ramifies in the n-th layer K_n of K_∞ and such that no prime of S is totally split in K_n/K. Both conditions can be ensured for large n since $K_\infty \in \mathcal{H}$).

Now suppose that the $\mathfrak{M}_H(G)$-property holds for E_1. Then it follows from Lemma 8.5 and Corollary 8.6 that

$$\mu(X(E_1/\tilde{K}_\infty)) = m_{0,1}$$

for each $\tilde{K}_\infty \in U$ (it might be necessary here to make U slightly smaller).

Since $U \subseteq \mathcal{E}_p \cap \mathcal{E}_{ns}$, we have by Propositions 2.2 and 2.3 that $X(E_i/\tilde{K}_\infty) = X^{Gr}(E_i/\tilde{K}_\infty)$ for each $\tilde{K}_\infty \in U$. Therefore, Theorem 4.3(b) implies that for any $\tilde{K}_\infty \in U$ we have a pseudo-isomorphism

$$X(E_1/\tilde{K}_\infty)[p^\infty] \longrightarrow X(E_2/\tilde{K}_\infty)[p^\infty].$$

In particular, $\mu(X(E_1/\tilde{K}_\infty)) = \mu(X(E_2/\tilde{K}_\infty)) = m_{0,1}$ for each $\tilde{K}_\infty \in U$.

As we have seen in the proof of Lemma 5.1, we have $\mu(X(E_2/F)) = m_{0,2}$ for each $F \in \mathcal{E}_p \cap \mathcal{E}_{ns}$ which is not contained in a finite number of $\mathbb{Z}_p^{d-1}$-extensions of K (here we again apply Propositions 2.2 and 2.3). Therefore from Lemma 7.8, we see that U contains a $\mathbb{Z}_p$-extension F of K such that $\mu(X(E_2/F)) = m_{0,2} := m_0(X(E_2/\mathbb{L}_\infty))$. This concludes the proof of the theorem. Indeed, it follows that

$$\mu(X(E_2/\tilde{K}_\infty)) = \mu(X(E_2/F)) = m_{0,2}$$

for each $\tilde{K}_\infty \in U$, that is, the $\mathfrak{M}_{\tilde{H}}(G)$-property holds for E_2 and every $\tilde{H} = \mathrm{Gal}(\mathbb{L}_\infty/\tilde{K}_\infty)$ in view of Lemma 8.5. In particular, it holds for $\tilde{K}_\infty = K_\infty$. □

In the above proof, we also showed the following

Corollary 8.8. *Let $\mathbb{L}_\infty$ be as in Theorem 8.7. We assume that $\mathcal{H} \neq \emptyset$. Then the $\mathfrak{M}_H(G)$-property holds for a dense subset of $\mathcal{E}$.*

Proof. If $\mathcal{H} \neq \emptyset$, then the decomposition field of any $v \in S$ is contained in some $\mathbb{Z}_p^{d-1}$-extension of K, and the inertia subfield $\mathbb{L}^{(v)} \subseteq \mathbb{L}_\infty$ of any $v \mid p$ is contained in a $\mathbb{Z}_p^{d-1}$-extension of K. Moreover, it follows from [35, Lemma 3.17] that both $X(E_1/\mathbb{L}_\infty)$ and $X(E_2/\mathbb{L}_\infty)$ are finitely generated and Λ_d-torsion. Therefore, [35, Lemma 3.1 and Corollary 3.15] (see also the proof of Lemma 5.1) imply that $X(E_i/K_\infty)$ is Λ-torsion and $\mu(X(E_i/K_\infty)) = m_0(X(E_i/\mathbb{L}_\infty))$ for both i as long as K_∞ is not contained in a certain finite number of $\mathbb{Z}_p^{d-1}$-extensions.

The assertion now follows from Lemma 7.8. □

9. Pseudo-null submodules

Now we prove two sufficient criteria for the hypothesis (ii) of Theorem 1.5 on the maximal pseudo-null submodules of $X(E_1/\mathbb{L}_\infty)$ and $X(E_2/\mathbb{L}_\infty)$. In fact, we describe two settings where these pseudo-null submodules are even *trivial*.

Lemma 9.1. *Let $\mathbb{L}_\infty/K$ be a $\mathbb{Z}_p^d$-extension, $d \ge 3$, and let E be an elliptic curve defined over K which has good ordinary reduction at p. We assume that the following conditions are met.*

(i) Every prime $v \in S_p$ ramifies in $\mathbb{L}_\infty/K$,
(ii) $E(\mathbb{L}_\infty)[p^\infty]$ is finite,

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

(iii) $X(E/\mathbb{L}_\infty)$ *is* Λ_d*-torsion,*
(iv) *The decomposition subgroups* $D_v(\mathbb{L}_\infty/K) \subseteq \mathrm{Gal}(\mathbb{L}_\infty/K)$ *are open for each* $v \in S_p$*, and*
(v) E *has good reduction everywhere.*

Then $X(E/\mathbb{L}_\infty)$ *does not contain any nontrivial pseudo-null submodules.*

Proof. In view of the hypotheses (ii) and (iii), it follows from [25, Theorem 7.2] that the weak Leopoldt conjecture holds for E over $\mathbb{L}_\infty$, that is, that $H^2(\mathrm{Gal}(K_S/\mathbb{L}_\infty), E[p^\infty]) = 0$. Condition (i) implies by Propositions 2.2 and 2.3 that $X(E/\mathbb{L}_\infty) = X^{str}(E/\mathbb{L}_\infty)$. Therefore, we prove the desired result for $X^{str}(E/\mathbb{L}_\infty)$.

Since the elliptic curve E has good reduction everywhere, the assertion of the lemma follows from [41, Proposition 5.1]. Indeed, since E has good reduction everywhere, we can take the set S to be the primes of K above p. Let S_∞ be the set of primes of $\mathbb{L}_\infty$ above those in S. By assumption (iv), the set S_∞ is finite. By [25, Theorem 7.2], we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}^{str}(E/\mathbb{L}_\infty) \longrightarrow H^1(G_S(\mathbb{L}_\infty), E[p^\infty]) \longrightarrow \bigoplus_{w \in S_\infty} H^1(\mathbb{L}_{\infty,w}, \tilde{E}[p^\infty]) \longrightarrow 0.$$

Here, $\tilde{E}$ denotes the reduction of E over the residue field.

Now we conclude as in the proof of [41, Proposition 5.1]: Taking Pontryagin duals of the above exact sequence, we get

$$0 \longrightarrow \left(\bigoplus_{w \in S_\infty} H^1(\mathbb{L}_{\infty,w}, \tilde{E}[p^\infty]) \right)^\vee \longrightarrow H^1(G_S(\mathbb{L}_\infty), E[p^\infty])^\vee \longrightarrow X^{str}(E/\mathbb{L}_\infty) \longrightarrow 0.$$

The first module in this exact sequence is reflexive by [48, Lemma 5.4] (this again uses assumption *(iv)*). It follows from the validity of the weak Leopoldt conjecture that $H^1(G_S(\mathbb{L}_\infty), E[p^\infty])^\vee$ does not contain any nonzero pseudo-null Λ_d-submodules (see [48, Theorem 4.7]). Therefore, the same holds true for $X^{str}(E/\mathbb{L}_\infty)$ by [24, Proposition 3.5]. □

Lemma 9.2. *Let* $\mathbb{L}_\infty/K$ *be a* $\mathbb{Z}_p^d$*-extension,* $d \geq 2$*, and let* E *be an elliptic curve defined over* K *which has good ordinary reduction at* p*. We assume that the following conditions are met.*

(i) *Every prime of* K *above* p *ramifies in* $\mathbb{L}_\infty/K$ *and no prime in* S *splits completely in* $\mathbb{L}_\infty/K$*,*
(ii) $E(K)[p] = 0$*,*
(iii) $X(E/\mathbb{L}_\infty)$ *is* Λ_d*-torsion.*

Then $X(E/\mathbb{L}_\infty)$ *does not contain any nontrivial pseudo-null submodules.*

Proof. The proof is based on the work of Greenberg [19]. Condition (i) implies by Propositions 2.2 and 2.3 that $X(E/\mathbb{L}_\infty) = X^{str}(E/\mathbb{L}_\infty)$. Therefore, we prove the desired result for $X^{str}(E/\mathbb{L}_\infty)$.

Let us denote the absolute Galois group of K by G_K, recall that $G := \mathrm{Gal}(\mathbb{L}_\infty/K)$, and $\Lambda_d = \mathbb{Z}_p[[G]]$. Let $\Psi : G_K \twoheadrightarrow G \hookrightarrow \Lambda_d^\times$ be the natural character and let $\Lambda_d(\Psi^{-1})$ be the free rank one Λ_d-module with G_K action by Ψ^{-1}. Denote the p-adic Tate module of E by $T_p(E)$. We define

$$\mathcal{T} := T_p(E) \otimes_{\mathbb{Z}_p} \Lambda_d(\Psi^{-1}) \quad \text{and} \quad \mathcal{D} := \mathcal{T} \otimes_{\Lambda_d} \Lambda_d^\vee,$$

where $\Lambda_d^\vee$ is the Pontryagin dual of Λ_d. We let G_K act diagonally on $\mathcal{T}$ and with left action on $\mathcal{D}$.

Now let v be a prime of K above p. Let $\overline{K}_v$ be an algebraic closure of K_v and k_v the residue field. We let $\tilde{E}(k_v)$ be the reduction of E over the residue field and denote by $E^1(\overline{K}_v)$ the kernel of the reduction map $E(\overline{K}_v) \longrightarrow \tilde{E}(k_v)$. We let $T_{v,p}^+(E)$ and $T_{v,p}^-(E)$ to be the Tate modules of $E^1(\overline{K}_v)$ and $\tilde{E}(k_v)$, respectively. Then similarly to the above, we define

$$\mathcal{T}_v^\pm := T_{v,p}^\pm(E) \otimes_{\mathbb{Z}_p} \Lambda_d(\Psi^{-1}) \quad \text{and} \quad \mathcal{D}_v^\pm := \mathcal{T}_v^\pm \otimes_{\Lambda_d} \Lambda_d^\vee.$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

It follows from Shapiro's lemma (see [58, Prop. 3.4]) that $\mathrm{Sel}^{str}(E/\mathbb{L}_\infty)$ is G-isomorphic to the kernel of the map

$$H^1(G_S(K), \mathcal{D}) \longrightarrow \prod_{v\in S\setminus S_p} H^1(K_v, \mathcal{D}) \times \prod_{v\in S_p} H^1(K_v, \mathcal{D}_v^-).$$

Let $v \in S_p$. It follows from [47, Theorem 7.1.8(i)] and Shapiro's lemma that $H^2(K_v, \mathcal{D}_v^+) = 0$. Therefore, if we let

$$L(K_v, \mathcal{D}) = \mathrm{img}(H^1(K_v, \mathcal{D}_v^+) \longrightarrow H^1(K_v, \mathcal{D})),$$

we see that $H^1(K_v, \mathcal{D}_v^-) = H^1(K_v, \mathcal{D})/L(K_v, \mathcal{D})$.

For any $v \in S \setminus S_p$ define $L(K_v, \mathcal{D}) = 0$. Let $P(K, \mathcal{D}) = \prod_{v\in S} H^1(K_v, \mathcal{D})$ and $L(K, \mathcal{D}) = \prod_{v\in S} L(K_v, \mathcal{D})$. With these definitions let

$$Q_{\mathcal{L}}(K, \mathcal{D}) = P(K, \mathcal{D})/L(K, \mathcal{D}).$$

From the above, we see that $\mathrm{Sel}(E/\mathbb{L}_\infty)$ is G-isomorphic to $S_{\mathcal{L}}(K, \mathcal{D})$ which is defined as:

$$0 \longrightarrow S_{\mathcal{L}}(K, \mathcal{D}) \longrightarrow H^1(G_S(K), \mathcal{D}) \longrightarrow Q_{\mathcal{L}}(K, \mathcal{D}).$$

We now list various hypotheses in Greenberg's paper:

- RFX($\mathcal{D}$): The module $\mathcal{T}$ is a reflexive Λ_d-module.
- $\mathrm{LOC}_v^{(1)}(\mathcal{D})$: $(\mathcal{T}^\vee)^{G_{K_v}} = 0$ for $v \in S$.
- $\mathrm{LOC}_v^{(2)}(\mathcal{D})$: The Λ_2-module $\mathcal{T}^\vee/(\mathcal{T}^\vee)^{G_{K_v}}$ is reflexive for $v \in S$.
- LEO($\mathcal{D}$): The discrete, co-finitely generated Λ_d-module

$$\mathrm{Ш}(K, S, \mathcal{D}) = \ker\left(H^2(G_S(K), \mathcal{D}) \longrightarrow \prod_{v\in S} H^2(K_v, \mathcal{D})\right)$$

  is cotorsion.
- CRK($\mathcal{D}, \mathcal{L}$): We have

$$\mathrm{corank}_{\Lambda_d}(H^1(G_S(K), \mathcal{D})) = \mathrm{corank}_{\Lambda_d}(S_{\mathcal{L}}(K, \mathcal{D})) + \mathrm{corank}_{\Lambda_d}(Q_{\mathcal{L}}(K, \mathcal{D})).$$

Greenberg calls a discrete Λ_d-module M *almost divisible* if $\Pi M = M$ for almost all height one prime ideals Π in $\mathrm{Spec}(\Lambda_d)$. This is equivalent to the Pontryagin dual of M having no nonzero pseudo-null submodules. Using the notation from Greenberg's paper [19], we say that $\mathcal{L}$ is almost Λ_d-divisible if $L(K_v, \mathcal{D})$ is almost Λ_d-divisible for each $v \in S$.

Let $\mathfrak{m}$ be the maximal ideal of Λ_2. Proposition 4.1.1 of Greenberg's paper [19] states that $S_{\mathcal{L}}(K, \mathcal{D})$ is almost divisible if the following are met:

(a) RFX($\mathcal{D}$), LEO($\mathcal{D}$), and CRK($\mathcal{D}, \mathcal{L}$) are satisfied.
(b) $\mathcal{L}$ is almost Λ_d-divisible.
(c) $\mathrm{LOC}_v^{(2)}(\mathcal{D})$ is satisfied for all $v \in S$, and there exists a nonarchimedean prime $v \in S$ such that $\mathrm{LOC}_v^{(1)}(\mathcal{D})$ is satisfied.
(d) $\mathcal{D}$ is a co-free Λ_d-module, and $\mathcal{D}[\mathfrak{m}]$ has no quotient isomorphic to μ_p for the action of G_K.

We now check each of the conditions above. Clearly, RFX($\mathcal{D}$) is true. Since $E(K)[p] = 0$, we have $E(\mathbb{L}_\infty)[p^\infty] = 0$ and so LEO($\mathcal{D}$) and CRK($\mathcal{D}, \mathcal{L}$) follow from [25, Theorem 7.2]. This takes care of (a). Condition (b) is true by [19, Prop. 4.3.2]. Since no prime $v \in S$ splits completely in $\mathbb{L}_\infty/K$, we get by [18, Lemma 5.2.2] that $\mathrm{LOC}_v^{(1)}(\mathcal{D})$ is satisfied for all $v \in S$. This implies that $\mathrm{LOC}_v^{(2)}(\mathcal{D})$ is satisfied for all $v \in S$. Therefore, (c) is true. Finally, as explained on pg. 48 of [19], properties of the Weil pairing $E[p] \times E[p] \longrightarrow \mu_p$ imply that if $E(K)[p] = 0$, then (d) is satisfied. This completes the proof. □

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

10. Examples for Theorems 1.4 and 1.5

In this final section, we show two examples that satisfy the conditions of Theorems 1.4 and 1.5. First, we fix some notation. As in the introduction, let p be a an odd prime. If F is a number field, let F_{cyc} denote the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. If E is an elliptic curve over $\mathbb{Q}$ and $L/\mathbb{Q}$ is an algebraic extension, we let $\mathrm{Sel}(E/L)$ denote the p-primary classical Selmer group for E/L and we let $X(E/L)$ denote its Pontryagin dual.

Now let $E/F : y^2 = x^3 + ax + b$ be an elliptic curve. If d is a non-square in F, then the quadratic twist of E by d, denoted E^d, is the elliptic curve defined by the equation $E^d : y^2 = x^3 + d^2ax + bd^3$. We have the following well-known result.

Lemma 10.1. *Let F be a number field, E be an elliptic curve over F and d a non-square in F. Let $L = F(\sqrt{d})$. Then we have an isomorphism*

$$\mathrm{Sel}(E/L) \cong \mathrm{Sel}(E/F) \oplus \mathrm{Sel}(E^d/F).$$

Proof. See the proof of [49, Lemma 3.1]. □

In the setup of the previous lemma, we note that since p is odd, the extensions F_{cyc}/F and L/F are linearly disjoint over F. Therefore, we may identify the Galois groups $\mathrm{Gal}(L_{cyc}/L) = \mathrm{Gal}(F_{cyc}/F) = \Gamma_{cyc}$. The proof of loc. cit, shows that the map defining the isomorphism of the previous lemma commutes with Γ_{cyc}. Therefore, we have

Lemma 10.2. *Let F be a number field, E be an elliptic curve over F and d a non-square in F. Let $L = F(\sqrt{d})$. Then we have an isomorphism of $\mathbb{Z}_p[[\Gamma_{cyc}]]$-modules*

$$X(E/L_{cyc}) \cong X(E/F_{cyc}) \oplus X(E^d/F_{cyc}).$$

For one of our examples, we need a similar result to the previous lemma but for quartic twists. First, we define these. Let F be a number field and let

$$E : y^2 = x^3 + ax \tag{17}$$

be an elliptic curve over F with j-invariant 1728. If $d \in F^\times$, then the quartic twist of E by d, denoted E_d, is the elliptic curve defined by the equation

$$E_d : y^2 = x^3 + dax.$$

Let ζ be a primitive fourth root of unity in $\bar{\mathbb{Q}}$.

Lemma 10.3. *Let F be a number field containing ζ, E an elliptic curve over F with j-invariant* 1728 *and $d \in F^\times$. Let $L = F(\sqrt[4]{d})$ and assume that $[L{:}F] = 4$. Then we have an isomorphism*

$$\mathrm{Sel}(E/L) \cong \mathrm{Sel}(E/F) \oplus \mathrm{Sel}(E_d/F) \oplus \mathrm{Sel}(E_{d^2}/F) \oplus \mathrm{Sel}(E_{d^3}/F).$$

Proof. Let $G = \mathrm{Gal}(L/F)$ and choose $c \in L$ with $c^4 = d$. Note that G is a cyclic group of order 4. Let σ be a generator of G such that $\sigma(c) = \zeta c$. Let $[\zeta] \in \mathrm{Aut}(E)$ be defined as $[\zeta](x, y) = (\zeta^2 x, \zeta y)$. This makes $\mathrm{Sel}_p(E/L)$ a $\mathbb{Z}[\mu]$-module, where μ is the group of fourth roots of unity. We define

$$\mathrm{Sel}(E/L)^i = \{s \in \mathrm{Sel}(E/L) \mid \sigma(s) = [\zeta^i]_*(s)\}.$$

We can write $\mathrm{Sel}(E/L)$ as a direct sum of eigenspaces

$$\mathrm{Sel}(E/L) = \mathrm{Sel}(E/L)^0 \oplus \mathrm{Sel}(E/L)^1 \oplus \mathrm{Sel}(E/L)^2 \oplus \mathrm{Sel}(E/L)^3.$$

Let $E : y^2 = x^3 + ax$, so that $E_{d^i} : y^2 = x^3 + d^i ax$. Then we have an isomorphism defined over L:

$$\phi^i : E \longrightarrow E_{d^i},$$

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

defined as $\phi^i(x, y) = (c^{2i}x, c^{3i}y)$. Then we have

$$\sigma(\phi^i(x, y)) = \sigma(c^{2i}x, c^{3i}y) = (\zeta^{2i}c^{2i}\sigma(x), \zeta^{3i}c^{3i}\sigma(y)) = \phi^i([\zeta^{-i}]\sigma(x, y)).$$

This shows that for $0 \leq i \leq 3$, we have an isomorphism

$$\mathrm{Sel}(E/L)^i \cong \mathrm{Sel}(E_{d^i}/F)^G.$$

The restriction map induces a map $\psi^i : \mathrm{Sel}(E_{d^i}/F) \longrightarrow \mathrm{Sel}(E_{d^i}/F)^G$. Using the snake lemma and the inflation restriction sequence (see e.g. the proof of [22, Lemma 3.3]), we see that the kernel and cokernel of the map ψ^i are both annihilated by p and 4. Since p is odd, the map ψ^i is an isomorphism. By putting the above facts together, we get the desired isomorphism in the statement of the lemma. □

If L/F is an extension of number fields with $[L : F] = 4$, then since p is odd, the extensions F_{cyc}/F and L/F are linearly disjoint over F. Therefore, we may identify the Galois groups $\mathrm{Gal}(L_{cyc}/L) = \mathrm{Gal}(F_{cyc}/F) = \Gamma_{cyc}$. All the maps in the previous lemma commute with Γ_{cyc}. Therefore, we get:

Lemma 10.4. *Let F be a number field containing ζ, E an elliptic curve over F with j-invariant* 1728 *and $d \in F^\times$. Let $L = F(\sqrt[4]{d})$ and assume that $[L{:}F] = 4$. Then we have an isomorphism of $\mathbb{Z}_p[[\Gamma_{cyc}]]$-modules*

$$X(E/L_{cyc}) \cong X(E/F_{cyc}) \oplus X(E_d/F_{cyc}) \oplus X(E_{d^2}/F_{cyc}) \oplus X(E_{d^3}/F_{cyc}).$$

We would like to prove a similar result to the above in the case when $\zeta \notin L$. To do this, we use a trick similar to [30, Proposition 4.2] using [56, Corollary 3.5].

Lemma 10.5. *Let F be a number field, E an elliptic curve over F with j-invariant* 1728 *and $d \in F^\times$. Let $L = F(\sqrt[4]{d})$ and assume that $[L : F] = 4$ and $\zeta \notin L$. Then we have the following relations of Iwasawa invariants of $\Lambda := \mathbb{Z}_p[[\Gamma_{cyc}]]$-modules.*

(1)

$$\mathrm{rank}_\Lambda(X(E/L_{cyc})) = \sum_{i=0}^{3} \mathrm{rank}_\Lambda(X(E_{d^i}/F_{cyc})).$$

(2) If the Λ-ranks in (1) are all zero, then

$$\mu(X(E/L_{cyc})) = \sum_{i=0}^{3} \mu(X(E_{d^i}/F_{cyc})).$$

Proof. Let $L' = L(\zeta)$ and $F' = F(\zeta)$. Then $[L'{:}F'] = 4$ and $\zeta \in F'$. Therefore by Lemma 10.4, we have

$$X(E/L'_{cyc}) \cong X(E/F'_{cyc}) \oplus X(E_d/F'_{cyc}) \oplus X(E_{d^2}/F'_{cyc}) \oplus X(E_{d^3}/F'_{cyc}). \tag{18}$$

In order to get a result over L_{cyc} and F_{cyc}, we use the following observation: If E is an elliptic curve over a field K with j-invariant 1728 and $\zeta \notin K$, then its quadratic twist E^{-1} is equal to E (recall that $b = 0$ in equation (17)) and hence from Lemma 10.2 we have

$$X(E/K_{cyc}(\zeta)) \cong X(E/K_{cyc}) \oplus X(E/K_{cyc}).$$

Using this with each of the terms in the isomorphism (18), we obtain the desired result. □

For the remainder of this section, let $\mathbb{L}_\infty$ be a fixed $\mathbb{Z}_p^d$-extension of K that contains K_{cyc}. Theorems 1.4 and 1.5 require that we know $m_{0,1}$. As we will explain later, we use the Iwasawa main conjecture to find the value of $\mu(X(E/K_{cyc}))$. The following proposition then allows us to get an upper bound on $m_{0,1}$.

Proposition 10.6. *Let E be an elliptic curve defined over K. Assume that $X(E/K_{cyc})$ is Λ-torsion. Then we have*

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

(1) $X(E/\mathbb{L}_\infty)$ *is* Λ_d*-torsion,*
(2) $m_0(X(E/\mathbb{L}_\infty)) \leq \mu(X(E/K_{cyc}))$.

Proof. Let $H = \mathrm{Gal}(\mathbb{L}_\infty/K_{cyc})$. By [35, Corollary 3.15], we have

$$\mathrm{rank}_\Lambda(X(E/K_{cyc})) = \mathrm{rank}_\Lambda(X(E/\mathbb{L}_\infty))_H).$$

By [40, Lemma 4.7], the hypothesis that $X(E/K_{cyc})$ is Λ-torsion therefore implies that

$$\mathrm{rank}_{\Lambda_d}(X(E/\mathbb{L}_\infty)) = 0.$$

Therefore, we get (1).

The proof of Corollary 7.4 shows that the image of the characteristic power series of $X(E/\mathbb{L}_\infty)$ under the canonical surjection $\pi : \Lambda_d \longrightarrow \Lambda$ divides the characteristic power series of $X(E/\mathbb{L}_\infty)_H$. Since no prime splits completely in K_{cyc}/K, loc. cit. shows that $\mu(X(E/K_{cyc})) = \mu(X(E/\mathbb{L}_\infty))_H)$. We then deduce (2) from these facts. □

Let $\Gamma_{cyc} = \mathrm{Gal}(\mathbb{Q}_{cyc}/\mathbb{Q})$ and fix the Iwasawa algebra $\Lambda := \mathbb{Z}_p[[\Gamma_{cyc}]] = \mathbb{Z}_p[[T]]$. Let E be an elliptic curve defined over $\mathbb{Q}$ with good ordinary reduction at p. Let $\mathcal{L}_p(E)$ be the p-adic L-function of E defined by Mazur and Swinnerton-Dyer [43]. By results of Kato [27] and Rohrlich [52], $X(E/\mathbb{Q}_{cyc})$ is a torsion Λ-module. Let $f_{cyc} \in \mathbb{Z}_p[[T]]$ be the characteristic polynomial of $X(E/\mathbb{Q}_{cyc})$. The Iwasawa main conjecture is the following

Conjecture 10.7. *We have an equality of ideals in* $\mathbb{Z}_p[[T]]$*:* $(f_{cyc}) = (\mathcal{L}_p(E))$.

Assuming that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$, Kato [27, Theorem 17.4] shows the inclusion of ideals $(\mathcal{L}_p(E)) \subseteq (f_{cyc})$. Assuming that there is a prime q where E has multiplicative reduction and which ramifies in $\mathbb{Q}(E[p])/\mathbb{Q}$, Skinner and Urban [58] establish the reverse inclusion thus proving Conjecture 10.7. Other cases that establish Conjecture 10.7 are Kim-Kim-Sun [29] and Wan [59]. For our examples, we need two remaining cases listed below.

Theorem 10.8. *If E has complex multiplication, then Conjecture 10.7 is true.*

Proof. This is proven by Rubin [53, Theorem 12.3]. □

If E has an isogeny of degree p defined over $\mathbb{Q}$, we have an isogeny character $\phi : G_\mathbb{Q} \longrightarrow \mathbb{F}_p^\times$. This is the character describing the action of $G_\mathbb{Q} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the kernel $C \subseteq E[p]$ of the underlying p-isogeny. Let $\chi : G_\mathbb{Q} \longrightarrow \mathbb{F}_p^\times$ be the mod-p cyclotomic character and let $G_p \subseteq G_\mathbb{Q}$ be a decomposition group at p. We have the following theorem.

Theorem 10.9. *Assume that E has an isogeny of degree p defined over* $\mathbb{Q}$*. Assume that* $\phi|_{G_p} \neq 1, \chi$*. Then Conjecture 10.7 is true.*

Proof. This is proven by Castella, Grossi, and Skinner [5, Theorem A]. □

We first show an example for Theorem 1.4. Let $E_1 : y^2 + xy + y = x^3 + 296x + 1702$ be the elliptic curve 110c2 with Cremona labeling [10]. Let $K = \mathbb{Q}(\sqrt{-7})$ and $\mathbb{L}_\infty$ be the $\mathbb{Z}_3^2$-extension of K so that $p = 3$. The quadratic twist of E_1 by -7 is $(E_1)^{-7} : y^2 + xy = x^3 + x^2 + 14528x - 569344$ (5390s2). Both E_1 and $(E_1)^{-7}$ have good ordinary reduction at 3. Computations in SAGE [55] and data from the LMFDB database [42] show that E_1 and $(E_1)^{-7}$ have isogenies of degree 3 with characters of their isogenies satisfying Theorem 10.9. Also we have $\mu(\mathcal{L}(E_1)) = 1$ and $\mu(\mathcal{L}((E_1)^{-7})) = 0$. Therefore by Theorem 10.9, we have $\mu(X(E_1/\mathbb{Q}_{cyc})) = 1$ and $\mu(X((E_1)^{-7}/\mathbb{Q}_{cyc})) = 0$. By Lemma 10.2, this implies that $\mu(X(E_1/K_{cyc})) = 1$. As $K/\mathbb{Q}$ is an abelian extension results of Kato [27] and Rohrlich [52] imply

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

that $X(E_1/K_{cyc})$ is Λ-torsion. Lemma 10.2 then implies that $\mu(X(E_1/K_{cyc})) = 1$. Proposition 10.6 in turn implies that $X(E_1/\mathbb{L}_\infty))$ is a torsion Λ_2-module with $m_{0,1} \leq 1$.

Now consider the elliptic curve

$$E_2 : y^2 + xy + y = x^3 - 41279995994x + 3252655872050692 \ \text{(60610m2)}.$$

From the tables in Tom Fisher's paper [13], E_1 and E_2 are 9-congruent. Since 3 is unramified in $K/\mathbb{Q}$, it is clear that condition (Δ) in the introduction is satisfied (note that by Remark 1.6 we actually do not have to check condition (Δ) here because E_1 and E_2 are defined and congruent over $\mathbb{Q}$). Finally since $K_{cyc} \subseteq \mathbb{L}_\infty$ and $K_{cyc} \in \mathcal{E}_p \cap \mathcal{E}_{ns}$, this data satisfies the conditions of Theorem 1.4.

Now we show an example for Theorem 1.5. Let $E_1 : y^2 = x^3 + x$ be the elliptic curve 64a4. Let $K = \mathbb{Q}(\sqrt[4]{-13})$ and let $\mathbb{L}_\infty$ be the $\mathbb{Z}_5^3$-extension of K so that $p = 5$. Now consider the three quartic twists of E_1: $(E_1)_{-13} : y^2 = x^3 - 13x$ (5408e1), $(E_1)_{169} : y^2 = x^3 + 169x$ (10816bb1), and $(E_1)_{-2197} : y^2 = x^3 - 2197x$ (5408k1). E_1 and its three quartic twists have good ordinary reduction at 5. In the LMFDB database, we see that the μ-invariants of the 5-adic L-functions of all four curves are zero. As all of these curves have complex multiplication, Theorem 10.8 shows that $\mu(X(A/\mathbb{Q}_{cyc})) = 0$ where A is any of the four curves. By the results of Kato [27] and Rohrlich [52] $X(A/\mathbb{Q}_{cyc})$ is Λ-torsion for each curve A. Therefore by Lemma 10.5 we have that $X(E_1/K_{cyc})$ is Λ-torsion with μ-invariant zero. Then by Proposition 10.6 $X(E_1/\mathbb{L}_\infty)$ is Λ_3-torsion with $m_{0,1} = 0$.

Now consider the elliptic curve

$$E_2 : y^2 = x^3 - 262140x^2 + 638353031830801x - 134326647870701706899652.$$

This elliptic curve is the curve with $D = -1$ and $t = 4$ described in [54, Theorem 5.3]. Loc. cit. shows that E_1 and E_2 are 5-congruent which implies that condition (iv) of Theorem 1.5 is satisfied. Let S be the set of primes of K above p and where either E_1 or E_2 have bad reduction. Our computations in SAGE reveal that both E_1 and E_2 satisfy condition ($\star$) for all $v \in S$. The prime 5 is inert in $K/\mathbb{Q}$ which implies that condition (iii) is satisfied. Also we have $E_1(K)[5] = E_2(K)[5] = 0$. This implies that $E_1(\mathbb{L}_\infty)[5^\infty] = E_2(\mathbb{L}_\infty)[5^\infty] = 0$ so condition (i) is satisfied. Since $K_{cyc} \subseteq \mathbb{L}_\infty$ and $K_{cyc} \in \mathcal{E}_p \cap \mathcal{E}_{ns}$, we also see that the conditions of Lemma 9.2 are satisfied for both E_1 and E_2 (note that $X(E_2/\mathbb{L}_\infty)$ is Λ_3-torsion because $X(E_1/\mathbb{L}_\infty)$ is Λ_3-torsion and Theorem 1.4 applies). Thus condition (ii) is satisfied. Finally since 5 is unramified in $K/\mathbb{Q}$, it is clear that condition (Δ) in the introduction is satisfied.

Acknowledgements. We would like to thank Tom Fisher, Sam Frengley, and Meng Fai Lim for helpful correspondences during the preparation of this article. Moreover, we are grateful to the anonymous referee and to the editor Alex Bartel for providing valuable comments and suggestions.

Competing interests. The authors declare none.

References

[1] M. Atiyah and I. Macdonald, *Introduction to commutative algebra* (Adison-Wesley, Reading, Massachusetts, 1969).
[2] V. A. Babaĭcev, On some questions in the theory of Γ-extensions of algebraic number fields, *Math. USSR-Izv*. **40**(4) (1976), 675–685.
[3] V. A. Babaĭcev, On the boundedness of the Iwasawa invariant μ, *Math. USSR-Izv*. **16**(1) (1981), 1–19.
[4] S. Bosch, *Algebra*, 5th ed. (Springer, 2003).
[5] F. Castella, G. Grossi and C. Skinner, Mazur's main conjecture at Eisenstein primes, *Math. Ann*. **393**(2), (2025), 2451–2506.
[6] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, The GL_2 main conjecture for elliptic curves without complex multiplication, *Publ. Math. Inst. Hautes Études Sci*. **101** (2005), 163–208.
[7] J. Coates and R. Greenberg, Kummer theory for Abelian varieties over local fields, *Invent. Math*. **124** (1996), 129–174.
[8] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, 2nd ed, (Published by Narosa Publishing House, New Delhi, Mumbai, 2010).
[9] J. Coates and R. Sujatha, On the $\mathfrak{M}_H(G)$-conjecture, in *Non-abelian fundamental groups and Iwasawa theory*, London Math. Soc. Lecture Note Ser., vol. 393, (Coates J., Kim M., Pop F., Saïdi M. and Schneider P., Editors) (Cambridge University Press, Cambridge, 2012), 132–161.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

[10] J. E. Cremona, *Algorithms for modular elliptic curves*, 2 ed. (Cambridge University Press, Cambridge, 1997).
[11] A. Cuoco and P. Monsky, Class numbers in $\mathbb{Z}_p^d$-extensions, *Math. Ann.* **255**(2) (1981), 235–258.
[12] D. Eisenbud, *Commutative algebra: with a view toward algebraic geometry*, Grad. Texts in Math. vol. 150 (Springer-Verlag, New York, 1995).
[13] T. A. Fisher, On families of n-congruent elliptic curves, (2011), Preprint. http://arxiv.org/abs/1105.1706.
[14] R. Greenberg, The iwasawa invariants of Γ-extensions of a fixed number field, *Amer. J. Math.* **95** (1973), 204–214.
[15] R. Greenberg, Iwasawa theory for p-adic representations, in *Algebraic number theory*, Adv. Stud. Pure Math., vol. 17 (Academic Press, Boston, MA, 1989), 97–137.
[16] R. Greenberg, Iwasawa theory for elliptic curves, in *Arithmetic theory of elliptic curves (Cetraro, 1997)*, Lecture Notes in Math., 1716, (Springer, Berlin, 1716), 51–144,
[17] R. Greenberg, Galois theory for the selmer group of an abelian variety, *Compos. Math.* **136** (2003), 255–297.
[18] R. Greenberg, Surjectivity of the global-to-local map defining a Selmer group, *Kyoto J. Math.* **50** (2011), 853–888.
[19] R. Greenberg, On the structure of Selmer groups, in *Elliptic curves, modular forms and iwasawa theory (in honour of John H. Coates' 70th birthday*, D. Loeffler and S. L. Zerbes, Editors), Springer, 2016), 225–252, Springer Proc. in Math. and Stat. 188.
[20] R. Greenberg and V. Vatsal, On the Iwasawa invariants of elliptic curves, *Invent. Math.* **142**(1) (2000), 17–63.
[21] L. Guo, On a generalization of Tate dualities with application to Iwasawa theory, *Compositio. Math.* **85** (1993), 125–161.
[22] Y. Hachimori and K. Matsuno, An analogue of Kida's formula for the Selmer groups of elliptic curves, *J. Algebraic Geometry* **8** (1999), 581–601.
[23] Y. Hachimori and K. Matsuno, On finite Λ-submodules of Selmer groups of elliptic curves, *Proc. Amer. Math. Soc.* **128**(9) (2000), 2539–2541.
[24] Y. Hachimori and T. Ochiai, Notes on non-commutative Iwasawa theory, *Asian J. Math.* **14**(1) (2010), 11–17.
[25] Y. Hachimori and O. Venjakob, Completely faithful Selmer groups over Kummer extensions, *Doc. Math. Extra Vol.* (2003), 443–478.
[26] S. Howson, Euler characteristics as invariants of Iwasawa modules, *Proc. London Math. Soc.* **85**(3–3) (2002), 634–658.
[27] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, in *Cohomologies p-adique et applications arithmetiques III*, Astérisque 295, (2004), 117–290.
[28] K. Kidwell, On the structure of Selmer groups of p-ordinary modular forms over $\mathbb{Z}_p$-extensions, *J. Number Theory* **187** (2018), 296–331.
[29] C. H. Kim, M. Kim and H. S. Sun, On the indivisibility of derived Kato's Euler systems and the main conjecture for modular forms, *Selecta Math. (N.S.)* **26**(31) (2020), 47.
[30] N. Kim, Twists of elliptic curves, *Ph.D. thesis*. Seoul National University; 2014
[31] S. Kleine, Local behavior of Iwasawa's invariants, *Int. J. Number Theory* **13**(4) (2017), 1013–1036.
[32] S. Kleine, Bounding the Iwasawa invariants of Selmer groups, *Canad. J. Math.* **73**(5) (2021), 1390–1422.
[33] S. Kleine and K. Müller, Fine Selmer groups of congruent p-adic Galois representations, *Canad. Math. Bull.* **65**(3) (2022), 702–722.
[34] S. Kleine and K. Müller, Fine Selmer groups and ideal class groups, *Ramanujan J.* **61**(4) (2023), 1213–1267.
[35] S. Kleine and A. Matar, Boundedness of Iwasawa invariants of fine Selmer groups and Selmer groups, *Results Math.* **78** (2023), 148.
[36] S. Kleine, A. Matar and R. Sujatha, On the $\mathfrak{M}_H(G)$-property, *Math. Proc. Camb. Philos. Soc.* **179**(2) (2025), 449–501.
[37] D. Kundu and A. Ray, Iwasawa invariants for elliptic curves over $\mathbb{Z}_p$-extensions and Kida's formula, *Forum Math.* **34**(4) (2022), 945–967.
[38] M. F. Lim, A remark on the $\mathfrak{M}_H G$-conjecture and Akashi series, *Int. J. Number Theory* **11**(1) (2015), 269–297.
[39] M. F. Lim, Comparing the π-primary submodules of the dual Selmer groups, *Asian Math. J.* **21**(6) (2017), 1153–1182.
[40] M. F. Lim, Notes on the fine Selmer groups, *Asian J. Math.* **21**(2) (2017), 337–362.
[41] M. F. Lim, $\mathfrak{M}_H(G)$*-property and congruence of Galois representations*, *J. Ramanujan Math. Soc.* **33**(1) (2018), 37–44.
[42] The LMFDB Collaboration, The L-functions and modular forms database. 2023. Available at https://www.lmfdb.org (accessed 11 October 2023).
[43] B. Mazur and P. Swinnerton-Dyer, Arithmetic of Weil curves, *Invent. Math.* **25** (1974), 1–61.
[44] J. S. Milne, *Arithmetic Duality theorems*, 2nd ed. BookSurge, LLC, Charleston, SC, 2006).
[45] J. Minardi, Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields. Thesis (University of Washington; 1986).
[46] P. Monsky, Some invariants of $\mathbb{Z}_p^d$-extensions, *Math. Ann.* **255**(2) (1981), 229–233.
[47] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, 2nd ed. Grundlehren der Mathematischen Wissenschaften, vol. 323 (Springer, 2008), xvi+825.
[48] Y. Ochi and O. Venjakob, On the structure of Selmer groups over p-adic Lie extensions, *J. Algebraic Geometry* **11** (2002), 547–580.
[49] K. Ono, M. Papanikolas and A. K. Peters, Quadratic twists of modular forms and elliptic curves, *Number theory for the millennium III*, (Urbana, IL, 2000) (Peters, A.K. and Natick, M.A., 2002), 73–85.
[50] G. Perbet, Sur les invariants d'Iwasawa dans les extensions de Lie *p*-adiques, *Algebra Number Theory* **5** (6) (2011), 819–848.
[51] L. Ribes and P. Zalesskii, *Profinite groups*, Ergeb. der Math. 40, (Springer-Verlag, 2000).

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press

[52] D. Rohrlich, On L-functions of elliptic curves and cyclotomic towers, *Invent. Math*. **75** (1984), 409–423.
[53] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math*. **103**(1) (1991), 25–68.
[54] K. Rubin and A. Silverberg, Families of elliptic curves with constant mod p representations, in *Elliptic curves, modular forms, & Fermat's last theorem*. (Hong Kong, 1993), Ser. Number Theory, I (Int. Press, Cambridge, MA, 1995), 148–161.
[55] SageMath, The Sage Mathematics Software System (Version 8.9). 2019, Available at http://www.sagemath.org.
[56] A. Sato, The behavior of Mordell-Weil groups under field extensions, *J. Health Inform*. **27** (2022), 15–26.
[57] J. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math. 106, (Springer-Verlag, 2009).
[58] C. Skinner and E. Urban, The Iwasawa main conjectures for GL_2, *Invent. Math*. **195** (2014), 1–277.
[59] X. Wan, The Iwasawa main conjecture for Hilbert modular forms, *Forum Math. Sigma*. **3**(e18) (2015), 95.

https://doi.org/10.1017/S0017089526100901 Published online by Cambridge University Press