ESTIMATING THE GROWTH IN MORDELL-WEIL RANKS AND SHAFAREVICH-TATE GROUPS OVER LIE EXTENSIONS

DANIEL DELBOURGO AND ANTONIO LEI

ABSTRACT. Let $E_{/\mathbb{Q}}$ be an elliptic curve, $p > 3$ a good ordinary prime for E, and K_∞ a p-adic Lie extension of a number field k. Under some standard hypotheses, we study the asymptotic growth in both the Mordell-Weil rank and Shafarevich-Tate group for E over a tower of extensions K_n/k inside K_∞; we obtain lower bounds on the former, and upper bounds on the latter's size.

CONTENTS

2010 *Mathematics Subject Classification.* 11R23, 11G05 (primary); 22E20, 22E05.

Key words and phrases. Elliptic curves, Mordell-Weil ranks, noncommutative Iwasawa theory.

The second named author's research is supported by FRQNT's Établissement de nouveaux chercheurs universitaires program 188809.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$, and assume E has good ordinary reduction at a prime number $p > 3$. In [DT10], Darmon and Tian showed under certain technical hypotheses that the Mordell-Weil rank of E over the fields $\mathbb{Q}\big(\mu_{p^n}, l^{1/p^n}\big)$ is exactly $p^n - 1$ for all $n \geq 1$, where l is a prime of split multiplicative reduction. In the first half of this paper, we generalise their result to

(i) p-adic Lie extensions of number fields whose Galois groups are $\mathbb{Z}_p^2 \rtimes \mathbb{Z}_p$;

(ii) the $(d-1)$-fold false Tate extensions $K_\infty = \mathbb{Q}\big(\mu_{p^\infty}, l_1^{1/p^\infty}, \ldots, l_{d-1}^{1/p^\infty}\big)$.

Let $G_\infty = \mathrm{Gal}(K_\infty/k)$, and consider the tower of extensions K_n given by taking the fixed field of K_∞ for the powers $G_\infty^{p^n}$; in particular $k = K_0 \subset K_1 \subset \ldots K_\infty$.

Under various hypotheses (see **(P1)**–**(P3)** and **(DT1)**–**(DT7)** in Section 2), we show that there exists an explicit rational number $\delta_p > 0$ such that

$$\delta_p \times p^{(d-1)n} - 1 \;\leq\; \mathrm{rank}_{\mathbb{Z}}\, E(K_n) \;\leq\; \tau \times p^{(d-1)n} \tag{1.1}$$

where τ is the generic λ-invariant of the Selmer group. To find an exact formulae for δ_p in some concrete examples, we refer the reader to Propositions 2.14 and 2.17. If $K_\infty = \mathbb{Q}\big(\mu_{p^\infty}, l_1^{1/p^\infty}, l_2^{1/p^\infty}\big)$ and $\tau = 1$, we can even say (Corollary 2.16) that

$$\mathrm{rank}_{\mathbb{Z}}\, E(K_n) \;=\; p^{2n} - 1 \;\text{ or }\; p^{2n}.$$

There are two approaches to obtain these results. The first uses the Dokchitsers' parity formulae [DD09], as well as results of Greenberg [Gre11] and Guo [Guo93] on Selmer multiplicities. The second directly generalises the techniques in [DT10]. We construct a tree whose vertices ρ are irreducible Artin representations of G_∞, and then analyse the ρ-part of the Mordell-Weil rank along branches of the tree.

In the second half of this paper, we examine the growth in the p-primary part of the Shafarevich-Tate groups $Ш(E/K_n)$ under the assumption that they are finite. We prove an asymptotic upper bound

$$\#Ш(E/K_n)[p^\infty] \;\leq\; p^{\mu p^{dn} + (\tau p^{(d-1)n} - \mathrm{rank}_{\mathbb{Z}}\, E(K_n))n + O(p^{(d-1)n})}$$

where 'μ' is the μ-invariant of the Pontryagin dual of the Selmer group of E/K_∞ (see Theorem 4.13). Hence, using the lower bound on $\mathrm{rank}_{\mathbb{Z}}\, E(K_n)$ given in (1.1):

$$\#Ш(E/K_n)[p^\infty] \;\leq\; p^{\mu p^{dn} + (\tau - \delta_p) n p^{(d-1)n} + O(p^{(d-1)n})}. \tag{1.2}$$

The proof of Theorem 4.13 needs a refinement of Greenberg's control theorem [Gre03] for the Selmer group; more precisely, one must study the kernel and cokernel of the restriction maps

$$\alpha_n : \mathrm{Sel}_p(E/K_n) \to \mathrm{Sel}_p(E/K_\infty)^{G_\infty^{p^n}}.$$

We shall prove that $\ker(\alpha_n)$ and $\mathrm{coker}(\alpha_n)$ are both finite groups, and then obtain an asymptotic estimate on their size as $n \to \infty$.

The bounds on the Shafarevich-Tate groups resemble the ones for class groups proved by Cuoco-Monsky [CM81] in the case $G_\infty \cong \mathbb{Z}_p^d$, and by Perbet [Per11] in the non-commutative case (our inequalities (1.2) have the same shape as the former). Furthermore, assuming the $\mathfrak{M}_{\mathcal{H}}(G_\infty)$-conjecture and other technical hypotheses, we obtain bounds that are marginally stronger than those in [Per11].

2. The structure of the Mordell-Weil group

Determining the exact growth rate in the rank of the Mordell-Weil group of an elliptic curve seems a difficult problem. If one lowers their expectations somewhat, in certain cases it is possible to bound (both above and below) the growth rate so the error term does not dominate the formula. We outline two such approaches here, and study their implications in some specific examples at the end of the section.

2.1. **Preliminaries.** Let k be a number field, and K_∞/k a p-adic Lie extension such that

$$G_\infty := \mathrm{Gal}(K_\infty/k) \;\cong\; \Gamma \ltimes \mathcal{H}, \quad \text{where } \Gamma \cong \mathbb{Z}_p \text{ and } \dim(\mathcal{H}) = d-1.$$

We assume G_∞ has no torsion, and identify Γ with the Galois group of the cyclotomic $\mathbb{Z}_p$-extension k^{cy} of k. Choose a generator γ of Γ, so that $\Gamma = \overline{\langle\gamma\rangle}$.

If $\dim(G_\infty) = 1$ clearly $G_\infty = \Gamma$. Similarly, if $\dim(G_\infty) = 2$ then either

$$G_\infty \cong \mathbb{Z}_p^2, \qquad \text{or} \qquad G_\infty \cong \Gamma \ltimes \mathbb{Z}_p.$$

Assume the dimension of G_∞ is equal to 3. We remark that G_∞ is soluble (because $G_\infty/\mathcal{H} \cong \Gamma$ and $\mathcal{H}$ is of dimension 2). The classification of such soluble groups was found by Klopsch and Gonzales-Sanchez, and is discussed at length in [Klo03, Theorem 7.4].

Theorem 2.1. *If G_∞ is soluble and torsion-free, then G_∞ is isomorphic to one of the following possibilities:*

1. *the abelian group $\mathbb{Z}_p^3$;*
2. *an open subgroup of the Heisenberg group, i.e. a group represented by $\langle \gamma, h_1, h_2 : [h_1,h_2]=1, [h_1,\gamma]=1, [h_2,\gamma]=h_1^{p^s}\rangle$ for some $s \in \mathbb{N}_0$;*
3. *$\langle \gamma, h_1, h_2 : [h_1,h_2]=1, [h_1,\gamma]=h_1^{p^s}, [h_2,\gamma]=h_2^{p^s}\rangle$ for some $s \in \mathbb{N}$;*
4. *$\langle \gamma, h_1, h_2 : [h_1,h_2]=1, [h_1,\gamma]=h_1^{p^s}h_2^{p^{s+r}d}, [h_2,\gamma]=h_1^{p^{s+r}}h_2^{p^s}\rangle$ for some $s, r \in \mathbb{N}$ and $d \in \mathbb{Z}_p$;*
5. *$\langle \gamma, h_1, h_2 : [h_1,h_2]=1, [h_1,\gamma]=h_2^{p^s d}, [h_2,\gamma]=h_1^{p^s}h_2^{p^{s+r}}\rangle$ where $s, r \in \mathbb{N}_0$ and $d \in \mathbb{Z}_p$, such that either $s \geq 1$, or $r \geq 1$ and $d \in p\mathbb{Z}_p$;*
6. *either one of $\langle \gamma, h_1, h_2 : [h_1,h_2]=1, [h_1,\gamma]=h_2^{p^{s+r}}, [h_2,\gamma]=h_1^{p^s}\rangle$ or $\langle \gamma, h_1, h_2 : [h_1,h_2]=1, [h_1,\gamma]=h_2^{p^{s+r}t}, [h_2,\gamma]=h_1^{p^s}\rangle$ where $s, r \in \mathbb{N}_0$ with $s+r \geq 1$ and $t \in \mathbb{Z}_p^\times$ is not a square modulo p.*

For example, in case (2) one has

$$G_\infty \lhd \begin{pmatrix} 1 & \mathbb{Z}_p & \mathbb{Z}_p \\ 0 & 1 & \mathbb{Z}_p \\ 0 & 0 & 1 \end{pmatrix}.$$

Likewise in case (3), provided $\mu_p \subset k$ then K_∞ may be realised as an extension of the form $k\big(\mu_{p^\infty}, m_1^{1/p^\infty}, m_2^{1/p^\infty}\big)$ where p, m_1, m_2 are pairwise coprime as integers.

Let E be an elliptic curve over k with good ordinary reduction at all primes above p. Given an extension L of k, we write $\mathcal{X}_E(L)$ for the Pontryagin dual of the p-primary part of the Selmer group of E over L. The following result from [DL15b] gives an upper bound on the Mordell-Weil rank of E.

Theorem 2.2. *If $\mathcal{X}_E(K_\infty)$ is a $\mathbb{Z}_p[\![G_\infty]\!]$-torsion module which belongs to the category $\mathfrak{M}_{\mathcal{H}}(G_\infty)$ and if $d = \dim(G_\infty) \leq 3$, then there exists a filtration*

$$k \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty \quad \text{with} \quad \big[K_n : k\big] = p^{dn}$$

and a natural number $n_0 \leq 2$, such that

$$\operatorname{rank}_{\mathbb{Z}} E(K_n) \ \leq \ \tau_{E,G_\infty} \times p^{(d-1)n} + 4 \quad \text{for all } n \geq n_0$$

where $\tau_{E,G_\infty} = \operatorname{rank}_{\mathbb{Z}_p[\![\mathcal{H}]\!]} \left(\frac{\mathcal{X}_E(K_\infty)}{\mathcal{X}_E(K_\infty)[p^\infty]} \right) \geq 0$.

Note the definition of τ_{E,G_∞} above appears slightly differently in [DL15b, Corollary 2] though the two are easily seen to be equivalent. The filtration itself arises by taking p-powers of the generators for G_∞, then fixing by the resulting subgroups.

Proposition 2.3. *If only finitely many primes ramify in K_∞/k, the prime $p > 3$ and $\mathcal{X}_E(K_\infty) \in \mathfrak{M}_{\mathcal{H}}(G_\infty)$, then*

$$\tau_{E,G_\infty} = \ \lambda(E/k^{\mathrm{cy}}) \ + \ m_{\mathrm{sm}}^{\mathrm{cy}} \ + \ 2 \times m_{\mathrm{pgr}}^{\mathrm{cy}}$$

where (i) $\lambda(E/k^{\mathrm{cy}})$ is the cyclotomic λ-invariant of $\mathcal{X}_E(k^{\mathrm{cy}})$ as a $\mathbb{Z}_p[\![\Gamma]\!]$-module, (ii) $m_{\mathrm{sm}}^{\mathrm{cy}}$ counts the number of primes ν of k^{cy} where E has split multiplicative reduction and ν is infinitely ramified in K_∞/k^{cy}, that is, it has infinite ramification index, and (iii) $m_{\mathrm{pgr}}^{\mathrm{cy}}$ denotes the number of primes ν of k^{cy} where $ord_\nu(j_E) > 0$, ν is infinitely ramified in K_∞/k^{cy} with $E(k_\nu^{\mathrm{cy}})_{p^\infty} \neq 0$.

Proof. If F is an extension of k, we shall write $Y(E/F)$ for the quotient $\frac{\mathcal{X}_E(F)}{\mathcal{X}_E(F)[p^\infty]}$.

For a prime ν of k^{cy}, let us write $I_{\nu,\infty} \subset \mathrm{Gal}(K_\infty/k^{\mathrm{cy}})$ for the inertia subgroup at ν. We use a general formula from [CFKS10, Theorem 3.5] which holds for extensions K_∞/k in which only finitely many primes can ramify – however we need only to specialise this formula at the trivial representation:

$$\operatorname{rank}_{\mathbb{Z}_p} H_0\big(\mathcal{H}, Y(E/K_\infty)\big) = \ \operatorname{rank}_{\mathbb{Z}_p} Y(E/k^{\mathrm{cy}}) \ + \sum_{\nu \nmid p, \ \# I_{\nu,\infty} = \infty} \operatorname{rank}_{\mathbb{Z}_p} H^0\big(\overline{k}_\nu / k_\nu^{\mathrm{cy}}, T_p E\big).$$

The left-hand side is precisely $\tau_{E,G_\infty} = \operatorname{rank}_{\mathbb{Z}_p[\![\mathcal{H}]\!]} Y(E/K_\infty)$, while the middle term coincides with the λ-invariant of $\mathcal{X}_E(k^{\mathrm{cy}})$.

We note that as $p \geq 5$ and K_∞/k is a pro-p-extension, the reduction type for E at any prime of k cannot change at all as we climb up the tower of number fields. The last summation can then be computed easily using [CFKS10, Lemma 3.7]. □

The goal in the rest of this section is to outline two different methods of obtaining lower bounds on the rank. The first of these uses parity statements from [CFKS10, Gre11, Dok05] as well as the main result of [DL15b], but it only works for orthogonal representations. The second method adapts work of Darmon and Tian [DT10, Theorem 1.8] concerning explicit Kummer extensions with Galois group $\mathbb{Z}_p^\times \ltimes \mathbb{Z}_p$.

2.2. **Trees associated to p-adic Lie groups.** Let us begin by reviewing the representation theory of G_∞. We assume in this section that $\mathcal{H}$ is a free $\mathbb{Z}_p$-module of rank $d-1$. The finite-dimensional irreducible representations of G_∞ are then of the form

$$\rho_{\chi,\psi} \ = \ \psi \otimes \mathrm{Ind}_{\mathrm{Stab}_\Gamma(\chi) \ltimes \mathcal{H}}^{G_\infty}(\chi)$$

where $\chi : \mathcal{H} \to \mu_{p^\infty}$ and $\psi : \Gamma \to \mathbb{C}^\times$ are multiplicative characters of finite order. Throughout we fix representatives for the orbit under Γ of each character on $\mathcal{H}$.

Definition 2.4. *We associate a tree* $\mathbb{T} = \mathbb{T}_{G_\infty} = (\mathcal{V}, \mathcal{E})$ *to our p-adic group* G_∞ *by setting its vertices to equal*

$$\mathcal{V} \ := \ \big\{\rho \text{ such that } \rho = \mathrm{Ind}_{\mathrm{Stab}_\Gamma(\chi)\ltimes\mathcal{H}}^{G_\infty}(\chi) \text{ for some } \chi \text{ on } \mathcal{H}\big\}$$

and defining its edge set by

$$\mathcal{E} \ := \ \big\{(\rho_1, \rho_2) \text{ such that } \rho_1 = \mathrm{Ind}(\chi) \text{ and } \rho_2 = \mathrm{Ind}(\chi^p) \text{ for some } \chi \neq \mathbf{1}\big\}.$$

The tree $\mathbb{T}$ is a combinatorial device for keeping track of arithmetic data at the irreducible representations $\rho \in \mathcal{V}$. Evidently $\rho_0 = \mathbf{1}$ is the root vertex, and the distance between $\rho \in \mathcal{V}$ and ρ_0 along the edges of the tree is denoted by 'length(ρ)'. The structure of each tree $\mathbb{T}_{G_\infty}$ is particular to the underlying Lie group G_∞, and (in general) the dimension of ρ should increase with length(ρ), unless G_∞ is abelian in which case $\dim(\rho)$ remains fixed at one.

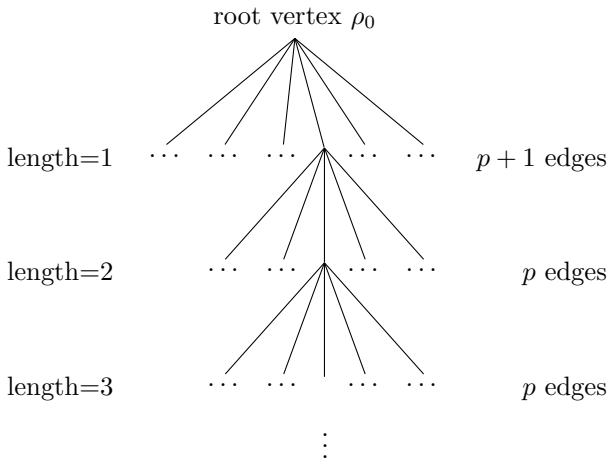

Figure 1. *The tree associated to a* 2*-fold false Tate extension.*

Let us now assume we are given a weighting $\underline{\mathcal{W}} = \big\{\mathcal{W}_\rho\big\}_{\rho\in\mathcal{V}}$ of non-negative integers attached to the vertices of $\mathbb{T}_{G_\infty}$ (for example, the weighting $\underline{\mathcal{W}}$ might encode the multiplicity of the Artin representations $\rho \in \mathcal{V}$ inside the vector space $E(K_\infty)\otimes\mathbb{C}$). The volume of $\underline{\mathcal{W}}$ at length $\leq n$ in the tree $\mathbb{T} = \mathbb{T}_{G_\infty}$ is defined by

$$\mathrm{vol}_{\leq n}\big(\mathbb{T}, \underline{\mathcal{W}}\big) \ := \sum_{\substack{\rho \ \in \ \mathcal{V}, \\ 0 \ < \ \mathrm{length}(\rho) \ \leq \ n}} \mathcal{W}_\rho \times \dim(\rho)$$

and measures the total weight contribution from vertices at most n edges from ρ_0. It also satisfies the following useful descent property.

Let k' be any subfield of k such that k/k' is a normal extension of number fields, and define the relative volume to equal

$$\mathrm{vol}_{\leq n}^{(k/k')}\big(\mathbb{T}, \underline{\mathcal{W}}\big) \ := \sum_{\substack{\rho' \ \subset \ \mathrm{Ind}_k^{k'}(\rho), \ \rho \ \in \ \mathcal{V}, \\ 0 \ < \ \mathrm{length}(\rho) \ \leq \ n}} \mathcal{W}_\rho \times \dim\big(\rho'\big).$$

Lemma 2.5. *(i) If at every vertex $\rho \in \mathcal{V}$ with $\dim(\rho) > 1$ each representation $\mathrm{Ind}_k^{k'}(\rho)$ is irreducible, one has an inequality*

$$\mathrm{vol}_{\leq n}^{(k/k')}\big(\mathbb{T}, \underline{\mathcal{W}}\big) \ \geq \ \big[k : k'\big] \times \Big(\mathrm{vol}_{\leq n}\big(\mathbb{T}, \underline{\mathcal{W}}\big) \ - \sum_{\substack{\rho \in \mathcal{V},\ \dim(\rho) = 1, \\ 0 < \mathrm{length}(\rho) \leq n}} \mathcal{W}_\rho\Big).$$

(ii) Furthermore, assuming the only characters on G_∞ factor through Γ then

$$\mathrm{vol}_{\leq n}^{(k/k')}\big(\mathbb{T}, \underline{\mathcal{W}}\big) \ = \ \big[k : k'\big] \times \mathrm{vol}_{\leq n}\big(\mathbb{T}, \underline{\mathcal{W}}\big).$$

Proof. We use the formula $\dim\big(\mathrm{Ind}_k^{k'}(\rho)\big) = [k : k'] \times \dim(\rho)$, together with the fact that the functor $\mathrm{Ind}_k^{k'}(-)$ identifies each ρ with a single unique ρ' if $\dim(\rho) > 1$. □

Definition 2.6. *A tree $\mathbb{T}_{G_\infty}$ is* **in bloom** *with respect to a weighting $\{\mathcal{W}_\rho\}_{\rho \in \mathcal{V}}$ if*

$$\max\big\{\mathcal{W}_\sigma \ \big| \ \sigma \in \mathcal{V} \text{ with } \mathrm{Ker}(\sigma) = \mathrm{Ker}(\rho)\big\} \ > \ 0$$

for all $\rho \in \mathcal{V}$ with $\mathrm{length}(\rho) > 0$.

The next result gives a non-trivial lower bound on the volume of a tree weighting.

Theorem 2.7. *Assume that the pair $\big(\mathbb{T}_{G_\infty}, \underline{\mathcal{W}}\big)$ is in bloom.*
(a) If G_∞ is abelian and $\dim(G_\infty) = d$, then

$$\mathrm{vol}_{\leq n}\big(\mathbb{T}, \underline{\mathcal{W}}\big) \ \geq \ \begin{cases} \frac{(p^{d-1}-1)(p^{n(d-2)}-1)}{(p-1)(p^{d-2}-1)} & \text{if } d > 2 \\ n(d-1) & \text{if } d = 1 \text{ or } 2. \end{cases}$$

(b) If $G_\infty \cong \Gamma \ltimes \mathbb{Z}_p^{d-1}$ is non-abelian of dimension d, then

$$\mathrm{vol}_{\leq n}\big(\mathbb{T}, \underline{\mathcal{W}}\big) \ \geq \ \frac{p^{(d-1)n} - 1}{p - 1}.$$

(c) If G_∞ is 3-dimensional and occurs as in Case (3) of Theorem 2.1,

$$\mathrm{vol}_{\leq n}\big(\mathbb{T}, \underline{\mathcal{W}}\big) \ \geq \ \frac{p^{2n-s+1} + p^s - p - 1}{p - 1}.$$

(d) If G_∞ is as in Case (5) of Theorem 2.1 with $s = d = 0$ and $r \geq 1$,

$$\mathrm{vol}_{\leq n}\big(\mathbb{T}, \underline{\mathcal{W}}\big) \ \geq \ p^{2n} \times \frac{p^{1-r}(p^2 + p + 1)}{(p-1)(p+1)^2} \ + \ \frac{n \times p^r}{p+1} \ + \ \textit{a constant.}$$

In principle we could treat all six three-dimensional types listed in Theorem 2.1, but we only make use of these limited cases (a)–(d) in our arithmetic applications.

Proof. (a) If $d = 1$ then $\mathbb{T}_{G_\infty} = \mathbb{T}_\Gamma$ consist of only the root vertex, and no edges. If $d > 1$, the vertices of $\mathbb{T}_{G_\infty}$ of length at most n are in one-to-one correspondence with characters $\chi : \mathcal{H} \to \mu_{p^n}$; consequently

$$\mathrm{vol}_{\leq n}\big(\mathbb{T}, \underline{\mathcal{W}}\big) \ = \ \sum_{\chi : \mathcal{H} \to \mu_{p^n}, \ \chi \neq \mathbf{1}} \mathcal{W}_{\mathrm{Ind}(\chi)} \times 1 \ = \ \sum_{j=1}^{n} \sum_{\chi : \mathcal{H} \twoheadrightarrow \mu_{p^j}} \mathcal{W}_{\mathrm{Ind}(\chi)}.$$

However for each set of characters $\chi : \mathcal{H} \twoheadrightarrow \mu_{p^j}$ there are precisely $\frac{p^{j(d-1)} - p^{(j-1)(d-1)}}{\phi(p^j)}$ distinct $\mathrm{Ker}(\chi)$'s, and also $\mathcal{W}_{\mathrm{Ind}(\chi)} \geq 1$ for at least one χ per kernel, whence

$$\mathrm{vol}_{\leq n}\big(\mathbb{T}, \underline{\mathcal{W}}\big) \ \geq \ \sum_{j=1}^{n} \frac{p^{j(d-1)} - p^{(j-1)(d-1)}}{\phi(p^j)} \ = \ \begin{cases} n & \text{if } d = 2 \\ \frac{(p^{d-1}-1)(p^{n(d-2)}-1)}{(p-1)(p^{d-2}-1)} & \text{if } d > 2. \end{cases}$$

(b) If $G_\infty \cong (1+p\mathbb{Z}_p) \ltimes \mathbb{Z}_p^{d-1}$ then $\mathbb{T}_{G_\infty}$ has $D_j = \frac{p^{j(d-1)}-p^{(j-1)(d-1)}}{\phi(p^j)}$ vertices of length j, let us call them $\rho_i^{(j)}$ say, each with their own unique kernel [DP15, Section 2] and of dimension p^{j-1} for $j>0$. It follows that

$$\mathrm{vol}_{\le n}\big(\mathbb{T},\underline{\mathcal{W}}\big) \;=\; \sum_{j=1}^{n}\sum_{i=1}^{D_j} \mathcal{W}_{\rho_i^{(j)}} \times p^{j-1} \;\ge\; \sum_{j=1}^{n}\sum_{i=1}^{D_j} 1 \times p^{j-1} \;=\; \sum_{j=1}^{n} D_j \times p^{j-1}$$

and the right-hand series sums to $\frac{p^{(d-1)n}-1}{p-1}$, so we are done.

(c) The topological generator γ of Γ acts on $\mathcal{H}$ via multiplication by $1+p^s$, hence $\gamma^{-p^m} h \gamma^{p^m} \equiv (1+p^{s+m})h \mod p^{s+m+1}$ for all $h \in \mathcal{H}$. If $\chi : \mathcal{H} \twoheadrightarrow \mu_{p^j}$ then

$$\dim\Big(\mathrm{Ind}_{\mathrm{Stab}_\Gamma(\chi)\ltimes\mathcal{H}}^{G_\infty}(\chi)\Big) \;=\; \big[\Gamma : \mathrm{Stab}_\Gamma(\chi)\big] \;=\; \begin{cases} p^{j-s} & \text{if } j \ge s \\ p^0 & \text{if } j < s. \end{cases}$$

Here each vertex $\rho = \mathrm{Ind}(\chi) \in \mathcal{V}$ of length j is in one-to-one correspondence with the subsets $\mathrm{Ker}(\chi) \subset \mathcal{H}$ of index p^j; the total number of $\mathrm{Ker}(\chi)$'s is $\frac{p^{2j}-p^{2(j-1)}}{\phi(p^j)}$ as we saw previously in (a). It follows that as $\big(\mathbb{T},\underline{\mathcal{W}}\big)$ is in bloom,

$$\begin{aligned}
\mathrm{vol}_{\le n}\big(\mathbb{T},\underline{\mathcal{W}}\big) \;&=\; \sum_{j=1}^{n} \sum_{\substack{\mathrm{Ker}(\chi)\,\subset\,\mathcal{H},\\ [\mathcal{H}\,:\,\mathrm{Ker}(\chi)]\,=\,p^j}} \mathcal{W}_{\mathrm{Ind}(\chi)} \times \big[\Gamma : \mathrm{Stab}_\Gamma(\chi)\big] \\
&\ge\; \sum_{j=1}^{n} \frac{p^{2j}-p^{2(j-1)}}{\phi(p^j)} \times \begin{cases} p^{j-s} & \text{if } j \ge s \\ p^0 & \text{if } j < s \end{cases} \\
&=\; \sum_{j=1}^{s-1} (p+1)p^{j-1} \;+\; \sum_{j=s}^{n} (p+1)p^{j-1} \times p^{j-s}
\end{aligned}$$

which yields $\frac{p^{2n-s+1}+p^s-p-1}{p-1}$ upon summing both geometric series.

(d) Here $G_\infty \cong \Gamma \ltimes \mathcal{H} \cong \big(\Gamma \times \langle h_1\rangle\big) \ltimes \langle h_2\rangle$ where h_1 commutes with h_2, and γ acts on h_2 through multiplication by $1+p^r$. There are two types of characters on $\mathcal{H} = \langle h_1, h_2\rangle$ of order p^j:

- $\chi = \chi_1\chi_2$ with $\chi_1 : \langle h_1\rangle \to \mu_{p^j}$ and $\chi_2 : \langle h_2\rangle \twoheadrightarrow \mu_{p^j}$ … "Type (I)"
- $\chi = \chi_1\chi_2$ with $\chi_1 : \langle h_1\rangle \twoheadrightarrow \mu_{p^j}$ and $\chi_2 : \langle h_2\rangle \to \mu_{p^{j-1}}$ … "Type (II)".

Every vertex ρ of length j is induced by such a character above, but each $\mathrm{Ker}(\chi)$ has $\phi(p^j)$ different characters with that same kernel. Also, in Type (I) the dimension of the associated vertex $\rho = \mathrm{Ind}(\chi)$ is always $p^{\max\{0,j-r\}}$, but in Type (II) the dimension of the associated ρ is $p^{\max\{0,i-r\}}$ where $\chi = \chi_1\chi_2$ and $p^i = \mathrm{order}(\chi_2)$. Since the pair $\big(\mathbb{T},\underline{\mathcal{W}}\big)$ is in bloom,

$$\begin{aligned}
\mathrm{vol}_{\le n}\big(\mathbb{T},\underline{\mathcal{W}}\big) \;&=\; \sum_{j=1}^{n} \sum_{\chi:\mathcal{H}\twoheadrightarrow\mu_{p^j}} \mathcal{W}_{\mathrm{Ind}(\chi)} \times \begin{cases} p^{\max\{0,j-r\}} & \text{if } \chi \text{ is Type(I)} \\ p^{\max\{0,i-r\}} & \text{if } \chi \text{ is Type(II)} \end{cases} \\
&\ge\; \sum_{j=1}^{n} p^j \times p^{\max\{0,j-r\}} \;+\; \sum_{j=1}^{n}\sum_{i=0}^{j-1} \phi(p^i) \times p^{\max\{0,i-r\}}
\end{aligned}$$

and the bottom line sums to the stated expression, after a tedious calculation. □

2.3. **Seeding – parity results on Selmer ranks.** We now explain how to use the work of Coates et al [CFKS10] and Greenberg-Guo [Gre11, Guo93] to establish some sufficient conditions under which the weighting associated to the Selmer group for E/K_∞ produces a tree $\mathbb{T}$ that is in bloom.

Definition 2.8. *For an Artin representation $\rho : G_\infty \to \mathrm{GL}_{\mathcal{O}}(V_\rho)$, one sets*

$$\mathfrak{s}_{E,\rho} \ := \ \textit{multiplicity of } V_\rho \otimes_{\mathcal{O}} \overline{\mathbb{Q}}_p \textit{ inside } \mathcal{X}_E(K_n) \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$$

where K_n denotes the field extension ρ factors through.

The Selmer weighting $\underline{\mathfrak{s}_E}$ associated to the tree $\mathbb{T}_{G_\infty}$ is then constructed so that the ρ-th component is assigned the value $\mathfrak{s}_{E,\rho}$ at each representation $\rho \in \mathcal{V}$.

Theorem 2.9. *Under the three conditions:*

(P1) *only finitely many primes ramify in K_∞/k*

(P2) *all representations $\rho \in \mathcal{V}$ of length ≥ 1 are orthogonal*

(P3) *$\mathfrak{s}_{E,\rho}$ is an* **odd** *number for all $\rho \in \mathcal{V}$ of length one,*

the pair $\big(\mathbb{T}_{G_\infty}, \underline{\mathfrak{s}_E}\big)$ is automatically in bloom.

Proof. One simply needs to check if $\big(\mathrm{Ind}(\chi), \mathrm{Ind}(\chi^p)\big) \in \mathcal{E}$ with $\chi^p \neq \mathbf{1}$, then

$$\mathfrak{s}_{E,\mathrm{Ind}(\chi)} \equiv \mathfrak{s}_{E,\mathrm{Ind}(\chi^p)} \mod 2.$$

Since $\rho = \mathrm{Ind}(\chi)$ is orthogonal and irreducible, it must automatically be self-dual; by Greenberg [Gre11, Prop 11.8] one has

$$\mathfrak{s}_{E,\rho} \ \equiv \ \mathrm{rank}_{\mathcal{O}}\Big(Y\big(\mathrm{tw}_\rho(E)/k^{\mathrm{cy}}\big)\Big) \mod 2$$

where $Y\big(\mathrm{tw}_\rho(E)/k^{\mathrm{cy}}\big) = \frac{X(\mathrm{tw}_\rho(E)/k^{\mathrm{cy}})}{X(\mathrm{tw}_\rho(E)/k^{\mathrm{cy}})[p^\infty]}$.

The $\mathcal{O}$-rank of the module occurring in the right-hand side of the congruence can be identified with the cyclotomic λ-invariant of $Y(\mathrm{tw}_\rho(E)/k^{\mathrm{cy}})$, which we shall label as $\lambda_\rho(E)$. Moreover the main result of [DL15b, Theorem 1] implies that

$$\lambda_\rho(E) \ = \ \sum_i n_i(\rho) \times \lambda_{\rho_i}(E)$$

where $\Psi_p \circ \mathrm{Tr}(\rho) = \sum_i n_i(\rho)\mathrm{Tr}(\rho_i)$ under the action the p-th Adams operator Ψ_p. However if $\mathrm{Stab}_\Gamma(\chi) = \Gamma^{p^n}$ and $\mathrm{Stab}_\Gamma(\chi^p) = \Gamma^{p^m}$, then

$$\sum_i n_i(\rho)\mathrm{Tr}(\rho_i) \ = \ \sum_{\psi : \Gamma^{p^m}/\Gamma^{p^n} \to \mathbb{C}^\times} \mathrm{Tr}\big(\psi \otimes \mathrm{Ind}(\chi^p)\big)$$

in which case

$$\lambda_\rho(E) \ = \ \sum_\psi \lambda_{\psi \otimes \mathrm{Ind}(\chi^p)}(E) \ = \ p^{n-m} \times \lambda_{\mathrm{Ind}(\chi^p)}(E)$$

(here we have used the fact that $\mathrm{char}_{\mathcal{O}[\![\Gamma^{p^m}]\!]}(M)$ and $\mathrm{char}_{\mathcal{O}[\![\Gamma^{p^m}]\!]}(M \otimes \psi)$ share the same number of zeroes on the open p-adic unit disk).

Because p^{n-m} is odd, one immediately deduces that

$$\mathfrak{s}_{E,\rho} \ \equiv \ \lambda_\rho(E) \ \equiv \ \lambda_{\mathrm{Ind}(\chi^p)}(E) \mod 2$$

and exploiting [Gre11, Prop 11.8] again, if $\widetilde{\rho} = \mathrm{Ind}(\chi^p)$ then

$$\lambda_{\mathrm{Ind}(\chi^p)}(E) \ = \ \mathrm{rank}_{\mathcal{O}}\Big(Y\big(\mathrm{tw}_{\widetilde{\rho}}(E)/k^{\mathrm{cy}}\big)\Big) \equiv \ \mathfrak{s}_{E,\widetilde{\rho}} \mod 2.$$

We have therefore shown $\mathfrak{s}_{E,\rho} \equiv \mathfrak{s}_{E,\widetilde{\rho}} \mod 2$, as required. □

To be in a position to apply the previous theorem, we are required to determine whether or not the parity of $\mathfrak{s}_{E,\rho}$ is odd at every single vertex $\rho \in \mathcal{V}$ of length one. The following result is a consequence of the Dokchitsers' fundamental work on the p-parity conjecture for abelian varieties over number fields, and provides us with a useful means to check when it is appropriate to apply Theorem 2.9.

Assume $k/\mathbb{Q}$ is a Galois extension, and the elliptic curve E is defined over $\mathbb{Q}$. We shall write $\rho_{\mathbb{Q}} = \mathrm{Ind}_k^{\mathbb{Q}}(\rho)$ for the representation over the rationals induced by ρ.

Proposition 2.10. *If ρ is orthogonal, $\rho_{\mathbb{Q}}$ is both irreducible and even dimensional, E has no wild ramification and the p-parity conjecture for E over k holds, then*

$$(-1)^{\mathfrak{s}_{E,\rho}} = (-1)^{\dim(\rho_{\mathbb{Q}}^-)} \times \prod_{q \in \mathcal{M}_E^{\mathrm{sm}}} (-1)^{\dim(\rho_{\mathbb{Q}}^{I_q})} \times \prod_{q \in \mathcal{M}_E^{\mathrm{sm}} \cup \mathcal{M}_E^{\mathrm{ns}}} \det\big(\mathrm{Frob}_q \big| \mathrm{Ind}_k^{\mathbb{Q}}(V_\rho)^{I_q}\big),$$

where I_q is the inertia subgroup at q, $\mathcal{M}_E^{\mathrm{sm}}$ denotes the set of split multiplicative primes for $E_{/\mathbb{Q}}$, and $\mathcal{M}_E^{\mathrm{ns}}$ denotes the set of non-split multiplicative primes.

Proof. Consider first the sign in the functional equation for $h^1(E)$ twisted by $\rho_{\mathbb{Q}}$, which we shall label as $w_{E,\rho_{\mathbb{Q}}}$ say. The main result in [Dok05] states that

$$\begin{aligned} w_{E,\rho_{\mathbb{Q}}} = w_E^{\dim(\rho_{\mathbb{Q}})} \times (-1)^{\dim(\rho_{\mathbb{Q}}^-)} \times \prod_{q \in \mathcal{M}_E^{\mathrm{sm}} \cup \mathcal{M}_E^{\mathrm{ns}}} \det\big(\mathrm{Frob}_q \big| \mathrm{Ind}_k^{\mathbb{Q}}(V_\rho)^{I_q}\big) \\ \times \prod_{q \in \mathcal{M}_E^{\mathrm{sm}}} (-1)^{\dim(\rho_{\mathbb{Q}}^{I_q})} \times \prod_{q \in \mathcal{M}_E^{\mathrm{add}}} \det\big(\mathrm{Frob}_q \big| \mathrm{Ind}_k^{\mathbb{Q}}(V_\rho)^{I_q}\big)^{\mathrm{ord}_p(N_E)} \end{aligned}$$

with $\mathcal{M}_E^{\mathrm{add}}$ indicating the set of primes of bad additive reduction for E over $\mathbb{Q}$. Since E has no wild ramification thus $\mathrm{ord}_p(N_E)$ is even, whilst $\dim(\rho_{\mathbb{Q}})$ is also even – the first and last terms on the right-hand side can therefore be omitted.

Now by assumption the p-parity conjecture holds for E over k, and also for all the quadratic extensions of k contained in K_∞ (in fact, there are none as K_∞ has odd profinite degree); thus applying [DD09, Theorem 4.5],

$$w_{E,\rho_{\mathbb{Q}}} = (-1)^{\mathfrak{s}_{E,\rho_{\mathbb{Q}}}} = (-1)^{\mathfrak{s}_{E,\rho}}.$$

Note the last equality follows as the ρ's and $\rho_{\mathbb{Q}}$'s are in one-to-one correspondence, which can be seen from the irreducibility of the latter as $\mathrm{Gal}(K_\infty/\mathbb{Q})$-modules. □

2.4. **Grafting – the Darmon-Tian method.** The principal advantage of the result in the last section is that it requires relatively few hypotheses in order to obtain positive growth in the Selmer corank for E over the fields K_n as $n \to \infty$. However a considerable disadvantage is it can only be applied where one expects the generic rank to be odd, i.e. the pair $\big(\mathbb{T}_{G_\infty}, \underline{\mathfrak{s}_E}\big)$ might already be in bloom with respect to a uniformly even weighting $\underline{\mathfrak{s}_E}$, yet the theorem only sees "0 mod 2".

Here we present an alternative method to establish when $\mathbb{T}$ is in bloom that is heavily based on the two-dimensional case studied in [DT10]. Since we will require modularity, henceforth we shall assume that the elliptic curve E is defined over $\mathbb{Q}$.

Definition 2.11. *For an Artin representation $\rho : G_\infty \to \mathrm{GL}_{\mathcal{O}}(V_\rho)$, one defines*

$$\mathfrak{d}_{E,\rho} := \textit{multiplicity of } V_\rho \otimes_{\mathcal{O}} \mathbb{C} \textit{ inside } E(K_n) \otimes \mathbb{C}$$

where again K_n denotes the field extension ρ factors through.

The associated Mordell-Weil weighting on $\mathbb{T}_{G_\infty}$ is then given by $\underline{\mathfrak{d}_E} = \{\mathfrak{d}_{E,\rho}\}_{\rho\in\mathcal{V}}$.

Remark: Given a tree $\mathbb{T}_{G_\infty}$ associated to our group G_∞, one can always decompose the tree into a disjoint union of branches $\mathcal{B}_j$ indexed by the vertices of length one from the root vertex ρ_0. In this way, it makes sense to speak of both:

(i) The weighting $\underline{\mathfrak{d}_E}$ restricted to a given branch $\mathcal{B}_j$;

(ii) The volume $\mathrm{vol}_{\leq n}(\mathcal{B}_j, \underline{\mathfrak{d}_E})$ along each branch $\mathcal{B}_j$.

Indeed if the graph structure of every branch is isomorphic to a single $\mathcal{B}'$ say, and if the weighting $\underline{\mathfrak{d}_E}$ is distributed identically amongst the branches, then clearly

$$\mathrm{vol}_{\leq n}(\mathbb{T}_{G_\infty}, \underline{\mathfrak{d}_E}) \;=\; \sum_{\text{all } j} \mathrm{vol}_{\leq n}(\mathcal{B}_j, \underline{\mathfrak{d}_E}) \;=\; \vartheta \times \mathrm{vol}_{\leq n}(\mathcal{B}', \underline{\mathfrak{d}_E})$$

where $\vartheta = \#\{\rho \in \mathcal{V} \;\big|\; \mathrm{length}(\rho) = 1\}$.

Suppose there is an edge $(\rho, \widetilde{\rho}) \in \mathcal{E}$ where $\rho = \mathrm{Ind}(\chi)$, $\widetilde{\rho} = \mathrm{Ind}(\chi^p)$ with $\chi \neq \mathbf{1}$. One can form the fixed field

$$K_{\infty,\rho} \;:=\; K_\infty^{\mathrm{Ker}(\rho)}$$

and if $\chi : \mathcal{H} \twoheadrightarrow \mu_{p^j}$ with $\mathrm{Stab}_\Gamma(\chi) = \Gamma^{p^n}$, the fixed field satisfies $[K_{\infty,\rho} : k_n] = p^j$ where $k_n = \big(k^{\mathrm{cy}}\big)^{\Gamma^{p^n}}$ for $n \geq 0$. Repeating the above using $\widetilde{\rho}$ instead, we find that

$$K'_{\infty,\widetilde{\rho}} \;:=\; K_\infty^{\mathrm{Ker}(\widetilde{\rho})} \cdot k_n$$

is a degree p^{j-1} extension of k_n, in fact $K_{\infty,\rho}/K'_{\infty,\widetilde{\rho}}$ is a cyclic degree p extension of number fields.

One crucial feature is that, in general, the map sending a vertex $\rho \in \mathcal{V}$ to the field $K_{\infty,\rho}$ need not be injective, i.e. there could well be multiple non-isomorphic representations of G_∞ which yield the same fixed field. This means it becomes difficult to distinguish whether a jump in the Mordell-Weil rank has arisen at the vertex ρ, or at another non-isomorphic vertex $\rho^\dagger$ sharing the same fixed field as ρ.

Let us now impose six hypotheses necessary for the Heegner point machinery:

(DT1) The representation $\sigma_{E,p} : \mathrm{Gal}\big(\mathbb{Q}(E_p)/\mathbb{Q}\big) \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective;

(DT2) The p-primary Selmer group for E over k^{cy} is trivial;

(DT3) Each k_n is a CM-field, and there exists a Hilbert modular form $\mathbf{f}_n$ over the totally real subfield $k_n^+ = k_n \cap \mathbb{R}$ such that $L(\mathbf{f}_n, s) = L(E/k_n^+, s)$;

(DT4) At the prime $\mathfrak{p}_n$ of k_n^+ lying over p one has $a_{\mathfrak{p}_n}(E) \not\equiv 0, 1 \pmod{\mathfrak{p}_n}$, and if a good prime $\nu \neq \mathfrak{p}_n$ ramifies in K_∞/k_n^+ then $a_\nu(E) \not\equiv 1 \pmod{\mathfrak{p}_n}$;

(DT5) The conductor $\mathfrak{n}_E$ of E over $k^+ = k \cap \mathbb{R}$ remains inert inside $\bigcup_{n\geq 0} k_n^+$, and is relatively prime to $\mathrm{disc}(k/k^+)$;

(DT6) If Σ' consists of the infinite places of k^+ and the finite places ν satisfying

$$\theta_{k/k^+}(\mathfrak{n}_E)_\nu \;=\; -1$$

where θ_{k/k^+} is the quadratic character associated to the CM extension, then the set Σ' has even cardinality.

Note that the natural generalisation of the last condition to the CM extensions k_n/k_n^+ is propagated by the original **(DT6)** because k^{cy}/k is a pro-p-extension,

and the conductor $\mathfrak{n}_E$ will remain inert as we climb the real subfields k_n^+/k^+ by **(DT5)**. Before introducing a seventh condition, we need to review the work of Zhang [Zha04]. Let Σ'_n denote the set of places of k_n^+ lying over Σ'; in particular Σ'_n must have even cardinality if both **(DT5)** and **(DT6)** hold.

We write $\mathbb{B}'_n$ for the totally definite quaternion algebra over k_n^+ which is ramified precisely at the places of Σ'_n, so $\mathbb{B}'_n$ is uniquely determined up to isomorphism. Fix an embedding $k_n^+ \hookrightarrow \mathbb{B}'_n$ and choose an order $\mathcal{O}_n \subset \mathbb{B}'_n$ which contains $\mathcal{O}_{k_n^+}$ as a subring of relative discriminant $\mathfrak{n}_E = \mathfrak{n}_{\mathbf{f}_n}$. If G'_n denotes the algebraic group representing the functor $R \mapsto (\mathbb{B}'_n \otimes_{k_n^+} R)^\times$ on k_n^+-algebras, one defines

$$\mathbf{X}'_n \;:=\; G'_n(k_n^+)\backslash G'_n(\mathbb{A}_f)/U'_n$$

where U'_n is the compact open subgroup $\big(\mathcal{O}_n \otimes \widehat{\mathbb{Z}}\big)^\times$. Indeed applying the strong approximation theorem $\#\mathbf{X}'_n < \infty$, so we can view the finite set $\mathbf{X}'_n$ as the points on a zero-dimensional Shimura variety associated to (G'_n, U'_n).

Let $\mathbb{H}_{\mathfrak{n}_E}$ denote the Hecke algebra acting on the space of Hilbert modular forms of level $\mathfrak{n}_E$, parallel weight two and trivial nebentypus. There is a non-degenerate bilinear form

$$\big\langle -, - \big\rangle_{\mathbf{X}'_n} : \mathbb{Z}[\mathbf{X}'_n] \times \mathbb{Z}[\mathbf{X}'_n] \longrightarrow \mathbb{Z}$$

and under this pairing the Hecke operators $T_{\mathfrak{m}} \in \mathbb{H}_{\mathfrak{n}_E}$ are self-adjoint with respect to their natural action on the module of functions $\mathbb{Z}[\mathbf{X}'_n]$. By multiplicity one, the $\mathbf{f}_n$-isotypic component of $\mathbb{Z}[\mathbf{X}'_n]$ is a line, and we write ϕ'_n for a generator of it.

Definition 2.12. *The algebraic part of $L(\mathbf{f}_n, 1)$ is given by*

$$\mathbb{L}(\mathbf{f}_n, 1) \;:=\; 2^{-[k_n^+:\mathbb{Q}]-1}\sqrt{\mathrm{Norm}\big(\mathrm{disc}_{k_n/k_n^+}\big)} \times \frac{L(\mathbf{f}_n, 1)}{\big(\mathbf{f}_n, \mathbf{f}_n\big)_{k_n^+}} \times \big\langle \phi'_n, \phi'_n \big\rangle_{\mathbf{X}'_n}$$

where $\big(\mathbf{f}_n, \mathbf{f}_n\big)_{k_n^+}$ is the automorphic period induced from the standard measure $\sum_{i=1}^{[k_n^+:\mathbb{Q}]} \mathrm{d}x_i \wedge \mathrm{d}y_i/y_i^2$ on

$$\mathrm{PGL}_2(k_n^+)\backslash \mathfrak{H}^{[k_n^+:\mathbb{Q}]} \times \mathrm{PGL}_2(\mathbb{A}_f)/U_0(\mathfrak{n}_{\mathbf{f}_n}).$$

The final assumption that we must impose is:

(DT7) The prime p does not divide the algebraic L-value $\mathbb{L}(\mathbf{f}_n, 1)$ for all n.

It should be pointed out that if $k = \mathbb{Q}(\mu_p)$ then **(DT2)** $\Longrightarrow$ **(DT7)** via the results of Skinner and Urban [SU14], so in this special case **(DT7)** is actually redundant.

Theorem 2.13. *Assume* **(DT1)**–**(DT7)** *hold, and that at each edge $(\rho, \widetilde{\rho})$ lying in some subset of tree branches*

$$\bigcup_{j \in J} \mathcal{B}_j \;\subset\; \mathcal{E},$$

there is a single prime of split multiplicative reduction for E ramified in $K_{\infty,\rho}/K'_{\infty,\widetilde{\rho}}$. Then for every $\rho \in \mathcal{V}$ appearing as a vertex in $\cup\mathcal{B}_j$ there exists at least one $\rho^\dagger \in \mathcal{V}$ of the same length, dimension and kernel as ρ, such that

$$\mathfrak{d}_{E,\rho^\dagger} > 0.$$

Furthermore, if the branches $\cup\mathcal{B}_j$ span the entirety of the tree $\mathbb{T}_{G_\infty}$ then the pair $\big(\mathbb{T}_{G_\infty}, \underline{\mathfrak{d}_E}\big)$ must be in bloom, in fact as a $\mathrm{Gal}(K_n/k)$*-module*

$$\bigoplus_{\substack{\rho\,\in\,\mathcal{V},\\ 0\,<\,\mathrm{length}(\rho)\,\leq\,n}} V_{\rho^\dagger}\otimes_{\mathcal{O}}\mathbb{C}\ \subset\ E(K_n)\otimes\mathbb{C} \quad \textit{for all integers } n>0.$$

Proof. Fix any edge $(\rho,\widetilde{\rho})$, and suppose $K_{\infty,\rho}\cap k^{\mathrm{cy}}=k_n$. To make the exposition a lot less cumbersome, we assume that the split multiplicative prime totally ramifies in the full cyclic p^j-extension $K_{\infty,\rho}/k_n$, not just in the subextension $K_{\infty,\rho}/K'_{\infty,\widetilde{\rho}}$. Let us write $\mathfrak{q}$ for the split multiplicative prime of k_n lying below it, and as in [DT10, Lemma 4.1] suppose that $p\nmid \mathrm{ord}_{\mathfrak{q}}(q_E)$ where q_E is the Tate period of the elliptic curve E over $k_{n,\mathfrak{q}}$.

The entire argument hinges on establishing the following two statements:

(A) There exists a surjective group homomorphism

$$\partial_{\mathfrak{q}} : E\big(K_{\infty,\rho}\otimes_{k_n} k_{n,\mathfrak{q}}\big)\longrightarrow \frac{\mathbb{Z}}{p^j\mathbb{Z}}$$

such that $\partial_{\mathfrak{q}}\big(E(K_{\infty,\widetilde{\rho}})+E(K_{\infty,\rho})_{\mathrm{tors}}\big)\subset \frac{p\,\mathbb{Z}}{p^j\mathbb{Z}}$;

(B) There exists a global point $P\in E(K_{\infty,\rho})$ such that $\partial_{\mathfrak{q}}(P)$ has order p^j.

Assuming these statements are true, it follows that the representation W_P generated by the $K_{\infty,\rho}$-rational point P under the action of $G=\mathrm{Gal}(K_{\infty,\rho}/k)$ must contain an irreducible subrepresentation $\rho^\dagger$, which factors through $\mathrm{Gal}(K_{\infty,\rho}/k)$ but not through $\mathrm{Gal}(K_{\infty,\widetilde{\rho}}/k)$, and satisfies

$$\mathrm{Hom}_G\big(V_{\rho^\dagger}, E(K_{\infty,\rho})\big)\neq 0.$$

Both $\rho^\dagger$ and the original ρ share the same kernel, dimension and distance from the root vertex, but need not be isomorphic as G-representations. At the level of $\mathbb{C}[G]$-modules,

$$E(K_{\infty,\widetilde{\rho}})\otimes\mathbb{C}\ \oplus\ V_{\rho^\dagger}\otimes_{\mathcal{O}}\mathbb{C}\ \subset\ E(K_{\infty,\rho})\otimes\mathbb{C}$$

and the rest of the theorem follows inductively along the branches $\cup\mathcal{B}_j$.

Proof of (A). To construct the homomorphism $\partial_{\mathfrak{q}}$ we use the non-archimedean parametrization for Tate curves. Let $\mathcal{Q}$ be the unique place of $K_{\infty,\rho}$ lying over $\mathfrak{q}$, and let $\mathcal{R}$ denote the ring of integers of $\mathcal{L}=(K_{\infty,\rho})_{\mathcal{Q}}$ with finite residue field $\mathfrak{r}$. The Néron model $\mathcal{C}$ for $E/\mathrm{Spec}\,\mathcal{R}$ will have group of connected components

$$\Phi_E:=\frac{(K_{\infty,\rho})_{\mathcal{Q}}^\times}{q_E^{\mathbb{Z}}\,\mathcal{R}^\times}\ \cong\ \frac{\mathbb{Z}}{\mathrm{ord}_{\mathfrak{q}}(q_E)p^j\mathbb{Z}},\quad \text{so that } (\Phi_E)_{p^\infty}=\left(\frac{(K_{\infty,\rho})_{\mathcal{Q}}^\times}{q_E^{\mathbb{Z}}\,\mathcal{R}^\times}\right)_{p^\infty}\cong\ \frac{\mathbb{Z}}{p^j\mathbb{Z}}$$

upon using the condition that $E_{/\mathcal{L}}$ is a Tate curve, and second that $p\nmid\mathrm{ord}_{\mathfrak{q}}(q_E)$. Because the generic fiber $\mathcal{C}\times_{\mathrm{Spec}\,\mathcal{R}}\mathrm{Spec}\,\mathcal{L}$ is isomorphic as a group variety to $E/\mathcal{L}$, one can identify $\mathcal{C}(\mathcal{R})$ with the $\mathcal{L}$-rational points on E; the mapping $\partial_{\mathfrak{q}}$ is then obtained through the compositions

$$\partial_{\mathfrak{q}}: E(\mathcal{L})\xrightarrow{\sim}\mathcal{C}(\mathcal{R})\ \xrightarrow{\mathrm{red}_{\mathfrak{q}}}\ \widetilde{\mathcal{C}}(\mathfrak{r})\ \twoheadrightarrow\ \frac{\widetilde{\mathcal{C}}(\mathfrak{r})}{\widetilde{\mathcal{C}}^0(\mathfrak{r})}\ \xrightarrow{\mathrm{proj}}\ (\Phi_E)_{p^\infty}\cong\frac{\mathbb{Z}}{p^j\mathbb{Z}}$$

where $\widetilde{\mathcal{C}}=\mathcal{C}\times_{\mathrm{Spec}\,\mathcal{R}}\mathrm{Spec}\,\mathfrak{r}$ denotes the special fiber.

It therefore remains to check that $\partial_{\mathfrak{q}}\big(E(K_{\infty,\widetilde{\rho}})+E(K_{\infty,\rho})_{\mathrm{tors}}\big)$ lies in $p\mathbb{Z}/p^j\mathbb{Z}$. Firstly we know that G_∞ has no quotient isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$ as G_∞ is pro-p, so from **(DT1)** one deduces that $E(K_{\infty,\rho})_{p^\infty}$ is trivial, whence $\partial_{\mathfrak{q}}\big(E(K_{\infty,\rho})_{\mathrm{tors}}\big)=0$. On the other hand, because $\mathfrak{q}$ totally ramifies in $K_{\infty,\rho}/k_n$ the group of connected components for E over $K_{\infty,\rho}\otimes_{k_n}k_{n,\mathfrak{q}}$ has order $p^j\times u$, whilst the group of connected components for E over $K_{\infty,\widetilde{\rho}}\otimes_{k_n}k_{n,\mathfrak{q}}$ has order $p^{j-1}\times u$ for some p-adic unit u; consequently $\partial_{\mathfrak{q}}\big(E(K_{\infty,\widetilde{\rho}}\otimes_{k_n}k_{n,\mathfrak{q}})\big)$ has size p^{j-1}, and (A) now follows.

Proof of (B). As the demonstration is a cannibalisation of the method in [DT10, §5 and §6] we briefly outline their argument, taking care to point out any areas of divergence. Let $R'\subset\mathbb{B}'_n$ be an order containing the ring of integers $\mathcal{O}_{k_n}$ as a subring of relative discriminant $\mathfrak{n}_E$, and set $\hat{R}'=R'\otimes\hat{\mathbb{Z}}$. An optimal embedding of $\mathcal{O}_{k_n}$ into the Eichler orders in $\mathbb{B}'_n$ that are locally conjugate to R', consists of a pair

$$(\Psi,\alpha)\ \in\ G'_n(k_n^+)\backslash\big(\mathrm{Hom}(k_n,\mathbb{B}'_n)\times G'_n(\mathbb{A}_f)\big)/U'_n$$

such that $\alpha_\nu^{-1}\Psi(\mathcal{O}_{k_n,\nu})\alpha_\nu\subset R'_\nu$ at all places ν.

The natural action of the finite group $k_n^\times\backslash\hat{k}_n^\times/\hat{\mathcal{O}}_{k_n}^\times$ on the optimal embeddings (Ψ,α) produces finitely many orbits $(\Psi_1,\alpha_1),\dots,(\Psi_{h_n},\alpha_{h_n})$ say, where h_n is the class number. Zhang [Zha04] has associated to $(\mathbf{X}'_n,k_n)$ the canonical element

$$\Delta'_{k_n}\ =\ \sum_{j=1}^{h_n}\big(\#\mathrm{Aut}(\Psi_j,\alpha_j)\big)^{-1}\times\alpha_j\ \in\ \mathbb{Q}[\mathbf{X}'_n]$$

belonging to the dual lattice $\mathbb{Z}[\mathbf{X}'_n]^\vee$, under the non-degenerate pairing $\langle-,-\rangle^2_{\mathbf{X}'_n}$. From [Zha04, Theorem 7.1] there is Zhang's celebrated formula

$$\frac{\big\langle\phi'_n,\Delta'_{k_n}\big\rangle^2_{\mathbf{X}'_n}}{\big\langle\phi'_n,\phi'_n\big\rangle^2_{\mathbf{X}'_n}}\ =\ 2^{-[k_n^+:\mathbb{Q}]-1}\sqrt{\mathrm{Norm}\big(\mathrm{disc}_{k_n/k_n^+}\big)}\times\frac{L(\mathbf{f}_n,1)}{\big(\mathbf{f}_n,\mathbf{f}_n\big)_{k_n^+}}$$

or in a more concise form,

$$\mathbb{L}(\mathbf{f}_n,1)=\ \big\langle\phi'_n,\Delta'_{k_n}\big\rangle^2_{\mathbf{X}'_n}\ \in\ \mathbb{Z}. \tag{2.1}$$

We shall also need imprimitive versions of Δ'_{k_n}. For an ideal $\mathcal{O}_{k_n^+}$-ideal $\mathfrak{c}$ the vector $\Delta'_{k_n,\mathfrak{c}}$ is defined as before, but this time summing instead over an orbit of optimal embeddings of conductor $\mathfrak{c}$ under the action of the group $k_n^\times\backslash\hat{k}_n^\times/(\hat{\mathcal{O}}_{k_n^+}+\mathfrak{c}\cdot\hat{\mathcal{O}}_{k_n})^\times$; in fact $\Delta'_{k_n,\mathfrak{c}}$ differs from Δ'_{k_n} by some simple Hecke operator relations.

Let $\mathfrak{q}_+=\mathfrak{q}\cap\mathcal{O}_{k_n^+}$ and $\Sigma_n=\Sigma'_n-\{\infty,\mathfrak{q}_+\}$, which has even size by **(DT5-6)**. We shall write G_{Σ_n} for the algebraic group over k_n^+ representing $R\mapsto(B\otimes_{k_n^+}R)^\times$ where B is the (definite) quaternion algebra ramified only at the places of $\nu\in\Sigma_n$. Fix an Eichler order $R_n\subset B$ of discriminant prime to $\mathfrak{q}_+$. We consider two Shimura curves over k_n^+, namely X and $X_0(\mathfrak{q}_+)$ of levels $U_n=\hat{R}_n^\times$ and $U_0(\mathfrak{q}_+)$ respectively, with complex points

$$\begin{aligned}X(\mathbb{C})\ &=\ G_{\Sigma_n}(k_n^+)\backslash\mathfrak{H}\times G_{\Sigma_n}(\mathbb{A}_f)/U_n\\ X_0(\mathfrak{q}_+)(\mathbb{C})\ &=\ G_{\Sigma_n}(k_n^+)\backslash\mathfrak{H}\times G_{\Sigma_n}(\mathbb{A}_f)/U_0(\mathfrak{q}_+).\end{aligned}$$

The curve E is k_n^+-isogenous to a quotient of the Jacobian of $X_0(\mathfrak{q}_+)$ (see **(DT3)**) and without loss of generality, assume the modular parametrisation

$$\eta : \mathrm{Jac}\ X_0(\mathfrak{q}_+) \twoheadrightarrow E \qquad \text{is optimal, with connected kernel.}$$

Remark: Let $\mathcal{K}$ be a finite extension of $(k_n^+)_{\mathfrak{q}_+}$. The generic fiber of the nodal model $\mathfrak{X}_0(\mathfrak{q}_+)$ is a $\mathfrak{q}_+$-adic rigid analytic space (actually the union of two wide open spaces), and there is a specialisation map

$$\partial_{\mathcal{K}} \circ \eta : \mathrm{Div}^0\big(\mathfrak{X}_0(\mathfrak{q}_+)\big)(\mathcal{K}) \longrightarrow \Phi_{E,\mathcal{K}}$$

where $\partial_{\mathcal{K}}$ denotes the reduction map from $\mathcal{C}(\mathcal{O}_{\mathcal{K}})$ to the cyclic group $\Phi_{E,\mathcal{K}}$ of connected components in the special fiber of $\mathcal{C}_{/\mathcal{O}_{\mathcal{K}}}$.

We now need arithmetically interesting points to plug into this homomorphism $\partial_{\mathcal{K}}$.

For an ideal $\mathfrak{c} \lhd \mathcal{O}_{k_n^+}$, one writes $H[\mathfrak{c}]$ for the ring class field of k_n of conductor $\mathfrak{c}$. If $g \in \mathrm{Gal}(H[\mathfrak{c}]/k_n)$ then choose a lift $\overline{g} \in \mathrm{Gal}(H[\mathfrak{c}\mathfrak{q}_+]/k_n)$, and pick closed points $z_1, z_2 \in \mathfrak{X}_0(\mathfrak{q}_+)(H[\mathfrak{c}\mathfrak{q}_+])$ satisfying $\pi_i(z_i) = z_0$ where z_0 is a CM point (see [DT10, §6]) of conductor $\mathfrak{c}$, and $\pi_1, \pi_2 : \mathfrak{X}_0(\mathfrak{q}_+) \longrightarrow X$ are the two natural degeneracy maps. Darmon and Tian construct Heegner points

$$\Delta_{\mathfrak{c},\mathfrak{q}} \ := \sum_{g \in \mathrm{Gal}(H[\mathfrak{c}]/k_n)} \big(z_1 - z_2\big)^{\overline{g}} \in \ \mathrm{Div}^0\big(\mathfrak{X}_0(\mathfrak{q})\big)(H[\mathfrak{c}\mathfrak{q}_+])$$

and if $\mathcal{K} = H[\mathfrak{c}\mathfrak{q}_+] \otimes_{k_n} k_{n,\mathfrak{q}}$, then $\partial_{\mathcal{K}} \circ \eta\big(\Delta_{\mathfrak{c},\mathfrak{q}}\big)$ will be independent of these choices.

Recall the field extension $K_{\infty,\rho}/k_n$ is ramified at the multiplicative prime $\mathfrak{q}$, therefore $K_{\infty,\rho} \subset H[\mathfrak{p}_n^t\mathfrak{m}\mathfrak{q}_+]$ for some square-free $\mathcal{O}_{k_n^+}$-ideal $\mathfrak{m}$ coprime to $\mathfrak{p}_n\mathfrak{q}_+$ and positive integer t (note that p is the only prime which can wildly ramify in the p-adic Lie extension K_∞/k). Henceforth set $\mathfrak{c} := \mathfrak{p}_n^t\mathfrak{m}$ and $\mathcal{K} := H[\mathfrak{p}_n^t\mathfrak{m}\mathfrak{q}_+] \otimes_{k_n} k_{n,\mathfrak{q}}$, so that

$$\partial_{\mathfrak{c},\mathfrak{q}_+} = \partial_{\mathcal{K}} : E\Big(H[\mathfrak{c}\mathfrak{q}_+] \otimes_{k_n} k_{n,\mathfrak{q}}\Big) \longrightarrow \frac{\mathbb{Z}}{d_{\mathfrak{c}}\mathbb{Z}}$$

denotes the reduction map to the group of connected components $\Phi_{E,\mathcal{K}} \cong \mathbb{Z}/d_{\mathfrak{c}}\mathbb{Z}$. It is shown in [DT10, Proof of Thm 6.1] that

$$\partial_{\mathfrak{c},\mathfrak{q}_+} \circ \eta\big(\Delta_{\mathfrak{c},\mathfrak{q}}\big) \ = \ (d_{\mathfrak{c}} - 2) \times \big\langle \phi_n', \Delta_{k_n,\mathfrak{c}}' \big\rangle_{\mathbf{X}_n'}$$

for the imprimitive vectors $\Delta_{k_n,\mathfrak{c}}'$, and squaring both sides

$$\partial_{\mathfrak{c},\mathfrak{q}_+} \circ \eta\big(\Delta_{\mathfrak{c},\mathfrak{q}}\big)^2 \equiv \ 4 \times \big\langle \phi_n', \Delta_{k_n,\mathfrak{c}}' \big\rangle_{\mathbf{X}_n'}^2 \mod d_{\mathfrak{c}}. \tag{2.2}$$

Remark: We now explain how to descend from $H[\mathfrak{p}_n^t\mathfrak{m}\mathfrak{q}_+]$ back down to $K_{\infty,\rho}$. Since $\mathfrak{q}$ must split completely in $H[\mathfrak{p}_n^t\mathfrak{m}]/k_n$ and is totally ramified in $K_{\infty,\rho}/k_n$, one can choose the above lifts $\overline{g} \in \mathrm{Gal}\left(H[\mathfrak{p}_n^t\mathfrak{m}\mathfrak{q}_+]/K_{\infty,\rho}\right)$ so that

$$\eta\big(\Delta_{K_{\infty,\rho}}\big) \ = \ \mathrm{Norm}_{H[\mathfrak{p}_n^t\mathfrak{m}\mathfrak{q}_+]\big/K_{\infty,\rho}\cdot H[\mathfrak{p}_n^t\mathfrak{m}]} \circ \eta\big(\Delta_{\mathfrak{c},\mathfrak{q}}\big)$$

where $\Delta_{K_{\infty,\rho}} := \sum_{g \in \mathrm{Gal}(H[\mathfrak{c}\mathfrak{q}_+]/K_{\infty,\rho})} \big(z_1 - z_2\big)^g$ belongs to $\mathrm{Div}^0\big(\mathfrak{X}_0(\mathfrak{q})\big)(K_{\infty,\rho})$.

This norm element is compatible with the natural projection map $\mathbb{Z}/d_{\mathfrak{c}}\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^j\mathbb{Z}$ on connected components [DT10, Thm 6.1], therefore

$$\partial_{\mathfrak{q}} \circ \eta\big(\Delta_{K_{\infty,\rho}}\big) \ \equiv \ \partial_{\mathfrak{c},\mathfrak{q}_+} \circ \eta\big(\Delta_{\mathfrak{c},\mathfrak{q}}\big) \mod p^j. \tag{2.3}$$

Combining Equations (2.2) and (2.3), it directly follows that

$$\partial_{\mathfrak{q}} \circ \eta\big(\Delta_{K_\infty,\rho}\big)^2 \equiv\ 4 \times \big\langle \phi'_n, \Delta'_{k_n,\mathfrak{c}} \big\rangle^2_{\mathbf{X}'_n} \mod p^j. \tag{2.4}$$

We will now need to pass from the imprimitive vector $\Delta'_{k_n,\mathfrak{c}}$ to the primitive Δ'_{k_n}. For every integer $t \geq 2$, there is a recurrence relation

$$\Delta'_{k_n,\mathfrak{p}_n^t} \ = \ \Delta'_{k_n,\mathfrak{p}_n^{t-1}} \big| T_{\mathfrak{p}_n} - p\Delta'_{k_n,\mathfrak{p}_n^{t-2}} \ \equiv \ \Delta'_{k_n,\mathfrak{p}_n^{t-1}} \big| T_{\mathfrak{p}_n} \mod p$$

whilst $\Delta'_{k_n,\mathfrak{p}_n} = \Delta'_{k_n} \big| (T_{\mathfrak{p}_n} - 1)$, and $\Delta'_{k_n,\mathfrak{c}} = \Delta'_{k_n,\mathfrak{p}_n^t} \Big| \prod_{\nu|\mathfrak{m}} (T_\nu - 1)$ since the ideal $\mathfrak{m}$ is square-free (we have written T_ν in place of U_ν at primes dividing the level). Because the Hecke operators are self-adjoint,

$$\begin{aligned} \big\langle \phi'_n, \Delta'_{k_n,\mathfrak{c}} \big\rangle_{\mathbf{X}'_n} \ &\equiv \ \Big\langle \phi'_n \ , \ \Delta'_{k_n} \Big| \prod_{\nu|\mathfrak{m}} (T_\nu - 1) \circ T_{\mathfrak{p}_n^{t-1}} \circ (T_{\mathfrak{p}_n} - 1) \Big\rangle_{\mathbf{X}'_n} \mod p \\ &\equiv \ \Big\langle \phi'_n \Big| \prod_{\nu|\mathfrak{m}} (T_\nu - 1) \circ T_{\mathfrak{p}_n^{t-1}} \circ (T_{\mathfrak{p}_n} - 1) \ , \ \Delta'_{k_n} \Big\rangle_{\mathbf{X}'_n} \mod p. \end{aligned}$$

But ϕ'_n is an eigenvector under the action of the Hecke algebra $\mathbb{H}_{\mathfrak{n}_E}$, thus

$$\phi'_n \ \Big| \ \prod_{\nu|\mathfrak{m}} (T_\nu - 1) \circ T_{\mathfrak{p}_n^{t-1}} \circ (T_{\mathfrak{p}_n} - 1) \ = \ a_{\mathfrak{p}_n}(E)^{t-1} \prod_{\nu|\mathfrak{p}_n\mathfrak{m}} \big(a_\nu(E) - 1\big) \times \phi'_n$$

and furthermore,

$$\big\langle \phi'_n, \Delta'_{k_n,\mathfrak{c}} \big\rangle_{\mathbf{X}'_n} \equiv\ a_{\mathfrak{p}_n}(E)^{t-1} \prod_{\nu|\mathfrak{p}_n\mathfrak{m}} \big(a_\nu(E) - 1\big) \times \big\langle \phi'_n, \Delta'_{k_n} \big\rangle_{\mathbf{X}'_n} \mod p. \tag{2.5}$$

Note that $a_\nu(E) - 1 = -2$ if ν is a non-split multiplicative prime, $a_\nu(E) - 1 = -1$ if ν is a bad additive prime, while $a_\nu(E) - 1 \not\equiv 0 \mod p$ if ν is a good prime by our assumption **(DT4)**; also $a_{\mathfrak{p}_n}(E)^{t-1}\big(a_{\mathfrak{p}_n}(E) - 1\big) \not\equiv 0 \mod p$ by **(DT4)** again. It follows directly that $a_{\mathfrak{p}_n}(E)^{t-1}\prod_{\nu|\mathfrak{p}_n\mathfrak{m}} \big(a_\nu(E) - 1\big)$ must be a p-adic unit.

The argument is almost complete – combining Equations (2.4) and (2.5) together with Zhang's formula (2.1):

$$\partial_{\mathfrak{q}} \circ \eta\big(\Delta_{K_\infty,\rho}\big)^2 \equiv\ (p\text{-adic unit}) \times \mathbb{L}(\mathbf{f}_n, 1) \mod p. \tag{2.6}$$

We now have our global point $P = \eta\big(\Delta_{K_\infty,\rho}\big) \in E(K_\infty,\rho)$, it remains to show that it has order p^j after hitting it with $\partial_{\mathfrak{q}}$. Under condition **(DT7)** the critical value

$$\mathbb{L}(\mathbf{f}_n, 1) = \ 2^{-[k_n^+:\mathbb{Q}]-1} \sqrt{\mathrm{Norm}\big(\mathrm{disc}_{k_n/k_n^+}\big)} \times \frac{L(\mathbf{f}_n, 1)}{\big(\mathbf{f}_n, \mathbf{f}_n\big)_{k_n^+}} \times \big\langle \phi'_n, \phi'_n \big\rangle_{\mathbf{X}'_n} \ \in \ \mathbb{Z} \cap \mathbb{Z}_p^\times,$$

hence the right-hand side of the congruence (2.6) is a p-adic unit; as a consequence $\partial_{\mathfrak{q}}(P)$ is a generator for $(\Phi_E)_{p^\infty} \cong \mathbb{Z}/p^j\mathbb{Z}$, and statement (B) is proved. □

2.5. **Three worked examples.** We should begin with some general comments. Suppose there exists a field $k' \subset k$ such that k/k' is a normal extension, and every vertex $\rho \in \mathcal{V}$ of dimension > 1 exhibits the property that $\mathrm{Ind}_k^{k'}(\rho)$ is irreducible. Assume the elliptic curve E is defined over $\mathbb{Q}$, and that as $\mathrm{Gal}(K_n/k)$-modules

$$\bigoplus_{\rho \in J_n} \big(V_\rho \otimes_{\mathcal{O}} \mathbb{C}\big)^{\oplus e_\rho} \ \subset \ E(K_n) \otimes \mathbb{C}$$

where the sum is over a subset J_n of ρ's of dimension >1. As E is defined over k' it follows that $\bigoplus_{\rho\in J_n}\big(\mathrm{Ind}_k^{k'}(V_\rho)\otimes_{\mathcal{O}}\mathbb{C}\big)^{\oplus e_\rho}$ is contained inside $E(K_n)\otimes\mathbb{C}$, hence

$$\mathrm{rank}_{\mathbb{Z}}E(K_n)\ \geq\ \sum_{\rho\in J_n} e_\rho\times\dim\big(\mathrm{Ind}_k^{k'}(V_\rho)\big).$$

In particular, if the pair $\big(\mathbb{T}_{G_\infty},\underline{\mathfrak{d}_E}\big)$ is in bloom then

$$\mathrm{rank}_{\mathbb{Z}}E(K_n)\ \geq\ \mathrm{vol}_{\leq n}^{(k/k')}\big(\mathbb{T}_{G_\infty},\underline{\mathfrak{d}_E}\big)$$

and the right-hand side is calculated using Theorem 2.7 and Lemma 2.5 in tandem. (The same is true on replacing $\underline{\mathfrak{d}_E}$ by $\underline{\mathfrak{s}_E}$, and $\mathrm{rank}_{\mathbb{Z}}E(K_n)$ by $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_p(E/K_n)$.)

Example A. Let $k'=\mathbb{Q}(\sqrt{-D})$, and we denote by k'_∞ the full $\mathbb{Z}_p^2$-extension of k'. It follows that $\mathrm{Gal}(k'_\infty/k')\cong\Gamma\times\mathcal{H}_1$ where $\mathcal{H}_1$ denotes the Galois group for the anticyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\sqrt{-D})$, so $\mathcal{H}_1=\overline{\langle h_1\rangle}$ is procyclic of $\mathbb{Z}_p$-rank one. If $k=k'(\mu_p)$ and $K_\infty=k'_\infty\big(\mu_p,q^{1/p^\infty}\big)$ for an odd prime q, then

$$G_\infty:=\mathrm{Gal}(K_\infty/k)\ \cong\ \Gamma\ltimes\big(\mathcal{H}_1\times\mathcal{H}_2\big)\ \cong\ \big(\Gamma\times\mathcal{H}_1\big)\ltimes\mathcal{H}_2$$

where h_1 acts trivially on $\mathcal{H}_2=\overline{\langle h_2\rangle}$, while γ acts on h_2 via multiplication by $1+p$ (we are therefore in Case (5) of Theorem 2.1 with $s=d=0$ and $r=1$).

Let E be a semistable elliptic curve over $\mathbb{Q}$ with conductor $N_E=q\times M_E$, where q is a prime of split multiplicative reduction, and M_E is a square-free integer coprime to q. We assume q generates $(\mathbb{Z}/p^2\mathbb{Z})^\times$ which implies q is inert in $\mathbb{Q}(\mu_{p^\infty})$, and further suppose that q is inert in k too. One also requires that E has non-split multiplicative reduction at every place of k lying over M_E.

If **(DT2)** holds and $\mathcal{X}_E(K_\infty)\in\mathfrak{M}_{\mathcal{H}}(G_\infty)$, then by Proposition 2.3 one has

$$\tau_{E,G_\infty}\ =\ 0\ +\ 1\ +\ 2\times 0\ =\ 1,$$

and so Theorem 2.2 implies

$$\mathrm{rank}_{\mathbb{Z}}\,E(K_n)\ \leq\ p^{2n}+4\quad\text{for } n\gg 0.$$

Note **(DT3)** is certainly true as $k/\mathbb{Q}$ is a solvable extension, and k is a CM field; we also assume that the primes dividing M_E are inert in k, which implies **(DT5)**. Since E has no complex multiplication thus **(DT1)** holds for almost all primes p. Moreover **(DT6)** holds provided the number of primes ν of k^+ dividing $p\times\mathrm{disc}_{k/k^+}$ with $\theta_{k/k^+}(\mathfrak{n}_E)_\nu=-1$ is *even*, as the number of archimedean places is even.

Finally most good ordinary primes p satisfy $a_p(E)\not\equiv 0,1\ (\mathrm{mod}\ p)$ to get **(DT4)**, and we will assume **(DT2)** $\Longrightarrow$ **(DT7)** in order to obtain **(DT7)** as a condition.

Proposition 2.14. *Under the above hypotheses, for $n\gg 0$ there are bounds*

$$p^{2n}\times\frac{p(p^2+p+1)}{(p+1)^3}\ \ \leq\ \ \mathrm{rank}_{\mathbb{Z}}\,E(K_n)\ \ \leq\ \ p^{2n}+4.$$

Proof. We have already obtained the upper bound, so we focus on the lower bound. Applying Theorem 2.13 we see that the pair $\big(\mathbb{T}_{G_\infty},\underline{\mathfrak{d}_E}\big)$ is only partially in bloom, corresponding to $\rho\in\mathcal{V}$ that 'see' the ramification of the prime above q in the subquotient $k^{\mathrm{cy}}\big(q^{1/p^\infty}\big)/k^{\mathrm{cy}}$. A quick calculation by hand shows the proportion

of ρ's for which a prime above q ramifies in $K_{\infty,\rho}/K'_{\infty,\widetilde{\rho}}$ equals $\frac{p^n}{p^n+p^{n-1}} = \frac{p}{p+1}$, therefore one concludes

$$\operatorname{rank}_{\mathbb{Z}} E(K_n) \;\geq\; \frac{p}{p+1} \times \operatorname{vol}_{\leq n}^{(k/k')}\big(\mathbb{T}_{G_\infty}, \underline{\mathfrak{d}_E}\big) \;\geq\; \frac{p(p-1)}{p+1} \times \operatorname{vol}_{\leq n}\big(\mathbb{T}_{G_\infty}, \underline{\mathfrak{d}_E}\big)$$

where the last inequality follows from Lemma 2.5(i) and the fact $[k : k'] = p - 1$. Plugging in our explicit formula from Theorem 2.7(d) and tidying up the result, the required lower bound is established. □

It seems somewhat disappointing that the upper and lower bounds are not equal, even though for large primes p the factor $\frac{p(p^2+p+1)}{(p+1)^3}$ becomes very close to one. We now describe a situation where the upper and lower bounds really do coincide, thereby yielding an equality for the Mordell-Weil rank over K_n.

Example B. Let E be a semistable elliptic curve over $\mathbb{Q}$, and $l_1, \ldots, l_{d-1}$ primes of non-split multiplicative reduction for E. We choose $k = \mathbb{Q}(\mu_p)$, $k' = \mathbb{Q}$ and set

$$K_\infty := \mathbb{Q}\Big(\mu_{p^\infty}, l_1^{1/p^\infty}, \ldots, l_{d-1}^{1/p^\infty}\Big).$$

Then $G_\infty := \operatorname{Gal}(K_\infty/k) \cong \Gamma \ltimes \mathbb{Z}_p^{d-1}$, corresponding to part (b) of Theorem 2.7. We shall also assume $l_1, \ldots, l_{d-1}$ are quadratic residues modulo p, and that

$$(-1)^{(p-1)/2} \times \prod_{q \mid M_E} \left(\frac{q}{p}\right) \;=\; -1 \tag{2.7}$$

where $N_E = l_1 \times \cdots \times l_{d-1} \times M_E$.

Proposition 2.15. *If $\mathcal{X}_E(K_\infty)$ belongs to $\mathfrak{M}_{\mathcal{H}}(G_\infty)$, then*

$$\operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_p(E/K_n) \;\geq\; p^{(d-1)n} - 1.$$

Proof. Firstly hypotheses **(P1)** and **(P2)** of Theorem 2.9 certainly hold true here. Also, if ρ is of the form $\operatorname{Ind}_k^{\mathbb{Q}}(\chi)$ where the character $\chi : \operatorname{Gal}\big(k(m^{1/p})/k\big) \twoheadrightarrow \mu_p$ for some p-power free m supported on $l_1 \times \cdots \times l_{d-1}$, then Proposition 2.10 informs us

$$(-1)^{\mathfrak{s}_{E,\rho}} = \; (-1)^{(p-1)/2} \times \prod_{q \mid (N_E \times m^{-1})} \left(\frac{q}{p}\right).$$

Under our residue assumptions on $l_1, \ldots, l_{d-1}$ and by Equation (2.7), the right-hand side equals -1 hence the multiplicity $\mathfrak{s}_{E,\rho}$ is always odd, and **(P3)** holds.

Applying Theorem 2.9, we deduce that the pair $\big(\mathbb{T}_{G_\infty}, \underline{\mathfrak{s}_E}\big)$ must be in full bloom; as a direct consequence

$$\operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_p(E/K_n) \;\geq\; \operatorname{vol}_{\leq n}^{(k/\mathbb{Q})}\big(\mathbb{T}, \underline{\mathfrak{s}_E}\big) \;\overset{\text{by 2.5(ii)}}{=}\; (p-1) \times \operatorname{vol}_{\leq n}\big(\mathbb{T}, \underline{\mathfrak{s}_E}\big).$$

However the right-hand volume equals $\frac{p^{(d-1)n}-1}{p-1}$ from Theorem 2.7(b). □

Corollary 2.16. *If $d = 3$, the cyclotomic λ-invariant of $\mathcal{X}_E(\mathbb{Q}(\mu_{p^\infty}))$ equals one, and the p-primary part of $Ш(E/K_n)$ is finite at each layer K_n, then for all $n \geq 1$:*

$$\operatorname{rank}_{\mathbb{Z}} E(K_n) \;=\; p^{2n} - 1 \;\text{ or }\; p^{2n}.$$

Proof. By Proposition 2.3 again, one has

$$\tau_{E,G_\infty} \,=\, 1 \,+\, 0 \,+\, 2\times 0 \,=\, 1,$$

hence Theorem 2.2 implies $\mathrm{rank}_{\mathbb{Z}}\, E(K_n) \leq p^{2n}+4$. Our assumption on $Ш(E/K_n)$ means we can interchange the Selmer corank with the Mordell-Weil rank over K_n, and from the previous proposition we have $\mathrm{rank}_{\mathbb{Z}} E(K_n) \,\geq\, p^{2n}-1$; therefore

$$p^{2n}-1 \,\leq\, \mathrm{rank}_{\mathbb{Z}} E(K_n) \,\leq\, p^{2n}+4.$$

Now $E(K_n)$ contains at most a single one-dimensional representation (character) because the λ-invariant of $\mathcal{X}_E(\mathbb{Q}(\mu_{p^\infty}))$ equals one; further, it cannot contain two copies of a particular $\rho \in \mathcal{V}$ of length one otherwise **(P3)** would then be violated. Thus the rank of $E(K_n)$ is either p^{2n} or $p^{2n}-1$, depending on whether the zero in the power series $\mathrm{char}_{\mathbb{Z}_p[\![\Gamma]\!]}\big(\mathcal{X}_E\big(\mathbb{Q}(\mu_{p^\infty})\big)\big)$ is of the form $e^{2\pi i j/p^n}-1$, where $i=\sqrt{-1}$ and j is an integer. □

Example C. Let E denote a semistable elliptic curve defined over $\mathbb{Q}$ of conductor $N_E = q\times l \times M_E$, such that E has split multiplicative reduction at the prime q, and non-split multiplicative reduction at the prime l. Put $k=\mathbb{Q}(\mu_{p^s})$, $k'=\mathbb{Q}$ and

$$K_\infty \,:=\, \mathbb{Q}\big(\mu_{p^\infty}, q^{1/p^\infty}, l^{1/p^\infty}\big).$$

Here $\mathrm{Gal}(K_\infty/k) \cong \Gamma \ltimes \mathbb{Z}_p^2$, corresponding to case (3) of Theorem 2.1 with $s\in\mathbb{N}$.

The hypothesis **(DT3)** is automatically true, and **(DT4)** holds precisely when $a_p(E) \not\equiv 0,1 \pmod p$. Likewise **(DT5)** is OK provided the primes dividing N_E are primitive roots modulo p^2. However **(DT6)** requires that

- $\omega_p(N_E)^{(p-1)/2} = +1$ if $p \equiv 1 \mod 4$, and
- $\omega_p(N_E)^{(p-1)/2} = -1$ if $p \equiv 3 \mod 4$

where ω_p is the Teichmüller character, as there are $\frac{(p-1)p^{s-1}}{2}$ infinite places in k.

Proposition 2.17. *If* **(DT1)**–**(DT7)** *hold for* $K_\infty = \mathbb{Q}\big(\mu_{p^\infty}, q^{1/p^\infty}, l^{1/p^\infty}\big)$, *then*

$$\big(p^{2n-s+1}+p^s-p-1\big)\times\frac{p}{p+1} \;\;<\;\; \mathrm{rank}_{\mathbb{Z}}\, E(K_n) \;\;\leq\;\; p^{2n}+4.$$

Proof. Here $\tau_{E,G_\infty} = 0+1+2\times 0 \,=\, 1$, so the upper bound again follows readily from Theorem 2.2. To get the lower bound, a simple calculation reveals that the number of extensions $\mathbb{Q}\big(\mu_{p^n}, (q^i l^k)^{1/p^j}\big)/\mathbb{Q}(\mu_{p^n})$ with $1\leq j\leq n$, in which the prime above q totally ramifies, equals $\frac{p^{n+1}-1}{p-1}$. However the total number of these types of extension $\mathbb{Q}\big(\mu_{p^n}, (q^i l^k)^{1/p^j}\big)/\mathbb{Q}(\mu_{p^n})$ equals $(p+1)\times\frac{p^n-1}{p-1}$, yielding the ratio

$$\frac{\frac{p^{n+1}-1}{p-1}}{(p+1)\times\frac{p^n-1}{p-1}} \;\;=\;\; \frac{p^{n+1}-1}{p^{n+1}+p^n-p-1} \;\;>\;\; \frac{p}{p+1} \quad \text{for all } n\geq 0.$$

Consequently Theorem 2.13 tells us that a portion of $\frac{p}{p+1}$-ths of the pair $\big(\mathbb{T}_{G_\infty}, \underline{\mathfrak{d}_E}\big)$ at least is in bloom, meaning that

$$\mathrm{rank}_{\mathbb{Z}}\, E(K_n) \;>\; \frac{p}{p+1}\times \mathrm{vol}_{\leq n}^{(k/k')}\big(\mathbb{T}_{G_\infty}, \underline{\mathfrak{d}_E}\big) \overset{\text{by 2.5(ii)}}{=} \frac{p(p-1)}{p+1}\times \mathrm{vol}_{\leq n}\big(\mathbb{T}_{G_\infty}, \underline{\mathfrak{d}_E}\big)$$

and the last volume equals $\frac{p^{2n-s+1}+p^s-p-1}{p-1}$ using Theorem 2.7(c). □

Corollary 2.18. *If $k = \mathbb{Q}(\mu_p)$ so that $s = 1$, then*

$$(p^{2n} - 1) \times \left(1 - \frac{1}{p+1}\right) \;<\; \mathrm{rank}_{\mathbb{Z}}\, E(K_n) \;\leq\; p^{2n} + 4.$$

As we also found in Example (A), if the prime p is very big then $1 - \frac{1}{p+1}$ becomes very close to 1, but these bounds will never be quite enough to produce an equality. It would be a worthwhile project to look for explicit p-adic Lie extensions K_∞/k where the two bounds agree, and thus equality follows.

Examples (A)–(C) suggest most of the cyclotomic λ-invariant for E over K_n is absorbed into the Mordell-Weil group. If we identify $\mathbb{Z}_p[\![\Gamma]\!]$ with the power series ring $\mathbb{Z}_p[\![X]\!]$, the characteristic power series over the number fields K_n are of the form

$$\mathrm{char}_{\mathbb{Z}_p[\![\Gamma]\!]}\big(\mathcal{X}_E(K_n^{\mathrm{cy}})\big) \;=\; p^{\mu_n} \times X^{p^{2n}\cdot\delta_p} \times g_n$$

where $\delta_p \sim 1$ if the prime $p \gg 1$, $\mu_n \geq 0$ denotes the cyclotomic μ-invariant, and g_n is some polynomial whose degree is significantly smaller than $p^{2n} \times \delta_p$.

3. Control theorems

Let us now suppose that the prime number $p \geq 5$, and fix an infinite extension K_∞ of k whose Galois group $G_\infty = \mathrm{Gal}(K_\infty/k)$ is a p-adic Lie group of dimension d. We also assume:

(A) The Galois group G_∞ is torsion-free.

(B) The cyclotomic $\mathbb{Z}_p$-extension k^{cy} of k is contained inside K_∞.

(C) At each prime v of k above p, the maximal unramified extension of $K_{\infty,w}/k_v$ is finite for all primes w of K_∞ lying above v.

Let $\mathcal{H} = \mathrm{Gal}(K_\infty/k^{\mathrm{cy}})$ and $\Gamma = \mathrm{Gal}(k^{\mathrm{cy}}/k)$. One may write G_∞ as the semi-direct product $\mathcal{H} \rtimes \Gamma$.

Suppose E/k is an elliptic curve that has good ordinary reduction at all primes above p; we abbreviate $E[p^\infty]$ by B. If L/k is an algebraic extension, we write $B(L)$ for $H^0(L, B) = E(L)[p^\infty]$, and recall from [Zer04, Prop10] that for any p-adic Lie extension F of k, either $B(F) = B$ or $\#B(F) < \infty$. We shall assume that

(D) $\#B(K_\infty)$ is finite.

We note that the situation where $K_\infty = k(B)$ has been extensively studied by Harris [Har79], Coates [Coa99] and many others.

Let Σ be the set of primes of k consisting of those above p, the archimedian primes and the places where E has bad reduction. For each prime $v \in \Sigma$ and an extension L/k, we write

$$J_v(L) = \bigoplus_{w|v} \frac{H^1(L_w, B)}{E(L_w) \otimes \mathbb{Q}_p/\mathbb{Z}_p}.$$

Let us also assume that

(E) There are finitely many primes of K_∞ lying above v for all $v \in \Sigma$.

We remind the reader that if L is an extension of k, we have written $\mathrm{Sel}_p(E/L)$ for the p-primary part of the Selmer group of E over L.

Theorem 3.1. *Let L/k be a finite extension contained inside K_∞, and let α denote the restriction map*

$$\mathrm{Sel}_p(E/L) \to \mathrm{Sel}_p(E/K_\infty)^{G_L}$$

where $G_L = \mathrm{Gal}(K_\infty/L)$. Under hypotheses **(A)**–**(D)**, *both $\ker\alpha$ and $\mathrm{coker}\alpha$ are finite; furthermore, there is an upper bound $\#\ker\alpha \leq \#B(K_\infty)^d$.*

Remark: Such a control theorem has been proved in [Gre03], and certain sufficient conditions for both $\ker\alpha$ and $\mathrm{coker}\alpha$ to be uniformly bounded have been given. For our purposes, we do not need to have uniform bounds, but rather, asymptotic growths of these groups. In the proof of Theorem 3.1, we shall give an explicit (but much more complicated) upper bound on $\#\mathrm{coker}\alpha$ – this allows us to analyse the asymptotic behaviour of these bounds in § 3.3 below.

Consider the fundamental diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_p(E/K_\infty)^{G_L} & \longrightarrow & H^1(G_\Sigma(K_\infty),B)^{G_L} & \longrightarrow & \bigoplus_{v\in\Sigma} J_v(K_\infty)^{G_L} \\
 & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \gamma=\oplus\gamma_v} \\
0 & \longrightarrow & \mathrm{Sel}_p(E/L) & \longrightarrow & H^1(G_\Sigma(L),B) & \longrightarrow & \bigoplus_{v\in\Sigma} J_v(L) \longrightarrow 0.
\end{array}$$

By the snake lemma, we have the exact sequence

$$0 \to \ker\alpha \to \ker\beta \to \ker\gamma \to \mathrm{coker}\alpha \to \mathrm{coker}\beta.$$

Therefore to bound $\ker\alpha$ and $\mathrm{coker}\alpha$, it is sufficient to bound $\ker\beta$, $\mathrm{coker}\beta$ and $\ker\gamma$, respectively.

3.1. Bounding $\ker\beta$ and $\mathrm{coker}\beta$.

Lemma 3.2. *Under hypothesis* **(D)**, *both $\ker\beta$ and $\mathrm{coker}\beta$ are finite. Furthermore, $\#\ker\beta \leq (\#B(K_\infty))^d$ and $\#\mathrm{coker}\beta \leq (\#B(K_\infty))^{2d}$.*

Proof. From the inflation-restriction exact sequence

$$0 \to H^1(G_L, B(K_\infty)) \to H^1(G_\Sigma(L),B) \to H^1(G_\Sigma(K_\infty),B)^{G_L} \to H^2(G_L, B(K_\infty))$$

we deduce that $\ker\beta = H^1(G_L, B(K_\infty))$ and $\mathrm{coker}\beta \hookrightarrow H^2(G_L, B(K_\infty))$. Because $\#B(K_\infty) < \infty$, it is clear both $H^1(G_L, B(K_\infty))$ and $H^2(G_L, B(K_\infty))$ are finite with bounds as stated in the lemma. □

Note that $\ker\alpha \hookrightarrow \ker\beta$, hence the finiteness of $\ker\alpha$ and the bound on $\#\ker\alpha$ in Theorem 3.1 follow from the above result.

3.2. Bounding $\ker\gamma$.

For each $v \in \Sigma$, fix a prime u of L (respectively w of K_∞) that lies above v (respectively above u). We shall write $G_u = \mathrm{Gal}(K_{\infty,w}/L_u)$, $\mathcal{H}_u = \mathrm{Gal}(K_{\infty,w}/L_u^{\mathrm{cy}})$ and $\Gamma_u = G_u/\mathcal{H}_u \cong \mathrm{Gal}(L_u^{\mathrm{cy}}/L_u)$, and study γ_v in a number of different cases.

3.2.1. *The study of* $\ker\gamma_v$ *for* $v \nmid p\infty$. Note that if $v \in \Sigma$ is a finite prime and $v \nmid p$, then

$$\ker\gamma_v = \bigoplus_{u|v} H^1(G_u, B(K_{\infty,w}))$$

by inflation-restriction. Furthermore, G_u is a p-adic Lie group of dimension ≤ 2. By [Ser63, II.§5 Ex 2], if q denotes the cardinality of the residue field L_u, then its maximal pro-p extension has Galois group isomorphic to either $\mathbb{Z}_p$ if $q \not\equiv 1 \mod p$, or to $\langle x, y : xyx^{-1} = y^q\rangle$ if $q \equiv 1 \mod p$. As a consequence, $\mathcal{H}_u$ is either trivial or isomorphic to $\mathbb{Z}_p$ (as G_u is torsion-free).

Case 1: $\mathcal{H}_u$ is trivial.

Let us first recall the following classical result from group cohomology.

Lemma 3.3. *Let G be a pro-cyclic group such that $G = \langle g\rangle \cong \mathbb{Z}_p$, and let A be a G-module; then $H^1(G, A) \cong A/(g-1)$. Suppose furthermore that A is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r$ as abelian groups for some integer $r \geq 0$. Then $H^0(G, A)$ and $H^1(G, A)$ have the same $\mathbb{Z}_p$-corank; in this case, if $H^0(G, A)$ is finite then $H^1(G, A) = 0$.*

Corollary 3.4. *Let F/L_u be a $\mathbb{Z}_p$-extension. Then $H^1(F/L_u, B(F))$ is finite, and its cardinality is bounded above by $\#B(F)/B(F)_{\mathrm{div}}$.*

Proof. We may decompose $B(F)$ into $B(F)_{\mathrm{div}} \oplus B(F)'$ for some finite subgroup $B(F)'$ of $B(F)$. Since both $B(F)_{\mathrm{div}}$ and $B(F)'$ are $\mathrm{Gal}(F/L_u)$-modules, we have

$$H^1(F/L_u, B(F)) \cong H^1(F/L_u, B(F)_{\mathrm{div}}) \oplus H^1(F/L_u, B(F)').$$

However the invariants $H^0(F/L_u, B(F)_{\mathrm{div}})$ are finite, in which case Lemma 3.3 tells us that $H^1(F/L_u, B(F)_{\mathrm{div}}) = 0$. Therefore

$$H^1(F/L_u, B(F)) = H^1(F/L_u, B(F)') \cong B(F)'/(\gamma - 1)$$

is finite, with cardinality bounded by $\#B(F)' = \#B(F)/B(F)_{\mathrm{div}}$ as required. □

If $\mathcal{H}_u$ is trivial, then $K_{\infty,w} = L_u^{\mathrm{cy}}$ is the unique unramified $\mathbb{Z}_p$-extension of L_u. Hence we may apply Corollary 3.4 to deduce that $\ker\gamma_u$ is finite, and that its cardinality is bounded above by $\#B(L_u^{\mathrm{cy}})/B(L_u^{\mathrm{cy}})_{\mathrm{div}}$.

Case 2: $\mathcal{H}_u \cong \mathbb{Z}_p$.
We consider two separate sub-cases.

Case 2.a: E does not have potential good reduction at v.
The extension $L_u(B)/L_u$ is also a p-adic Lie extension of dimension 2, which means that $K_{\infty,w} = L_u(B)$. We can therefore apply [Coa99, Proposition 3.9] to deduce that $\ker\gamma_u$ is finite and its cardinality is the exact power of p dividing $c_u/L_u(E, 1)$, where c_u is the local Tamagawa number of E at u.

Case 2.b: E has potential good reduction at v.
Suppose that M/L is a finite extension in which u is totally ramified, and that E has good reduction at u' the unique prime of M above u. We shall now write $M_\infty = K_{\infty,w} \cdot M$, which is a finite extension of $K_{\infty,w}$. Let $G_{u'} = \mathrm{Gal}(M_\infty/M_{u'})$, $\mathcal{H}_{u'} = \mathrm{Gal}(M_\infty/M_{u'}^{\mathrm{cy}})$ and $\Gamma_{u'} = G_{u'}/\mathcal{H}_{u'} \cong \mathrm{Gal}(M_{u'}^{\mathrm{cy}}/M_{u'})$ as before.

Lemma 3.5. *There exists an isomorphism*

$$H^1(G_{u'}, B) \cong \mathrm{Hom}(\mathcal{H}_{u'}, B)^{\Gamma_{u'}}.$$

Proof. Our assumption $v \nmid p$ means that the p-power torsion points on E generate an unramified extension of $M_{u'}$, so $M_{u'}(B) = M_{u'}^{\mathrm{cy}} \subset M_\infty$ and $B^{\mathcal{H}_{u'}} = B$.

Note that $H^2(\Gamma_{u'}, B) = 0$, as the cohomological dimension of $\Gamma_{u'}$ is 1 given that it is procyclic. Inflation-restriction yields the short exact sequence

$$0 \to H^1(\Gamma_{u'}, B) \to H^1(G_{u'}, B) \to H^1(\mathcal{H}_{u'}, B)^{\Gamma_{u'}} \to 0.$$

Now Lemma 3.3 tells us that $H^1(\Gamma_{u'}, B) = 0$, in which case there are isomorphisms $H^1(G_{u'}, B) \cong H^1(\mathcal{H}_{u'}, B)^{\Gamma_{u'}} \cong \mathrm{Hom}(\mathcal{H}_{u'}, B)^{\Gamma_{u'}}$. □

Proposition 3.6. *Let q be the order of the residue field of $M_{u'}$, and let $\mathrm{Frob}_{u'}$ be the Frobenius element in $\Gamma_{u'}$. Then, there is an isomorphism*

$$\mathrm{Hom}(\mathcal{H}_{u'}, B)^{\Gamma_{u'}} \cong \ker(\mathrm{Frob}_{u'} - q : B \to B).$$

Furthermore, the above is a finite group, whose cardinality is equal to the exact power of p dividing $1/L_{u'}(E, 1)$.

Proof. Fix a topological generator y of $\mathcal{H}_{u'}$. Then, the conjugation action of $\mathrm{Frob}_{u'}$ on y is given by $y^{\mathrm{Frob}_{u'}} = y^q$. Note that if θ is an element of $\mathrm{Hom}(\mathcal{H}_{u'}, B)$, it is uniquely determined by $\theta(y) \in B$; we shall set $Q = \theta(y) \in B$. If in addition θ is invariant under the action of $\Gamma_{u'}$, then

$$\theta(y^{\mathrm{Frob}_{u'}}) = \mathrm{Frob}_{u'} \cdot \theta(y)$$

which is equivalent to

$$q \cdot Q = \mathrm{Frob}_{u'} \cdot Q.$$

Recall that the Pontryagin dual $B^\vee$ of B is $T_p(E)$ via the Weil pairing. It follows that the dual of $\ker(\mathrm{Frob}_{u'} - q : B \to B)$ is isomorphic to $T_p(E)/(\mathrm{Frob}_{u'} - q)$ as $\mathrm{Frob}_{u'} - q$ is self-dual. The latter is a finite group because q is not a Weil number, and its cardinality is equal to the exact power of p dividing $\det(\mathrm{Frob}_{u'} - q | T_P(E))$, which coincides with $1/L_{u'}(E, 1)$. This concludes the proof. □

Corollary 3.7. *The group $\ker \gamma_u$ is finite of cardinality bounded by the exact p power dividing $1/L_{u'}(E, 1)$.*

Proof. Without loss of generality, we may assume that $M_{u'}/L_u$ is a Galois extension of degree co-prime to p, because $p \geq 5$. We have the inflation-restriction exact sequence

$$0 \to H^1(M_{u'}/L_u, B(M_{u'})) \to H^1(M_\infty/L_u, B) \to H^1(G_{u'}, B).$$

However $H^1(M_{u'}/L_u, B(M_{u'})) = 0$ by our assumption on the degree of $M_{u'}/L_u$. Therefore, we deduce from Lemma 3.5 and Proposition 3.6 that $H^1(M_\infty/L_u, B)$ is in fact finite of cardinality bounded by the exact p power dividing $1/L_{u'}(E, 1)$. Since $\ker \gamma_u = H^1(G_u, B(K_{\infty,w}))$ is a subgroup of $H^1(M_\infty/L_u, B)$ via inflation, the corollary follows. □

3.2.2. *The study of $\ker \gamma_v$ for $v|p\infty$.* It is clear that if $v|\infty$, $\ker \gamma_v = 0$ since we assume that $p \neq 2$. It remains to study the case where $v|p$, for which we have the following result of Greenberg.

Proposition 3.8. *If $v|p$, then $\ker \gamma_v$ is finite. Furthermore, there exists a constant C_p such that $\#\ker \gamma_v \leq C_p$ for all L and u.*

Proof. Note that E has good ordinary reduction at v and that our assumption **(C)** implies that the residue field of $K_{\infty,w}$ is a finite extension of that of k_v. In particular, if $\tilde{E}$ denotes the reduced curve for E at the place w, $\tilde{E}(K_{\infty,w})$ is finite and [Gre03, Propositions 4.2 and 4.4] apply. □

Finally we conclude that $\mathrm{coker}\alpha$ is finite, and that there exists some constant C_L such that

$$\#\mathrm{coker}\alpha \leq C_L$$

where C_L is given by a product $C_\infty \times \prod_u C_u$, with u running through the finite primes of L that divide Σ, and

$$C_u = \begin{cases} \#B(K_\infty))^{2d} & \text{if } u = \infty; \\ \#B(L_u^{\mathrm{cy}})/B(L_u^{\mathrm{cy}})_{\mathrm{div}} & u \nmid p,\ \dim G_u = 1; \\ |c_u/L_u(E,1)|_p^{-1} & u \nmid p,\ \dim G_u = 2 \text{ and } E \text{ not potential good at } u; \\ |1/L_{u'}(E,1)|_p^{-1} & u \nmid p,\ \dim G_u = 2 \text{ and } E \text{ potential good at } u; \\ C_p & u|p. \end{cases}$$

Here $|-|_p$ denotes the p-adic norm given normalized by $|p|_p = p^{-1}$, so that $|\star|_p^{-1}$ is the exact p-power dividing $\star$ for any rational number $\star$.

3.3. **Variation of C_L.** We now study the constant C_L as L varies. We first remark that C_∞ and C_p are independent of L by definition. If $u \nmid p$ and $\dim G_u = 1$, then C_u is uniformly bounded. For $u|p$, if the maximal unramified extension of L_u inside $K_{\infty,w}$ is finite, then C_u is also uniformly bounded.

For $u \nmid p$ and $\dim G_u = 2$, we remark that the terms $1/L_u(E,1)$ and $1/L_{u'}(E,1)$ correspond to the number points on the reduced curves $\tilde{E}$ modulo u and u'; hence, the exact powers of p dividing these terms are given by $\#\tilde{B}_u(\ell_u)$ and $\#\tilde{B}_{u'}(\ell_{u'})$.

Lemma 3.9. *If E has multiplicative reduction at u, then* $\left|\frac{1}{L_u(E,1)}\right|_p^{-1} = \left|\#\ell_u - 1\right|_p^{-1}$.

Proof. This follows from the fact that $\tilde{E}(\ell_u) \cong \ell_u^\times$. □

Corollary 3.10. *Suppose that* $\dim G_u = 2$. *If E has split multiplicative reduction at u, then $C_u = [L_u : k_v]C_v$. If E has non-split multiplicative reduction at u, then $C_u = [\mathbb{F}_u : \mathbb{F}_v]C_v$ where $\mathbb{F}_u$ and $\mathbb{F}_v$ are the residue fields of L_u and k_v, respectively.*

Proof. Let e and f be the ramification index and the inertia degree of the extension L_u/k_v. Then both e and f are p-powers since L_u/k_v is a p-extension.

Let q_v and q_u be the cardinalities of the residue fields of k_v and L_u, respectively. Clearly $q_u = q_v^f$, and we write $q_v = 1 + p^r s$ where $p \nmid s$. By Lemma 3.9, the exact order of p dividing $1/L_v(E,1)$ is p^r. If $f = p^t$ then

$$q_u = (1 + p^r s)^{p^t} = 1 + p^{r+t}s + O(p^{r+t+1}),$$

and the latter implies the exact p-power dividing $q_u - 1$ is $p^{r+t} = f \times p^r$.

Note if E has split multiplicative reduction at u, then the Tamagawa number c_u is given by $\mathrm{ord}_u(\Delta_E)$, therefore $c_u = e \times c_v$; we may deduce that $C_u = e \times f \times C_v$. If E has non-split multiplicative reduction, then c_u is coprime to p as we assume that $p \geq 5$, and we are done. □

Proposition 3.11. *Suppose that $u \nmid p$, $\dim G_u = 2$ and E has potential good reduction at u. Then $C_u \leq [\mathbb{F}_u : \mathbb{F}_v]^2 C_v$.*

Proof. Assume that E has good reduction over the finite extension $M_{v'}$ of k_v, whose degree is coprime to p. Then L_u and $M_{v'}$ are linearly disjoint over k_v, and E has good reduction over $M_{u'} := M_{v'} \cdot L_u$. We have

$$C_v = |1/L_{u'}(E,1)|_p^{-1} = |1 + q_{v'} - a_{v'}|_p^{-1} = |(1-s)(1-t)|_p^{-1}$$

where $q_{v'} = \#\mathbb{F}_{v'}$, $a_{v'}$ is the trace of the Frobenius on the Tate module and s, t are the roots of $X^2 - a_{v'}X + q_{v'}$. Suppose $[\mathbb{F}_{u'} : \mathbb{F}_{v'}] = p^n$, so that

$$C_u = |1/L_{u'}(E,1)|_p^{-1} = |(1-s^{p^n})(1-t^{p^n})|_p^{-1}.$$

If $|1-s|_p^{-1} = 1$, then the same is true for $1 - s^{p^n}$ by Fermat's little theorem; otherwise, we may write $1 - s = a\pi$ where $a, \pi \in \mathcal{O}_{\mathbb{C}_p}$ with $|a|_p = 1$ and $|b|_p < 1$. One has the π-adic expansion

$$1 - s^{p^n} = 1 - (1 - a\pi)^{p^n} = ap^n\pi + O(p^n\pi^2)$$

and the above implies $|1-s^{p^n}|_p^{-1} = p^n \times |1-s|_p^{-1}$. Undertaking a similar calculation with t replacing s, we deduce that

$$C_u \leq p^{2n} \times C_v = [\mathbb{F}_{u'} : \mathbb{F}_{v'}] C_v.$$

However $M_{v'}/k_v$ and $M_{u'}/L_u$ are totally ramified, thus $[\mathbb{F}_{u'} : \mathbb{F}_{v'}] = [\mathbb{F}_u : \mathbb{F}_v]$. □

3.4. **Control theorem for infinite extensions.** Theorem 3.1 deals with finite extensions L/k. We now introduce an analogous result that deals with infinite algebraic extensions containing the cyclotomic $\mathbb{Z}_p$-extension k^{cy} of k.

Theorem 3.12. *Let L/k be a finite extension contained inside K_∞, and α' the restriction map*

$$\mathrm{Sel}_p(E/L^{\mathrm{cy}}) \to \mathrm{Sel}_p(E/K_\infty)^{\mathcal{H}_L}$$

where $\mathcal{H}_L = \mathrm{Gal}(K_\infty/L^{\mathrm{cy}})$. Under hypotheses **(A)**–**(E)**, *both* $\ker\alpha'$ *and* $\mathrm{coker}\alpha'$ *have finite $\mathbb{Z}_p$-coranks, and their maximal finite quotients are bounded as L varies.*

Proof. We once again consider the fundamental diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_p(E/K_\infty)^{\mathcal{H}_L} & \longrightarrow & H^1(G_\Sigma(K_\infty), B)^{\mathcal{H}_L} & \longrightarrow & \bigoplus_{v\in\Sigma} J_v(K_\infty)^{\mathcal{H}_L} \\
 & & \uparrow{\scriptstyle \alpha'} & & \uparrow{\scriptstyle \beta'} & & \uparrow{\scriptstyle \gamma' = \oplus\gamma_v'} \\
0 & \longrightarrow & \mathrm{Sel}_p(E/L^{\mathrm{cy}}) & \longrightarrow & H^1(G_\Sigma(L^{\mathrm{cy}}), B) & \longrightarrow & \bigoplus_{v\in\Sigma} J_v(L^{\mathrm{cy}}) \longrightarrow 0.
\end{array}$$

It is clear that the same argument as in Lemma 3.2 shows both $\ker\beta'$ and $\mathrm{coker}\beta'$ are finite, bounded above independently of L. It remains to consider $\ker\gamma_v'$.

If $v \nmid p\infty$, and $\mathcal{H}_u = 1$, then we have trivially $\gamma_v' = 0$. If $\mathcal{H}_u \cong \mathbb{Z}_p$, we may apply [HV03, Lemma 3.4] and deduce that $\ker\gamma_v \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{n_v}$ for some integer n_v, depending on the number of primes lying above v. If $v|p\infty$, the results in §3.2.2 still apply, and the theorem follows. □

Remark: The $\mathbb{Z}_p$-coranks in Theorem 3.12 are in fact given by $m_{\mathrm{sm}}^{\mathrm{cy}} + 2 \times m_{\mathrm{pgr}}^{\mathrm{cy}}$, in the terminology of Proposition 2.3.

4. Bounding Shafarevich-Tate groups

We write $\mathfrak{M}_{\mathcal{H}}(G_\infty)$ (respectively $\mathfrak{M}_{\mathcal{H}}(G_\infty)^*$) for the category of $\mathbb{Z}_p[\![G_\infty]\!]$-modules M such that $M/M[p^\infty]$ (respectively M) is finitely generated over the ring $\mathbb{Z}_p[\![\mathcal{H}]\!]$. Applying [BV11, Proposition 3.4], there is an isomorphism of algebraic K-groups

$$K_0(\mathfrak{M}_{\mathcal{H}}(G_\infty)) \cong K_0(\mathfrak{M}_{\mathcal{H}}(G_\infty)^*) \oplus K_0(\mathbb{F}_p[\![G_\infty]\!]). \tag{4.1}$$

Note that $K_0(\mathbb{F}_p[\![G_\infty]\!])$ is in fact isomorphic to $\mathbb{Z}$ since G_∞ is torsion-free (c.f the discussion at the beginning of Section 3.3 in *op. cit.*).

For each $M \in K_0(\mathfrak{M}_{\mathcal{H}}(G_\infty))$, we define the μ-invariant $\mu_{G_\infty}(M) \in \mathbb{Z}$ to be its image inside $K_0(\mathbb{F}_p[\![G_\infty]\!])$. The μ-invariant has been equivalently defined in [How02] and [Ven02] to be

$$\sum_{i\geq 0} \mathrm{rank}_{\mathbb{F}_p[\![G_\infty]\!]} \left(M[p^{i+1}]/M[p^i]\right).$$

Inside G_∞, we fix a series of open subgroups $G_\infty \supset G_1 \supset G_2 \supset \cdots$ such that $[G_\infty : G_n] = Cp^{dn}$ for $n \gg 0$. We shall analyse the growth of $M_{G_n}[p^\infty]$ for a given $M \in \mathfrak{M}_{\mathcal{H}}(G_\infty)$. This will be done in three steps:

(i) We analyse the growth of $M[p^\infty]$ by studying the variation of μ-invariants;
(ii) We study the module $M/M[p^\infty] \in \mathfrak{M}_{\mathcal{H}}(G_\infty)^*$ and in particular, upon taking $\mathcal{H}^{p^n}$-coinvariants, the growth in the resulting λ-invariants as $n \to \infty$;
(iii) Lastly, we study the contribution to $M_{G_n}[p^\infty]$ coming from these λ-invariants, using the techniques of Iwasawa and Mazur.

4.1. Estimations of $\mathbb{Z}_p$-torsion modules.

Lemma 4.1. *Let M be a finitely generated $\mathbb{Z}_p[\![G_\infty]\!]$-module that is $\mathbb{Z}_p$-torsion. If M/p is a torsion $\mathbb{F}_p[\![G_\infty]\!]$-module, then for all $i \geq 0$*

$$\#H_i(G_n, M) = p^{O(p^{(d-1)n})}.$$

Proof. This result is based on [Per11, Corollaire 2.4]. Since $\mathbb{Z}_p[\![G_\infty]\!]$ is Noetherian, there exists an integer r such that $M[p^r] = M$. For all $k < r$, we may apply Corollaire 2.3 of *op. cit.* to obtain the bound

$$\#H_i(G_n, p^k M/p^{k+1}M) \leq p^{C_k p^{(d-1)n}}$$

where C_k is some constant that is independent of n. From the short exact sequence

$$0 \to p^{k+1}M \to p^k M \to p^k M/p^{k+1}M \to 0,$$

we obtain the inequality $\#H_i(G_n, p^k M) \leq \#H_i(G_n, p^{k+1}M) \times p^{C_k p^{(d-1)n}}$. Now $p^r M = 0$, hence one deduces that

$$\#H_i(G_n, M) \leq p^{(C_1+\cdots C_r)p^{(d-1)n}}.$$

□

Lemma 4.2. *Let M and N be finitely generated $\mathbb{Z}_p[\![G_\infty]\!]$-modules that are $\mathbb{Z}_p$-torsion. If M and N are pseudo-isomorphic as $\mathbb{Z}_p[\![G_\infty]\!]$-modules, then*

$$\#M_{G_n} = \#N_{G_n} \times p^{O(p^{(d-1)n})}.$$

Proof. This result is based on [Per11, Proposition 2.5]. As in the proof of *op. cit.*, there is an exact sequence

$$0 \to A \to M \xrightarrow{f} N \to B \to 0$$

where A, B are pseudo-null $\mathbb{Z}_p[\![G_\infty]\!]$-modules. This gives two short exact sequences

$$0 \to A \to M \to \mathrm{im}(f) \to 0,$$
$$0 \to \mathrm{im}(f) \to N \to B \to 0.$$

Furthermore, our assumption on the $\mathbb{Z}_p$-torsioness means that A and B are also $\mathbb{Z}_p$-torsion. By [Per11, Lemme 1.9], we may apply Lemma 4.1 to both A and B. From the homologies of the two short exact sequences above, we deduce that

$$\#M_{G_n} = \#\,\mathrm{im}(f)_{G_n} \times p^{O(p^{(d-1)n})} = \#N_{G_n} \times p^{O(p^{(d-1)n})}.$$

□

Corollary 4.3. *If M is a finitely generated $\mathbb{Z}_p[\![G_\infty]\!]$-module that is also $\mathbb{Z}_p$-torsion,*

$$\#M_{G_n} = p^{[G_\infty : G_n] \times \mu_{G_\infty}(M) + O(p^{(d-1)n})}.$$

Proof. Using the main result of [Ven02], there exists a pseudo-isomorphism of $\mathbb{Z}_p[\![G_\infty]\!]$-modules

$$\varphi : M[p^\infty] \to \oplus \mathbb{Z}_p[\![G_\infty]\!]/p^{n_i}$$

for unique integers $n_i \geq 0$ and $\mu_\Gamma(M[p^\infty]) = \sum n_i$. Therefore by Lemma 4.2,

$$\#M_{G_n} \;=\; \prod_i \#(\mathbb{Z}_p[\![G_\infty]\!]/p^{n_i})_{G_n} \times p^{O(p^{(d-1)n})} \;=\; p^{\sum n_i \times [G_\infty : G_n] + O(p^{(d-1)n})}.$$

□

4.2. **Estimations for elements in $K_0(\mathfrak{M}_{\mathcal{H}}(G_\infty)^*)$.** Throughout this section, we fix an element $Y \in K_0(\mathfrak{M}_{\mathcal{H}}(G_\infty)^*)$.

Lemma 4.4. *Let $\mathcal{H}' \leq \mathcal{H}$ be an open subgroup for which $H_1(\mathcal{H}', Y)$ is finite. Then, $\mu_\Gamma(Y_{\mathcal{H}'}) = 0$.*

Proof. There is a short exact sequence

$$0 \to N \to \mathbb{Z}_p[\![\mathcal{H}]\!]^{\oplus r} \to Y \to 0$$

for some $r \geq 0$ and some sub-module N of $\mathbb{Z}_p[\![\mathcal{H}]\!]^{\oplus r}$. This induces an exact sequence

$$H_1(\mathcal{H}', Y) \to N_{\mathcal{H}'} \xrightarrow{\delta} \mathbb{Z}_p[\mathcal{H}/\mathcal{H}']^{\oplus r} \to Y_{\mathcal{H}'} \to 0.$$

Note that $\mathbb{Z}_p[\mathcal{H}/\mathcal{H}']^{\oplus r}$ is a free $\mathbb{Z}_p$-module, so $\mu_\Gamma(\mathbb{Z}_p[\mathcal{H}/\mathcal{H}']^{\oplus r}) = 0$. Furthermore, since $H_1(\mathcal{H}', Y)$ is finite we obtain the finiteness of $\ker \delta$ as well, which then implies $\mu_\Gamma(N_{\mathcal{H}'}) = 0$. As μ-invariants respect exact sequences, we deduce $\mu_\Gamma(Y_{\mathcal{H}'}) = 0$. □

Remark: In [CFKS10, Theorem 3.5] it is shown, under certain hypotheses, that the condition $H_i(\mathcal{H}', Y)$ is finite holds for all $i \geq 1$.

From now on, we assume that

(U) Either G_∞ is a uniform pro-p group, or $\mathcal{H}$ is an abelian group.

In general G_∞ contains a uniform open subgroup, so we may always achieve **(U)** by taking a finite extension of k. Under this hypothesis, let $\mathcal{H}_n := \mathcal{H}^{p^n}$, $\Gamma_n := \Gamma^{p^n}$ and $G_n := G_\infty^{p^n} = \mathcal{H}_n \rtimes \Gamma_n$.

Lemma 4.5. *Suppose that G_∞ is uniform, and both $H_i(\mathcal{H}_n, Y)$ and $H_i(\mathcal{H}_{n+1}, Y)$ are finite for all $i \geq 1$. Then*

$$\mathrm{rank}_{\mathbb{Z}_p}(Y_{\mathcal{H}_{n+1}}) = p^{d-1} \times \mathrm{rank}_{\mathbb{Z}_p}(Y_{\mathcal{H}_n}).$$

Proof. This is proven in [DL15b, proof of Theorem 2.6] for the case $d = 3$ and n sufficiently large using the Ritter-Weiss congruence from [RW06]. The condition $d \leq 3$ was needed to show the uniformity of the p-adic Lie group ([DL15b, Lemma 3.2 and Theorem 4.2]) and that the characteristic ideals of $H_i(-, Y)$ vanish for all $i \geq 1$ (Lemma 2.3 of *op. cit.*). Since we are assuming that G_∞ is uniform and that the relevant homology groups are finite, the same proof goes through verbatim. □

Corollary 4.6. *If G_∞ is uniform and $H_i(\mathcal{H}_n, Y)$ are finite for all $n \gg 0$ and $i \geq 1$, then there exists some constant τ_Y such that $\lambda_\Gamma(Y_{\mathcal{H}_n}) = \tau_Y p^{(d-1)n}$ for all $n \gg 0$.*

Proposition 4.7. *Suppose that $\mathcal{H}$ is abelian. Then $Y_{\mathcal{H}_n}$ is a torsion $\mathbb{Z}_p[\![\Gamma]\!]$-module whose λ-invariant is given by $\tau_Y p^{(d-1)n} + O(p^{(d-2)n})$, where $\tau_Y = \mathrm{rank}_{\mathbb{Z}_p[\![\mathcal{H}]\!]} Y$.*

Proof. From the structure theorem [Bou65, §4, Théorème 4] for finitely-generated modules over $\mathbb{Z}_p[\![\mathcal{H}]\!]$, there is a pseudo-isomorphism

$$M \sim \mathbb{Z}_p[\![\mathcal{H}]\!]^{\tau_Y} \oplus T$$

where T is a finitely-generated torsion $\mathbb{Z}_p[\![\mathcal{H}]\!]$-module whose μ-invariant vanishes. By [CM81, Lemma 3.3], if M and N are pseudo-isomorphic $\mathbb{Z}_p[\![\mathcal{H}]\!]$-module, then

$$\left| \mathrm{rank}_{\mathbb{Z}_p}(M)_{\mathcal{H}_n} - \mathrm{rank}_{\mathbb{Z}_p}(N)_{\mathcal{H}_n} \right| = O(p^{(d-3)n}).$$

Therefore one may assume that Y is of the form $\mathbb{Z}_p[\![\mathcal{H}]\!]^{\tau_Y} \oplus T$. Theorem 3.14 of *op. cit.* says that $\mathrm{rank}_{\mathbb{Z}_p} T_{\mathcal{H}_n} = O(p^{(d-2)n})$, and moreover

$$\mathrm{rank}_{\mathbb{Z}_p} \mathbb{Z}_p[\![\mathcal{H}/\mathcal{H}_n]\!]^{\tau_Y} = \tau_Y \times [\mathcal{H} : \mathcal{H}_n] = \tau_Y \times p^{(d-1)n}.$$

Hence $Y_{\mathcal{H}_n}$ must be of rank $\tau_Y p^{(d-1)n} + O(p^{(d-2)n})$, which means it is a torsion module over $\mathbb{Z}_p[\![\Gamma]\!]$, with the λ-invariant as claimed. □

4.3. **Estimations in cyclotomic extensions.** Throughout this section, we shall identify the Iwasawa algebra $\mathbb{Z}_p[\![\Gamma]\!]$ with the power series ring $\mathbb{Z}_p[\![X]\!]$. For an integer $i \geq 1$, we fix a primitive p^i-th root of unity ζ_{p^i}. We shall write $\epsilon_i = \zeta_{p^i} - 1$ and let ω_i and Φ_i be $(1+X)^{p^i} - 1$ and the minimal polynomial of ϵ_i respectively. For $i = 0$, we set $\epsilon_0 = 0$ and $\omega_0 = \Phi_0 = X$.

Lemma 4.8. *Let $n \geq 1$ and $f \in \mathbb{Z}_p[\![\Gamma]\!]$. We write $h = \gcd(f, \omega_{n-1})$ and $f = gh$. Consider the projection map*

$$\pi_n : \mathbb{Z}_p[\![\Gamma]\!]/(f, \omega_n) \to \mathbb{Z}_p[\![\Gamma]\!]/(f, \omega_{n-1}).$$

We have

(1) $\mathrm{rank}_{\mathbb{Z}_p} \mathbb{Z}_p[\![\Gamma]\!]/(f, \omega_{n-1}) = \mathrm{ord}_{\epsilon_n} h(\epsilon_n)$*;*
(2) If $f(\epsilon_n) \neq 0$, then $\ker \pi_n$ is finite with $\mathrm{len}_{\mathbb{Z}_p} \ker \pi_n = \mathrm{ord}_{\epsilon_n} g(\epsilon_n)$;
(3) If $f(\epsilon_n) = 0$, then $\ker(\pi_n)$ is a free $\mathbb{Z}_p$-module of rank $\phi(p^n)$.

Proof. The first two parts of the lemma are proved in [Kob03, proof of Lemma 10.5(i)]. To show (3), we make use of the isomorphism in *op. cit.*:

$$\ker \pi_n \cong \mathbb{Z}_p[\![\Gamma]\!]/(g, \Phi_n).$$

If $f(\epsilon_n) = 0$, we have $\Phi_n | f$. In particular $\Phi_n | g$, which implies that $(g, \Phi_n) = (\Phi_n)$. Therefore, the isomorphism above becomes $\ker \pi_n \cong \mathbb{Z}_p[\![\Gamma]\!]/\Phi_n$, hence the result. □

Lemma 4.9. *Suppose that $f(0) \neq 0$, then $\mathrm{len}_{\mathbb{Z}_p} \mathbb{Z}_p[\![\Gamma]\!]/(f, X) = \mathrm{ord}_p(f(0))$. Otherwise, $\mathbb{Z}_p[\![\Gamma]\!]/(f, X)$ is free of rank 1 over $\mathbb{Z}_p$.*

Proof. This is immediate from the fact that $\mathbb{Z}_p[\![\Gamma]\!]/(f, X) \cong \mathbb{Z}_p/f(0)$. □

Combining these two lemmas, we obtain the following proposition.

Proposition 4.10. *Let $f \in \mathbb{Z}_p[\![\Gamma]\!]$, and for each integer $n \geq 0$ set*

$$M_n \ = \ \mathbb{Z}_p[\![\Gamma]\!]/(f, \omega_n).$$

One defines $h_n = \gcd(f, \omega_n)$, $g_n = f/h_n$ and chooses $I \subset \{0, 1, \ldots, n\}$ such that $\prod_{i \in I} \Phi_{p^i}(1 + X) = \omega_n/h_n$. Then

(i) $\mathrm{rank}_{\mathbb{Z}_p} M_n = \deg(h_n)$;

(ii) If there exists an integer $n_0 \geq 1$ such that $\omega_{n_0} | f$, then $\# M_n[p^\infty] \leq p^{\sum_{i \in I} \mathrm{ord}_{\epsilon_i} g_i(\epsilon_i)}$;

Proof. Consider the short exact sequence

$$0 \to \ker \pi_i \to M_i \to M_{i-1} \to 0,$$

for $i = 1, \ldots, n$. This tells us that

$$\mathrm{rank}_{\mathbb{Z}_p} M_n = \mathrm{rank}_{\mathbb{Z}_p} M_0 + \sum_{i=1}^{n} \mathrm{rank}_{\mathbb{Z}_p} \ker \pi_i.$$

Hence, Lemmas 4.8 and 4.9 imply that this is equal to $\sum_i \phi(p^i)$, where the sum runs through $1 \leq i \leq n$, with $\Phi_i | h_n$. This gives part (i).

We now prove part (ii). By assumption, $\Phi_0, \ldots, \Phi_{n_0}$ all divide f. The same short exact sequence above and the previous two lemmas tell us that $M_0, M_1, \ldots, M_{n_0}$ are all free $\mathbb{Z}_p$-modules and that

$$\# M_n[p^\infty] \leq \prod_{i \in I} \# \ker(\pi_i)[p^\infty].$$

By Lemma 4.8(2), $\# \ker(\pi_i)[p^\infty] = p^{\mathrm{ord}_{\epsilon_i} g_{i-1}(\epsilon_i)}$. If $i \in I$, we have $\Phi_i \nmid f$, which implies that $g_{i-1} = g_i$. Hence the result. □

Corollary 4.11. *Let $f \in \mathbb{Z}_p[\![\Gamma]\!]$ such that $f = \omega_{n_0} \times R$ for some $n_0 \geq 0$ and R a polynomial over $\mathbb{Z}_p$ whose irreducible factors all have degree $< p^{n_0}(p-1)$. For all $n \geq n_0$,*

$$\# M_n[p^\infty] \leq p^{n \times (\deg f - \mathrm{rank}_{\mathbb{Z}_p} M_n)},$$

where $M_n = \mathbb{Z}_p[\![\Gamma]\!]/(f, \omega_n)$ is as defined in Proposition 4.10.

Proof. By assumption, $\Phi_i \nmid f$ for all $i > n_0$. In particular, under the notation of Proposition 4.10, we have $h_n = \omega_{n_0}$ and $g_i = R$ for all $i \geq n_0$. Hence, $\mathrm{rank}_{\mathbb{Z}_p} M_n = \deg \omega_{n_0}$ and

$$\# M_n[p^\infty] \leq p^{\sum_{i=n_0+1}^{n} \mathrm{ord}_{\epsilon_i} R(\epsilon_i)}.$$

By the Weierstrass preparation theorem, we may assume that $R(X) = X^{\deg R} + pQ(X)$ with $\deg R < p^{n_0}(p-1)$ and $Q(X) \in \mathbb{Z}_p[X]$. Let $i \geq n_0 + 1$. Then $R(\epsilon_i) = \epsilon_i^{\deg R} + pQ(\epsilon_i)$, and since

$$\mathrm{ord}_{\epsilon_i}(pQ(\epsilon_i)) \ \geq \ p^{i-1}(p-1) \ \geq \ p^{n_0}(p-1) \ > \ \deg R \ = \ \mathrm{ord}_{\epsilon_i}(\epsilon_i^{\deg R}),$$

one deduces that $\mathrm{ord}_{\epsilon_i} R(\epsilon_i) = \deg R$. Therefore,

$$\#M_n[p^\infty] \leq p^{(n-n_0)\times \deg R} \leq p^{n(\deg f - \deg \omega_{n_0})},$$

which finishes the proof. □

Definition 4.12. *Let $f \in \mathbb{Z}_p[\![\Gamma]\!]$. We say that f is **almost cyclotomic** if $f = \omega_{n_0} \times R$ for some integer $n_0 \geq 0$ and $R \in \mathbb{Z}_p[\![\Gamma]\!]$ which, up to units, factorises into a product of irreducible polynomials whose degrees are all $< p^{n_0}(p-1)$. If M is a finitely generated torsion $\mathbb{Z}_p[\![\Gamma]\!]$-module, we say that M is almost cyclotomic if it is pseudo-isomorphic to a direct sum $\bigoplus_i \mathbb{Z}_p[\![\Gamma]\!]/f_i$, where each f_i is almost cyclotomic.*

The three examples discussed in §2.5 suggest that the characteristic power series of the Iwasawa modules $\mathcal{X}_E(K_n^{\mathrm{cyc}})$ are 'almost cyclotomic' in nature, for these specimens at least. To establish this requires us to show most p-adic zeroes arise from finite order characters ψ on Γ for which $\mathrm{rank}_{\mathbb{Z}_p}\big(H^0\big(\Gamma_n, \mathcal{X}_E(K_n^{\mathrm{cyc}})\otimes\psi^{-1}\big)\big) > 0$, while the remaining p-adic zeroes (those which are not of the form $\zeta_{p^i} - 1$) have small algebraic degrees over $\mathbb{Q}_p$.

In the appendix, we shall show that it is in fact possible to bound the latter by the $\mathbb{Z}_p[\![\mathcal{H}]\!]$-rank of $\mathcal{X}_E(K_\infty)$, giving evidence for the almost cyclotomic condition *provided* X divides the characteristic ideal of $\mathcal{X}_E(K_n^{\mathrm{cyc}})$ and that the $\mathbb{Z}_p[\![\mathcal{H}]\!]$-rank of $\mathcal{X}_E(K_\infty)$ is $< p-1$. However, as John Coates pointed out to us, there are cases where the characteristic power series for the Selmer group over K_n is **not** almost cyclotomic – e.g. see [Coa02, Thm 7] corresponding to $E = X_1(11)$, $p = 5$, $K_\infty = \mathbb{Q}(E[5^\infty])$ where this condition fails.

4.4. **Estimations of $\#Ш(E/K_n)[p^\infty]$.** We decompose K_∞ into a series of sub-extensions $k \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty$, where each K_n is given by $(K_\infty)^{G_n}$. For a sub-extension L of K_∞/k, recall we wrote $\mathcal{X}_E(L)$ for the Pontryagin dual of the p-Selmer group $\mathrm{Sel}_p(E/L)$, and assume that $\mathcal{X}_E(K_\infty) \in \mathfrak{M}_{\mathcal{H}}(G_\infty)$.

Theorem 4.13. *Let $M = \mathcal{X}_E(K_\infty)$ and write $Y = M/M[p^\infty] \in K_0(\mathfrak{M}_{\mathcal{H}}(G_\infty)^*)$. Suppose that the hypotheses* **(A)**–**(E)** *and* **(U)** *hold, and that $H_i(\mathcal{H}_n, Y)$ is finite for all $i \geq 1$ and $n \gg 0$ if $\mathcal{H}$ is not abelian. Furthermore, suppose that $M_{\mathcal{H}_n}$ is almost cyclotomic for n sufficiently large. Then*

$$\#M_{G_n}[p^\infty] \;\leq\; p^{\mu_{G_\infty}(M)p^{dn} + (\tau_Y p^{(d-1)n} - \mathrm{rank}_{\mathbb{Z}_p} M_{G_n})n + O(p^{(d-1)n})}. \tag{4.2}$$

Proof. From the short exact sequence

$$0 \to M[p^\infty] \to M \to Y \to 0$$

we have

$$\#M_{G_n}[p^\infty] \leq \#M[p^\infty]_{G_n} \times \#Y_{G_n}[p^\infty]. \tag{4.3}$$

Using a combination of Lemma 4.4, Corollary 4.6 and Proposition 4.7, there is an isomorphism of $\mathbb{Z}_p$-modules

$$Y_{\mathcal{H}_n} \;\cong\; \mathbb{Z}_p^{\tau_Y p^{(d-1)n} + O(p^{(d-2)n})} \oplus T_n$$

where T_n is finite.

The main result of [Mat03] tells us that the maximal finite Λ-submodule of $\mathcal{X}_E(K_n^{\mathrm{cy}})$ is bounded by $\#B(K_n^{\mathrm{cy}}) \leq \#B(K_\infty)$ (which is finite by hypothesis **(D)**). Therefore, we deduce from Theorem 3.12 that $\#T_n$ is bounded independently of n.

Our assumption on the characteristic ideals of $M_{\mathcal{H}_n}$ being almost cyclotomic allows us to apply Corollary 4.11, and thereby obtain the bound

$$\#Y_{G_n}[p^\infty] \leq p^{(\tau_Y p^{(d-1)n} - \mathrm{rank}_{\mathbb{Z}_p} M_{G_n})n + O(np^{(d-2)n})}.$$

Moreover Corollary 4.3 tells us that

$$\#M[p^\infty]_{G_n} = p^{\mu_{G_\infty}(M)p^{dn} + O(p^{(d-1)n})},$$

thus we can deduce (4.2) from (4.3). □

Corollary 4.14. *Under the same hypotheses as Theorem 4.13,*

$$\#\mathcal{X}_E(K_n)[p^\infty] \ \leq \ p^{\mu_{G_\infty}(M)p^{dn} + (\tau_Y p^{(d-1)n} - \mathrm{rank}_{\mathbb{Z}_p} M_{G_n})n + O(p^{(d-1)n})}.$$

Proof. This follows directly from Theorem 3.1 and the fact that the constant C_{K_n} in the control theorem is $p^{O(p^n)}$, which is itself a consequence of hypothesis **(C)** and the results in §3.3. □

Remark: One may obtain the weaker estimate

$$\#\mathcal{X}_E(K_n)/p^n \ = \ p^{(\rho_{G_\infty}(M)n + \mu_{G_\infty}(M))p^{dn} + O(np^{(d-1)n})},$$

where $\rho_{G_\infty}(M)$ denotes the rank of M over $\mathbb{Z}_p[\![G_\infty]\!]$, by using Theorem 3.1 together with [Per11, Théorème 2.1], and without assuming that M is inside $K_0(\mathfrak{M}_{\mathcal{H}}(G_\infty))$ (nor the assumption on 'almost cyclotomic', nor that on the homology of Y).

If L is a finite sub-extension of K_∞/k, we shall write $Ш(E/L)$ for the Shafarevich-Tate group of E over L. Assuming the p-primary part $Ш(E/K_n)[p^\infty]$ over the field K_n is finite, from the short exact sequence

$$0 \to E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_p(E/K_n) \to Ш(E/K_n)[p^\infty] \to 0 \tag{4.4}$$

one immediately deduces

$$\#Ш(E/K_n)[p^\infty] \ = \ \#\mathcal{X}_E(K_n)[p^\infty].$$

Moreover Theorem 4.13 tells us that

$$\#Ш(E/K_n)[p^\infty] \ \leq \ p^{\mu p^{dn} + (\tau_Y p^{(d-1)n} - \mathrm{rank}_{\mathbb{Z}_p} M_{G_n})n + O(p^{(d-1)n})}$$

where $\mu = \mu_{G_\infty}(M)$, so in particular

$$\#Ш(E/K_n)[p^\infty] \ \leq \ p^{\mu p^{dn} + \tau_Y np^{(d-1)n} + O(p^{(d-1)n})}.$$

We may refine this bound using Theorem 2.7, under suitable conditions.

Suppose G_∞ is one of the non-commutative groups considered in Theorem 2.7. If the weighted tree $\big(\mathbb{T}_{G_\infty}, \underline{\mathfrak{d}_E}\big)$ associated to the multiplicity of the Artin representations inside $E(K_\infty) \otimes \mathbb{C}$ is in bloom, there exists a rational number $\delta_p \in (0, \tau_Y]$ such that

$$\mathrm{rank}_{\mathbb{Z}} E(K_n) \ \geq \ \delta_p p^{(d-1)n}.$$

By Theorem 3.1, $\mathrm{rank}_{\mathbb{Z}_p} M_{G_n} = \mathrm{rank}_{\mathbb{Z}_p} \mathcal{X}_E(K_n)$. Because we are assuming that $\#Ш(E/K_n)[p^\infty] < \infty$, (4.4) implies that $\mathrm{rank}_{\mathbb{Z}_p} M_{G_n} = \mathrm{rank}_{\mathbb{Z}} E(K_n)$. Therefore

$$\#Ш(E/K_n)[p^\infty] \ \leq \ p^{\mu p^{dn} + \tau^* np^{(d-1)n} + O(p^{(d-1)n})}$$

where $\tau^* = \tau_Y - \delta_p$ (we should point out that $\tau_Y = \tau_{E,G_\infty}$ in our earlier notation). To further illustrate, we apply this formula to the various specimens studied in §2.5:

• If E is one of the elliptic curves studied in **Example A**, then $d = 3$, $\tau_Y = 1$ and $\delta_p = \frac{p(p^2+p+1)}{(p+1)^3}$. Furthermore, **(DT2)** means that the μ-invariant of $\mathrm{Sel}(k^{\mathrm{cy}})$ is 0, and by [CSS03, Corollary 2.14] this forces $\mu_{G_\infty}(M)$ to vanish under our hypotheses on E and K_∞. Hence, we have the formula

$$\#Ш(E/K_n)[p^\infty] \ \leq \ p^{\frac{(2p^2+2p+1)np^{2n}}{(p+1)^3}+O(p^{2n})}.$$

• If E is one of the elliptic curves studied in **Example B**, then $\tau_Y = \delta_p = 1$. Our formula simplifies to become

$$\#Ш(E/K_n)[p^\infty] \ \leq \ p^{\mu p^{dn}+O(p^{(d-1)n})}.$$

• If E is one of the elliptic curves studied in **Example C**, then $d = 3$, $\tau_Y = 1$ and $\delta_p = \frac{p^{2-s}}{p+1}$. As in the first example one has $\mu = 0$, so our bound reduces to

$$\#Ш(E/K_n)[p^\infty] \ \leq \ p^{\frac{(p+1-p^{2-s})np^{2n}}{p+1}+O(p^{2n})}.$$

• If E is one of the elliptic curves studied in [DT10], then $d = 2$ and $\tau_Y = \delta_p = 1$. Furthermore $\mu = 0$ (as in the case of **Example A**), thence

$$\#Ш(E/K_n)[p^\infty] \ \leq \ p^{O(p^n)}.$$

Finally, we remark that similar bounds on Ш should be possible in the situation where $p \neq 2$ is a prime of bad multiplicative reduction; see [DL15a, Section 3.3] for the formulation of an Iwasawa Main Conjecture in the false Tate curve setting.

Acknowledgements: The majority of this work was carried out during the first named author's visit to Université Laval in May-June 2015, and he would like to thank them for their generous hospitality, and in particular Hugo Chapdelaine. The authors would also like to thank Wei Lu for his comments on an earlier version of this article.

Appendix A. Skew power series rings and characteristic ideals

Let G be a d-dimensional torsion-free p-adic Lie group, given by $H \rtimes \Gamma$, where $\Gamma \cong \mathbb{Z}_p$ and H is a uniform pro-p group. Let $\Lambda(\star)$ be the Iwasawa algebra $\mathbb{Z}_p[[\star]]$ for $\star \in \{G, H, \Gamma\}$. Suppose that $\Gamma = \overline{\langle\gamma\rangle}$ and $H = \overline{\langle\sigma_1, \ldots, \sigma_{d-1}\rangle}$. An element of $\Lambda(G)$ if a (possibly infinite) sum of $(\sigma_1 - 1)^{n_1} \cdots (\sigma_{d-1} - 1)^{n_{d-1}} \cdot (\gamma - 1)^n$ for some non-negative integers $n_1, \ldots, n_{d-1}, n$. We may identify $\Lambda(G)$ with the skew power series ring $R[\![X; \sigma, \delta]\!]$, where $R = \Lambda(H)$, X is an indeterminant, which can be identified with $\gamma - 1$, $\sigma : R \to R$ is a ring homomorphism and $\delta : R \to R$ is a σ-derivation. If $r \in R$,

$$Xr = \sigma(r)X + \delta(r).$$

More generally, for $n \geq 1$, we have

$$X^n r = \sum_{i=0}^{n} (X^n r)_i X^i, \tag{A.1}$$

where $(X^n r)_i$ are elements of R.

For $f = \sum_{i=0}^{\infty} r_i X^i$, we say that f has ***finite reduced order*** if $r_i \in \Lambda(H)^\times$ for some $i \geq 0$. Recall the Weierstrass Preparation Theorem of Venjakob in [Ven03] states that such f admits the factorization

$$f = u \times \tilde{f}$$

where $u \in \Lambda(G)^\times$ and $\tilde{f}$ is a polynomial over $\Lambda(H)$ in X.

Lemma A.1. *Let $M = \Lambda(G)/I$ be a $\Lambda(G)$-module that is finitely generated over $\Lambda(H)$. Then, there exists $f \in I$ that has finite reduced order.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of $\Lambda(H)$. For each element $f \in I$, we may write $f = \sum_{i=0}^{\infty} r_i X^i$. Suppose that f does not have finite reduced order. Then, $r_i \in \mathfrak{m}$ for all i.

Note that we have the following isomorphism of $\Lambda(H)$-modules:

$$\begin{aligned} s_H : \Lambda(G) &\to \Lambda(H)^{\mathbb{N}} \\ \sum_{i=0}^{\infty} a_i X^i &\mapsto (a_i)_{i=0,1,\ldots}. \end{aligned}$$

The image of $\Lambda(G)f$ at the i-th component is

$$\sum_{k+\ell=i, k\leq j} \Lambda(H)(X^j r_\ell)_k.$$

as given by (A.1). Since we assume that $r_\ell \in \mathfrak{m}$ for all ℓ. The $\Lambda(H)$-module above is contained in $\mathfrak{m}$ by [Ven03, Lemma 2.1]. If this is the case for all $f \in I$, the image of M under s_H in $\Lambda(H)^{\mathbb{N}}$ is non-trivial at all components, which contradicts the fact that M is finitely generated over $\Lambda(H)$. Therefore, we conclude that there must exist $f \in I$ with finite reduced order. □

Lemma A.2. *Let $f = \sum_{i=0}^{n} r_i X^i$ be a polynomial in $\Lambda(G)$. There exists $r'_0, \ldots, r'_n \in \Lambda(H)$ such that*

$$f = \sum_{i=0}^{n} X^i r'_i.$$

Proof. Note that for all $m \geq 0$ and $h \in H$, there exists $h' \in H$ such that $\gamma^m h = h'\gamma^m$ by the fact that H is normal in G. Hence the result by identifying X with $\gamma - 1$. □

For all $n \geq 1$, we write $H_n = H^{p^n}$, which is a subgroup of H and H/H^{p^n} is a p-group of order $p^{(d-1)n}$ by the uniformality of H.

Proposition A.3. *Let $M = \Lambda(G)/I$ be a $\Lambda(G)$-module that is finitely generated over $\Lambda(H)$ and that I contains a polynomial f in X of degree τ. Then, M_{H_n} is a finitely generated $\Lambda(\Gamma)$-torsion module. Furthermore, its characteristic power series factorizes into polynomial of degree $\leq \tau$.*

Proof. Note that $\Lambda(G)_{H_n}$ can be identified with $\Lambda(H/H_n \rtimes \Gamma) = \mathbb{Z}_p[H/H_n][\![X; \sigma, \delta]\!]$. We fix a set of coset representatives of H/H_n, say $\{h_i : i = 1, \ldots, p^{(d-1)n}\}$. Each

element of $\Lambda(G)_{H_n}$ can be written as $\sum_i f_i h_i$, where f_i are some elements of $\Lambda(\Gamma)$. As $\Lambda(\Gamma)$-modules, we have the isomorphism

$$\begin{aligned} s_\Gamma : \Lambda(G)_{H_n} &\to \Lambda(\Gamma)^{\oplus p^{dn}} \\ \sum_i f_i h_i &\mapsto (f_i)_{i=1,\dots,p^{(d-1)n}}. \end{aligned}$$

We know that M_{H_n} is a quotient of $\Lambda(G)_{H_n}/I_{H_n}$, so it suffices to prove our result for the latter. Since In particular, $s_\Gamma(\Lambda(G)_{H_n})/s_\Gamma(I_{H_n})$ is a quotient of $\Lambda(\Gamma)^{\oplus p^{dn}}$, it is finitely generated over $\Lambda(\Gamma)$.

By Lemma A.2, the image of f under s_Γ is a polynomial of degree τ at each component. Therefore, $s_\Gamma(\Lambda(G)_{H_n})/s_\Gamma(I_{H_n})$ may be decomposes as a direct sum of $\Lambda(\Gamma)$-modules where each summand is killed by a polynomial of degree d. □

Corollary A.4. *Let $M = \Lambda(G)/I$ be a $\Lambda(G)$-module that is finitely generated over $\Lambda(H)$. Then, M_{H_n} is a finitely generated $\Lambda(\Gamma)$-torsion module for all $n \geq 1$. Furthermore, there exists an integer τ, independent of n, such that the characteristic power series of M_{H_n} factorizes into polynomial of degree $\leq \tau$.*

Proof. By Lemma A.1, I contains an element of f that is of finite reduced order. Venjakob's Weierstrass Preparation Theorem tells us that we may replace f by a polynomial in X, say of degree τ. The result now follows from Proposition A.3. □

References

[Bou65] N. Bourbaki, *Éléments de mathématique. Fasc. XXXI. Algèbre commutative. Chapitre 7: Diviseurs*, Actualités Scientifiques et Industrielles, No. 1314, Hermann, Paris, 1965.

[BV11] David Burns and Otmar Venjakob, *On descent theory and main conjectures in non-commutative Iwasawa theory*, J. Inst. Math. Jussieu **10** (2011), no. 1, 59–118.

[CFKS10] John Coates, Takako Fukaya, Kazuya Kato, and Ramdorai Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*, J. Algebraic Geom. **19** (2010), no. 1, 19–97.

[CM81] Albert A. Cuoco and Paul Monsky, *Class numbers in $\mathbf{Z}_p^d$-extensions*, Math. Ann. **255** (1981), no. 2, 235–258.

[Coa99] John Coates, *Fragments of the GL_2 Iwasawa theory of elliptic curves without complex multiplication*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 1–50.

[Coa02] ———, *Elliptic curves - the crossroads of theory and computation*, Lecture Notes in Computer Science **2369** (2002), 9–19.

[CSS03] John Coates, Peter Schneider, and Ramdorai Sujatha, *Links between cyclotomic and GL_2 Iwasawa theory*, Doc. Math. (2003), no. Extra Vol., 187–215 (electronic), Kazuya Kato's fiftieth birthday.

[DD09] Tim Dokchitser and Vladimir Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), no. 1, 23–71.

[DL15a] Daniel Delbourgo and Antonio Lei, *Non-commutative Iwasawa theory for elliptic curves with multiplicative reduction*, to appear in Math. Proc. Cambridge Phil. Soc., 2015.

[DL15b] ———, *Transition formulae for ranks of abelian varieties*, to appear in Rocky Mountain J. Math., 2015.

[Dok05] Vladimir Dokchitser, *Root numbers of non-abelian twists of elliptic curves*, Proc. London Math. Soc. (3) **91** (2005), no. 2, 300–324, With an appendix by Tom Fisher.

[DP15] Daniel Delbourgo and Lloyd Peters, *Higher order congruences amongst Hasse-Weil L-values*, J. Aust. Math. Soc. **98** (2015), no. 1, 1–38.

[DT10] Henri Darmon and Ye Tian, *Heegner points over towers of Kummer extensions*, Canad. J. Math. **62** (2010), no. 5, 1060–1081.

[Gre03] Ralph Greenberg, *Galois theory for the Selmer group of an abelian variety*, Compositio Math. **136** (2003), no. 3, 255–297.

[Gre11] ———, *Iwasawa theory, projective modules, and modular representations*, Mem. Amer. Math. Soc. **211** (2011), no. 992, vi+185.

[Guo93] Li Guo, *General Selmer groups and critical values of Hecke L-functions*, Math. Ann. **297** (1993), no. 2, 221–233.

[Har79] Michael Harris, *p-adic representations arising from descent on abelian varieties*, Compositio Math. **39** (1979), no. 2, 177–245.

[How02] Susan Howson, *Euler characteristics as invariants of Iwasawa modules*, Proc. London Math. Soc. (3) **85** (2002), no. 3, 634–658.

[HV03] Yoshitaka Hachimori and Otmar Venjakob, *Completely faithful Selmer groups over Kummer extensions*, Doc. Math. (2003), no. Extra Vol., 443–478 (electronic), Kazuya Kato's fiftieth birthday.

[Klo03] Benjamin Klopsch, *Pro-p groups with linear subgroup growth*, Math. Z. **245** (2003), no. 2, 335–370.

[Kob03] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.

[Mat03] Kazuo Matsuno, *Finite Λ-submodules of Selmer groups of abelian varieties over cyclotomic $\mathbb{Z}_p$-extensions*, J. Number Theory **99** (2003), no. 2, 415–443.

[Per11] Guillaume Perbet, *Sur les invariants d'Iwasawa dans les extensions de Lie p-adiques*, Algebra Number Theory **5** (2011), no. 6, 819–848.

[RW06] Jürgen Ritter and Alfred Weiss, *Toward equivariant Iwasawa theory. III*, Math. Ann. **336** (2006), no. 1, 27–49.

[Ser63] Jean-Pierre Serre, *Cohomologie galoisienne*, Cours au Collège de France, vol. 1962, Springer-Verlag, Berlin-Heidelberg-New York, 1962/1963.

[SU14] Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195** (2014), no. 1, 1–277.

[Ven02] Otmar Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc. (JEMS) **4** (2002), no. 3, 271–311.

[Ven03] ———, *A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory*, J. Reine Angew. Math. **559** (2003), 153–191, With an appendix by Denis Vogel.

[Zer04] Sarah Livia Zerbes, *Selmer groups over p-adic Lie extensions. I*, J. London Math. Soc. (2) **70** (2004), no. 3, 586–608.

[Zha04] Shou-Wu Zhang, *Gross-Zagier formula for* GL(2). *II*, Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ., vol. 49, Cambridge Univ. Press, Cambridge, 2004, pp. 191–214.

Daniel Delbourgo, The Department of Mathematics, University of Waikato, Private Bag 3105, Hamilton 3240, New Zealand

E-mail address: delbourg@waikato.ac.nz

Antonio Lei, Département de mathématiques et de statistique, Université Laval, Pavillon Alexandre-Vachon, 1045 avenue de la Médecine, Québec QC, Canada G1V 0A6

E-mail address: antonio.lei@mat.ulaval.ca