# Iwasawa theory of elliptic curves at supersingular primes over $\mathbf{Z}_p$-extensions of number fields

Adrian Iovita and Robert Pollack

October 10, 2006

**Abstract**

In this paper, we make a study of the Iwasawa theory of an elliptic curve at a supersingular prime $p$ along an arbitrary $\mathbf{Z}_p$-extension of a number field $K$ in the case when $p$ splits completely in $K$. Generalizing work of Kobayashi [8] and Perrin-Riou [16], we define restricted Selmer groups and $\lambda^{\pm}$, $\mu^{\pm}$-invariants; we then derive asymptotic formulas describing the growth of the Selmer group in terms of these invariants. To be able to work with non-cyclotomic $\mathbf{Z}_p$-extensions, a new local result is proven that gives a complete description of the formal group of an elliptic curve at a supersingular prime along any ramified $\mathbf{Z}_p$-extension of $\mathbf{Q}_p$.

## 1 Introduction

Over the last few years, much light has been shed on the subject of Iwasawa theory of elliptic curves at supersingular primes. In [9] and [16], asymptotic formulas for the size of $Ш(E/\mathbf{Q}_n)[p^\infty]$ have been established where $\mathbf{Q}_n$ runs through the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. In [8] and [17], a theory of algebraic and analytic $p$-adic $L$-functions is formed that closely parallels the case of ordinary reduction. The methods of all of the above papers depend heavily upon varying the fields considered in the cyclotomic direction. The purpose of this paper is to extend some of these results to a more general collection of $\mathbf{Z}_p$-extensions.

The essential difference in Iwasawa theory between the ordinary and the supersingular case is that, in the later case, the Galois theory of Selmer groups is badly behaved. Namely, if $K_\infty/K$ is a $\mathbf{Z}_p$-extension with layers $K_n$ and $E/K$ is an elliptic curve supersingular at some prime over $p$, then the Selmer group of $E$ over $K_n$ is much smaller than the $\mathrm{Gal}(K_\infty/K_n)$-invariants of the Selmer group of $E$ over $K_\infty$. (In the case of ordinary reduction, these two groups are nearly the same by Mazur's control theorem.) The reason descent fails in the supersingular case boils down to the fact that the trace map on $\widehat{E}$ (the formal group of $E/\mathbf{Q}_p$) is not surjective along a ramified $\mathbf{Z}_p$-extension. Following [13], we make a careful study of how the trace map affects the Galois theory and

we propose an analogous "control theorem" that takes into account the formal group of $E$ (see Theorem 3.1). In the end, this setup allows one to convert the local information of $\widehat{E}$ into global information about the Selmer group of $E$. These considerations are carried out in section 3.

In [8], a complete description of the Galois module structure of $\widehat{E}(k_n)$ is given in terms of generators and relations where $k_n$ runs through the local cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}_p$. The new local result of this paper is a generalization of the above result to any ramified $\mathbf{Z}_p$-extension of $\mathbf{Q}_p$. Namely, if $L_\infty/\mathbf{Q}_p$ is a ramified $\mathbf{Z}_p$-extension with layers $L_n$ then we produce points $d_n \in \widehat{E}(L_n)$ such that $\mathrm{Tr}_{n-1}^n(d_n) = -d_{n-2}$ for $n \geq 2$ where $\mathrm{Tr}_{n-1}^n : \widehat{E}(L_n) \longrightarrow \widehat{E}(L_{n-1})$ is the trace map. Furthermore, $d_n$ and $d_{n-1}$ generate $\widehat{E}(L_n)$ over $\mathbf{Z}_p[\mathrm{Gal}(L_n/\mathbf{Q}_p)]$ (see Theorem 4.5). From this result, we can completely describe the kernel and cokernel of the trace map. This local analysis is done in section 4. Note that the above analysis of $\widehat{E}$ not only gives generators and relations, but the generators satisfy a compatibility as the level varies. It is precisely this compatibility that allows Iwasawa theory in the supersingular case to retain the flavor of the ordinary case.

To be able to apply these local results, we are obliged to work with number fields $K$ for which $p$ splits completely (since the local result assumes that we are working over $\mathbf{Q}_p$). For such $K$ and $p$, we analyze arbitrary $\mathbf{Z}_p$-extensions of $K$. Following [13], we produce algebraic $p$-adic $L$-functions and then using the ideas of [8] and [17] we form plus/minus $L$-functions that actually lie in the Iwasawa algebra (assuming $a_p = 0$). Attached to these $L$-functions, we can associate plus/minus $\mu$ and $\lambda$-invariants.

In section 5, we analyze the case where these $L$-functions are units (i.e. when all the $\mu$ and $\lambda$-invariants are zero). In terms of $E$, this is the case when $E(K)/pE(K) = 0$, $Ш(E/K)[p] = 0$ and $p \nmid \mathrm{Tam}(E/K)$; here $\mathrm{Tam}(E/K)$ represents the Tamagawa factor of $E$ over $K$. (Note that by the Birch and Swinnerton-Dyer conjecture, these hypotheses are equivalent to $\frac{L(E/K,1)}{\Omega_{E/K}}$ being a $p$-adic unit.) Under these strict global hypotheses, we prove that $E(K_n)$ and $Ш(E/K_n)[p^\infty]$ are finite for all $n$. Furthermore, we describe precisely the Galois structure of $Ш(E/K_n)[p^\infty]$ and in particular, produce precise formulas for its size.

When $K = \mathbf{Q}$ and $\frac{L(E/\mathbf{Q},1)}{\Omega_{E/\mathbf{Q}}}$ is a $p$-adic unit, using Kato's Euler system we can verify our algebraic hypotheses and we recover the main result of [9] (see Corollary 5.10). When $K$ is an imaginary quadratic extension of $\mathbf{Q}$ where $p$ splits and $\frac{L(E/K,1)}{\Omega_{E/K}}$ is a $p$-adic unit, we can again verify our algebraic hypotheses via Kato's result and produce exact descriptions of the the size and structure of $Ш(E/K_n)[p^\infty]$ (see Corollary 5.11).

In section 6, we give two different constructions of these plus/minus algebraic $p$-adic $L$-functions. Namely, we follow [13] and use the points $\{d_n\}$ to produce $p$-adic power series. Alternatively, we use the methods of [8] to produce restricted Selmer groups (which behave more like Selmer groups at ordinary primes). These two approaches are related in that the characteristic power se-

ries of the restricted Selmer groups agree with the power series constructed (see Proposition 6.9).

Finally, in section 7, we study the arithmetic of $E$ along the extension $K_\infty/K$. When the coranks of the Selmer groups grow without bound along this extension, the algebraic $p$-adic $L$-functions vanish and the restricted Selmer groups are not cotorsion (over the Iwasawa algebra). In this case, the coranks of these restricted Selmer groups control the rate of growth of the coranks of the Selmer groups at each finite level (see Proposition 7.1). On the other hand, when these coranks remain bounded, we prove that these $L$-functions are non-zero and the restricted Selmer groups are indeed cotorsion. In this case, we produce asymptotic formulas for the growth of these Selmer group in terms of the Iwasawa invariants of the plus/minus $L$-functions as in [16] (see Theorem 7.15).

*Acknowledgments*: We are grateful to Ralph Greenberg for many interesting discussions on subjects pertaining to this paper. We thank Shin-ichi Kobayashi for conversations relating to [8]. We also thank Nigel Byott and Cornelius Greither for very useful email exchanges. Both authors were partially supported by NSF grants.

# 2 Preliminaries

Let $E/\mathbf{Q}$ be an elliptic curve and $p$ an odd supersingular prime for $E$. Let $K/\mathbf{Q}$ be a finite extension and $K_\infty/K$ a $\mathbf{Z}_p$-extension with layers $K_n$. Denote by $\Lambda$ the Iwasawa algebra $\mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$ and let $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$. We will impose the following hypothesis on the splitting type of the prime $p$ in $K_\infty$.

- **Hypothesis S** (for splitting type): The prime $p$ splits completely in $K$ into $d = [K : \mathbf{Q}]$ distinct primes, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_d$. Also, each $\mathfrak{p}_i$ is totally ramified in $K_\infty$.

By abuse of notation, we will denote the unique prime over $\mathfrak{p}_i$ in either $K_n$ or $K_\infty$ simply by $\mathfrak{p}_i$.

**Lemma 2.1.** *Hypothesis (S) implies that* $E(K_{\mathfrak{p}_i})[p] = 0$ *and* $E(K_\infty)[p] = 0$.

*Proof.* We have an exact sequence

$$0 \longrightarrow E_1(\mathbf{Q}_p) \longrightarrow E(\mathbf{Q}_p) \longrightarrow \widetilde{E}(\mathbf{F}_p) \longrightarrow 0 \tag{1}$$

where $\widetilde{E}$ denotes the reduction of $E$ mod $p$ and where $E_1$ is defined by the above sequence. Since $p$ is supersingular, $\widetilde{E}(\mathbf{F}_p)$ has no $p$-torsion (see [21, V. Theorem 3.1]). Furthermore, since $E_1(\mathbf{Q}_p) \cong \widehat{E}(\mathbf{Q}_p)$, we have $E_1(\mathbf{Q}_p)$ has no $p$-torsion (see [21, VII. Proposition 2.2 and IV. Theorem 6.1]). Hence, $E(\mathbf{Q}_p)[p] = 0$. Now since $p$ splits completely in $K$, we have that $K_{\mathfrak{p}_i} \cong \mathbf{Q}_p$ and $E(K_{\mathfrak{p}_i})[p] = 0$.

For the second part, if $E(K_\infty)[p] \neq 0$ then $E(K)[p] = E(K_\infty)[p]^\Gamma \neq 0$ since $\Gamma = \mathrm{Gal}(K_\infty/K)$ is pro-$p$. However, $E(K)[p] \subseteq E(K_{\mathfrak{p}_i})[p] = 0$. □

## 2.1 Selmer groups

For $L$ an algebraic extension of $\mathbf{Q}$ and $v$ a prime of $L$, define

$$\mathcal{H}_E(L_v) = \frac{H^1(L_v, E[p^\infty])}{E(L_v) \otimes \mathbf{Q}_p/\mathbf{Z}_p} \text{ and } \mathcal{P}_E(L) = \prod_v \mathcal{H}_E(L_v)$$

where the product is taken over all primes of $L$. (Here $L_v$ is a union of completions of finite extensions of $\mathbf{Q}$ in $L$.) Then the Selmer group of $E[p^\infty]$ is defined as

$$\mathrm{Sel}(E[p^\infty]/L) = \ker\left(H^1(L, E[p^\infty]) \longrightarrow \mathcal{P}_E(L)\right).$$

The Selmer group of $T_pE$ (the Tate module of $E$) is defined similarly (the cocycles should locally lie in $E(L_v) \otimes \mathbf{Z}_p$) and will be denoted by $\mathrm{Sel}(T_pE/L)$. We then have

$$0 \longrightarrow E(L) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathrm{Sel}(E[p^\infty]/L) \longrightarrow Ш(E/L)[p^\infty] \longrightarrow 0$$

and

$$0 \longrightarrow E(L) \otimes \mathbf{Z}_p \longrightarrow \mathrm{Sel}(T_pE/L) \longrightarrow T_p(Ш(E/L)) \longrightarrow 0 \tag{2}$$

where $Ш(E/L)$ denotes the Tate-Shafarevich group and where $T_p(Ш(E/L)) = \varprojlim_n Ш(E/L)[p^n]$ is its Tate module (which is zero if $Ш(E/L)$ is finite).

We will use the following abbreviations:

$$S_n = \mathrm{Sel}(E[p^\infty]/K_n),\ S = \mathrm{Sel}(E[p^\infty]/K_\infty),$$

$$S_n(T) = \mathrm{Sel}(T_pE/K_n),\ X_n = S_n^\wedge \text{ and } X = S^\wedge$$

where $Y^\wedge = \mathrm{Hom}(Y, \mathbf{Q}_p/\mathbf{Z}_p)$.

## 2.2 Local duality

**Theorem 2.2 (Tate Local Duality).** *Let $v$ be a finite place of $K$. There exists a perfect pairing*

$$H^1(K_v, E[p^\infty]) \times H^1(K_v, T_pE) \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p$$

*induced by cup-product. Furthermore, under this pairing $E(K_v) \otimes \mathbf{Q}_p/\mathbf{Z}_p$ is the exact annihilator of $E(K_v) \otimes \mathbf{Z}_p$, inducing an isomorphism*

$$\mathcal{H}_E(K_v)^\wedge \cong E(K_v) \otimes \mathbf{Z}_p. \tag{3}$$

*Proof.* See [22, Theorem 2.1]. □

We can use local duality to analyze the local factors $\mathcal{H}_E(K_v)$ appearing in the definition of the Selmer group.

**Lemma 2.3.**

1. *If $v \nmid p$ then $\mathcal{H}_E(K_v)$ is finite.*

2. *If $\mathfrak{p}|p$ then $\mathcal{H}_E(K_\mathfrak{p})^\wedge \cong \widehat{E}(K_\mathfrak{p})$ assuming hypothesis (S).*

*Proof.* We have that $E(K_v) \cong \mathbf{Z}_l^{[K_v:\mathbf{Q}_p]} \times T$ where $v \mid l$ and $T$ is a finite group (see [21, VII. Proposition 6.3]). Hence by (3), $\mathcal{H}_E(K_v) \cong (T \otimes \mathbf{Z}_p)^\wedge$ if $l \neq p$ and is therefore finite. For $\mathfrak{p}|p$,

$$\mathcal{H}_E(K_\mathfrak{p})^\wedge \cong E(K_\mathfrak{p}) \otimes \mathbf{Z}_p \cong E_1(K_\mathfrak{p}) \otimes \mathbf{Z}_p \cong \widehat{E}(K_\mathfrak{p})$$

by (1) since $p$ is supersingular and $K_\mathfrak{p} \cong \mathbf{Q}_p$. □

### 2.3 Global duality

Let $\Sigma$ be a finite set of primes of $L$ containing $p$, the infinite primes and all primes of bad reduction for $E$ and let $K_\Sigma$ be the maximal extension of $K$ that is unramified outside of $\Sigma$. We have two exact sequences

$$0 \longrightarrow S_n \longrightarrow H_n \xrightarrow{\gamma_n} \bigoplus_{v \in \Sigma} \mathcal{H}_E(K_{n,v}) \tag{4}$$

and

$$0 \longrightarrow S_{n,\Sigma}(T) \longrightarrow S_n(T) \longrightarrow \bigoplus_{v \in \Sigma} E(K_v) \otimes \mathbf{Z}_p \tag{5}$$

where $H_n = H^1(K_\Sigma/K_n, E[p^\infty])$ and where $S_{n,\Sigma}(T)$ is defined by the second sequence. By Tate local duality, $E(K_v) \otimes \mathbf{Z}_p$ is dual to $\mathcal{H}_E(K_{n,v})$. Global duality asserts that these two sequences splice into a five term exact sequence.

**Theorem 2.4 (Global duality).** *The sequence*

$$0 \longrightarrow S_n \longrightarrow H_n \xrightarrow{\gamma_n} \bigoplus_{v \in \Sigma} \mathcal{H}_E(K_{n,v}) \longrightarrow S_n(T)^\wedge \longrightarrow S_{n,\Sigma}(T)^\wedge \longrightarrow 0$$

*is exact where the first two maps come from (4) and the last two maps come from (5) and Tate local duality.*

*Proof.* For a statement of global duality in this form see [19, Section 1.7]). □

## 3 A control theorem in the supersingular case

When $p$ is an ordinary prime for $E$, Mazur proved that the natural map of restriction between $S_n$ and $S^{\Gamma_n}$ has finite kernel and cokernel of size bounded independent of $n$ (see [11]). A theorem of this form, that compares $S_n$ to $S^{\Gamma_n}$ is often called a control theorem. A key ingredient needed for this result is that the trace map on the formal group of $E$ is surjective along a ramified $\mathbf{Z}_p$-extension.

In the supersingular case, the trace fails to be surjective (see [10]). In fact, the $\mathbf{Z}_p$-corank of $\operatorname{coker}\left(S_n \longrightarrow S^{\Gamma_n}\right)$ grows without bound. In this section, we

will produce an analogous control theorem that describes this cokernel in terms of the formal group of $E$. Throughout this section, we will be assuming (S).

Let $s_n : S_n \longrightarrow S^{\Gamma_n}$ and $r_{n,v} : \mathcal{H}_E(K_{n,v}) \longrightarrow \mathcal{H}_E(K_{\infty,v'})$ denote the natural restriction maps with $v'$ some prime of $K_\infty$ over $v$. The following theorem can be thought of as a control theorem in the supersingular case.

**Theorem 3.1.** *We have a four term exact sequence*

$$0 \longrightarrow \frac{S_n(T)}{S_{n,\Sigma}(T)} \longrightarrow \widehat{E}(K_{n,p}) \times B_n \longrightarrow X_{\Gamma_n} \xrightarrow{x_n} X_n \longrightarrow 0$$

*where* $x_n = s_n^\wedge$, $\widehat{E}(K_{n,p}) = \oplus_{j=1}^d \widehat{E}(K_{n,\mathfrak{p}_j})$ *and* $B_n$ *is a finite group whose size is bounded by the p-part of* $\mathrm{Tam}(E/K_n)$.

To prove this theorem, we will need to control the kernel and cokernel of $s_n$. We follow the methods of [2] and [3] and direct the reader to these articles for more details.

**Proposition 3.2.** *We have*

1. $\ker(s_n) = 0$
2. $\mathrm{coker}(s_n) \cong \mathrm{im}(\gamma_n) \cap (\oplus_{v \in \Sigma} \ker(r_{n,v}))$

*where* $\gamma_n$ *is defined in (4).*

*Proof.* This proposition follows from applying the snake lemma to the diagram defining $S_n$ and $S$. See [2, Chapter 4] especially Lemma 4.2 and 4.3 for details. □

The following proposition describes $\ker(r_{n,v})$. The case of primes dividing $p$ behaves quite differently from primes not over $p$.

**Proposition 3.3.** *We have*

1. *For* $v \nmid p$, $\ker(r_{n,v})$ *is finite. If* $v$ *splits completely in* $K_\infty$ *then* $\ker(r_{n,v}) = 0$*; otherwise it has size equal to* $\mathrm{Tam}(E/K_{n,v})$ *up to a p-adic unit.*
2. *For* $\mathfrak{p}|p$, $\ker(r_{n,\mathfrak{p}}) = \mathcal{H}_E(K_{n,\mathfrak{p}})$.

*Proof.* For part (1), see the comments after Lemma 3.3 in [3]. For part (2), we have

$$\mathcal{H}_E(K_{\infty,\mathfrak{p}}) = \varinjlim_n \mathcal{H}_E(K_{n,\mathfrak{p}}) = \left( \varprojlim_n \widehat{E}(K_{n,\mathfrak{p}}) \right)^\wedge$$

where the last inverse limit is taken with respect to the trace map. However, there are no universal norms for $\widehat{E}$ along the ramified $\mathbf{Z}_p$-extension $K_{\infty,\mathfrak{p}}/K_\mathfrak{p}$ since $p$ is supersingular (see [10]). Therefore, $\mathcal{H}_E(K_{\infty,\mathfrak{p}}) = 0$ and $\ker(r_{n,\mathfrak{p}}) = \mathcal{H}_E(K_{n,\mathfrak{p}})$. □

**Remark 3.4.** The fact that $\ker(r_{n,\mathfrak{p}})$ equals all of $\mathcal{H}_E(K_{n,\mathfrak{p}})$ is the essential difference between the ordinary case and the supersingular case and is the reason why the cokernel of $s_n$ grows without bound.

*Proof of Theorem 3.1.* To control $\operatorname{coker}(s_n)$ we will need to understand how $\operatorname{im}(\gamma_n)$ relates to $\oplus_{v\in\Sigma}\ker(r_{n,v})$. To ease notation, let $\mathcal{H}_v = \oplus_{v\nmid p}\mathcal{H}_E(K_{n,v})$ and $\mathcal{H}_p = \oplus_{\mathfrak{p}|p}\mathcal{H}_E(K_{n,\mathfrak{p}})$. By global duality

$$\operatorname{im}(\gamma_n) = \ker\left(\mathcal{H}_v \times \mathcal{H}_p \longrightarrow S_n(T)^\wedge\right).$$

For $v \nmid p$, the image of $\mathcal{H}_E(K_{n,v})$ in $S_n(T)^\wedge$ is zero (the former is a finite group by Lemma 2.3 and the later is a free module by (S) and (2) ). Hence, we can write $\operatorname{im}(\gamma_n) = \mathcal{H}_v \times A$ with $A \subseteq \mathcal{H}_p$ and applying global duality again yields

$$\frac{\mathcal{H}_p}{A} = \left(\frac{S_n(T)}{S_{n,\Sigma}(T)}\right)^\wedge. \tag{6}$$

By Proposition 3.3, $\oplus_{\mathfrak{p}|p}\ker(r_{n,\mathfrak{p}}) = \mathcal{H}_p$ and hence

$$\operatorname{im}(\gamma_n) \cap (\oplus_{v\in\Sigma}\ker(r_{n,v})) \cong \left(\oplus_{v\nmid p}\ker(r_{n,v})\right) \times A.$$

Therefore, by Proposition 3.2 and (6), we have

$$0 \longrightarrow \operatorname{coker}(s_n) \longrightarrow \left(\oplus_{v\nmid p}\ker(r_{n,v})\right) \times \mathcal{H}_p \longrightarrow \left(\frac{S_n(T)}{S_{n,\Sigma}(T)}\right)^\wedge \longrightarrow 0. \tag{7}$$

By Lemma 2.3, $\mathcal{H}_p^\wedge \cong \widehat{E}(K_{n,p})$ and by Proposition 3.3, $\#\ker(r_{n,v})$ is bounded by the $p$-part of $\operatorname{Tam}(E/K_{n,v})$. Therefore, dualizing (7) yields the theorem. □

# 4 Structure of some formal groups

## 4.1 Lubin-Tate formal groups

$\mathfrak{p}_n$ be the unique prime of completion of $K_n$ Let $p > 2$ be a prime and $\{L_n\}_{n\geq 0}$ with $\mathbf{Q}_p = L_0 \subset L_1 \subset L_2 ... \subset L_\infty = \cup_n L_n$ be a tower of fields such that $L_\infty$ is a totally ramified $\mathbf{Z}_p$-extension of $\mathbf{Q}_p$. Let $k_{n+1} := L_n[\mu_p]$ for $n \geq 0$ and $k_\infty = \cup_n k_n = L_\infty[\mu_p]$. Here, if $M$ is a field by $M[\mu_p]$ we mean the extension of $M$ obtained by adjoining to $M$ the $p$-th roots of unity in some fixed algebraic closure of $M$. Then $k_\infty$ is a $\mathbf{Z}_p^\times$-extension of $\mathbf{Q}_p$ and the group of its universal norms is generated by a uniformizer of $\mathbf{Z}_p$, say $\pi$, such that $\operatorname{ord}_p\left(\frac{\pi}{p} - 1\right) > 0$. Now we would like to carefully choose a Lubin-Tate formal group (by choosing a "lift of Frobenius" corresponding to $\pi$) whose $\pi^n$-division points generate $k_n$ over $\mathbf{Q}_p$.

Namely, let us define

$$f(X) := \pi X + \sum_{i=2}^{p} \frac{p(p-1)\cdots(p-i+1)}{i!} X^i \in \mathbf{Z}_p[[X]].$$

Then $f(X)$ is a lift of Frobenius corresponding to $\pi$, that is $f(X) = \pi X \pmod{\deg 2}$ and $f(X) = X^p \pmod{p}$ and moreover it satisfies the properties:

1. $f(X) = (X+1)^p - 1 \pmod{p^2}$
2. the coefficient of $X^{p-1}$ is $p$.

We call this a **good lift** of Frobenius.

**Lemma 4.1.** *For $\pi$ as above and for a good lift of Frobenius $f(X)$ let us denote by $F_f(X,Y)$ the corresponding formal group law. We have $F_f(X,Y) = X+Y+XY \pmod{p}$ and $[a]_f(X) = (X+1)^a - 1 \pmod{p}$ for all $a \in \mathbf{Z}_p$.*

*Proof.* Let us write $f(X) = (X+1)^p - 1 + p^2 g(X)$ where $g(X) \in \mathbf{Z}_p[[X]]$. Then $F_f(X,Y)$ (respectively $[a]_f(X)$) is the unique power series with coefficients in $\mathbf{Z}_p$ such that $F_f(X,Y) = X+Y \pmod{\deg 2}$ and $f(F_f(X,Y)) = F_f(f(X), f(Y))$ (resp. such that $[a]_f(X) = aX \pmod{\deg 2}$ and $f([a]_f(X)) = [a]_f(f(X))$).

Writing the identity for $F_f$ we get:

$$(F_f(X,Y)+1)^p - 1 + p^2 g(F_f(X,Y)) = F_f((X+1)^p - 1, (Y+1)^p - 1) + p^2 G(X,Y)$$

for some $G(X,Y) \in \mathbf{Z}_p[[X,Y]]$. Therefore $F_f(X,Y)$ satisfies the identity

$$(F_f(X,Y)+1)^p - 1 = F_f((X+1)^p - 1, (Y+1)^p - 1) \pmod{p^2}. \tag{8}$$

If we write

$$F_f(X,Y) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^j \tag{9}$$

with $a_{ij} \in \mathbf{Z}/p^2\mathbf{Z}$, the coefficients $a_{ij}$ are obtained by identifying the coefficients of the monomials of same degree in (8) and solving for $a_{ij}$. This process of solving for $a_{ij}$ requires division by a multiple of $p \pmod{p^2}$ and therefore $a_{ij}$ is only uniquely determined $\pmod{p}$. In other words, any power series as in (9) above, satisfying (8), is unique $\pmod{p}$. But the power series $X+Y+XY$ satisfies these conditions and so we have $F_f(X,Y) = X+Y+XY \pmod{p}$. The proof for $[a]_f(X)$ is similar. □

Let us fix for the rest of this section $f(X)$ and $F_f(X,Y)$ as in Lemma 4.1 and let $[i]_f(X) = \sum_{j=1}^{\infty} a_j(i) X^j$, for $i = 1, 2, ..., p-1$.

**Corollary 4.2.** *We have that the determinant $(a_j(i))_{1 \leq i \leq p-1, 1 \leq j \leq p-1}$ is in $\mathbf{Z}_p^\times$.*

*Proof.* From Lemma 4.1, we see that $(a_j(i))$ is a lower triangular matrix modulo $p$ with ones along the diagonal. Hence, $\det(a_i(j)) \in \mathbf{Z}_p^\times$. □

Let us denote by $\mathcal{O}_n$ the ring of integers in $k_n$ and by $M_n$ its maximal ideal. For every $n$ we have $k_n = \mathbf{Q}_p[F_f[\pi^n]]$.

**Corollary 4.3.** *Let $\beta \in F_f[\pi^n] - F_f[\pi^{n-1}]$. Then for every $1 \leq b \leq p-1$ we can find a linear combination with coefficients in $\mathbf{Z}_p$ of $[1]_f(\beta), [2]_f(\beta), ..., [p-1]_f(\beta)$ which has the form $\beta^b + \beta^p V$ with $V \in \mathcal{O}_n$.*

*Proof.* Apply Corollary 4.2. □

For every $s \in \mathbf{Z}^{\geq 1}$ we denote by $G_s(f)$ the $\mathbf{Z}_p$-submodule of $M_s$ generated by $F_f[\pi^s]$. The main result of this section is the following proposition.

**Proposition 4.4.**

1. *We have $G_n(f) = M_n$ for all $n \geq 1$.*
2. *Each $\beta \in F_f[\pi^n] - F_f[\pi^{n-1}]$ generates $M_n/M_{n-1}$ as a $\mathbf{Z}_p[\mathrm{Gal}(k_n/\mathbf{Q}_p)]$-module.*

*Proof.* As $F_f[\pi^{n-1}] \subset M_{n-1}$ and as $\mathrm{Gal}(k_n/\mathbf{Q}_p)(\beta) = F_f[\pi^n] - F_f[\pi^{n-1}]$ part (1) implies part (2).

To prove part (1), let us first remark that $p \in G_s(f)$ for all $s$, because $\mathrm{Tr}_{k_s/k_{s-1}}(\beta) = -p$ for $\beta \in F_f[\pi^s] - F_f[\pi^{s-1}]$. Hence in order to show that $G_n(f) = M_n$, we need to show that $G_n(f)$ contains elements of valuation $\dfrac{b}{p^n - p^{n-1}}$ for all $1 \leq b \leq p^n - p^{n-1} - 1$. So far from Corollary 4.3 we know that $G_n(f)$ contains elements of valuation $\dfrac{b}{p^n - p^{n-1}}$ for all $0 \leq b \leq p - 1$.

Let us formulate the statement $P(s)$ depending on $s \geq 1$:

$P(s)$: *For all $n \geq s$, all $\beta \in F_f[\pi^n] - F_f[\pi^{n-1}]$ and all $b$ with $0 \leq b \leq p^s - p^{s-1} - 1$, there is a linear combination with coefficients in $\mathbf{Z}_p$ of $[1]_f(\beta), [2]_f(\beta), ..., [p^s - p^{s-1} - 1]_f(\beta)$ which has the form $u\beta^b + \beta^{b+1}V$ where $u \in \mathcal{O}_n^\times$ and $V \in \mathcal{O}_n$.*

Notice that if for some $s \geq 1$, $P(s)$ is true then $G_s(f) = M_s$, i.e. part (1) is true for that $s$. We will prove that the statement $P(s)$ is true for all $s \geq 1$ by induction on $s$. The statement is true for $s = 1$ by Corollary 4.3.

Let us now suppose that $P(t)$ is true for all $1 \leq t < s$. Let $n \geq s$, $\beta \in F_f[\pi^n] - F_f[\pi^{n-1}]$ and fix $b$ with $0 \leq b \leq p^s - p^{s-1} - 1$. Let us denote $\gamma := [p]_f(\beta)$; then as $p = \pi u$ with $u \in \mathbf{Z}_p^\times$, $\gamma \in F_f[\pi^{n-1}] - F_f[\pi^{n-2}]$. Moreover, from Lemma 4.1 it follows that we have

$$[i + pj]_f(\beta) - [i]_f(\beta) - [j]_f(\gamma) = [i]_f(\beta)[j]_f(\gamma) + pU, \tag{10}$$

where $U \in \mathcal{O}_n$, $0 \leq i \leq p - 1$ and $0 \leq j \leq p^{s-1} - p^{s-2} - 1$.

Now use the induction hypothesis on $\gamma$ to get that a linear combination with coefficients in $\mathbf{Z}_p$ of $[1]_f(\gamma), [2]_f(\gamma), ..., [p^{s-1} - p^{s-2} - 1]_f(\gamma)$ has the form

$$(v\gamma^c + \gamma^{c+1}W) + pU_1$$

with $v \in \mathcal{O}_{n-1}^\times$, $W \in \mathcal{O}_{n-1}$ and $U_1 \in \mathcal{O}_n$. Then for each $i$ between 0 and $p - 1$, by (10), there is a linear combination with coefficients in $\mathbf{Z}_p$ of the elements $[1]_f(\beta), [2]_f(\beta), ..., [p^s - p^{s-1} - 1]_f(\beta)$ having the form

$$[i]_f(\beta)(v\gamma^c + \gamma^{c+1}W) + pU_2$$

with $U_2 \in \mathcal{O}_n$. Now again use Corollary 4.3 to get a linear combination over $\mathbf{Z}_p$ of $[1]_f(\beta), [2]_f(\beta), ..., [p^s - p^{s-1} - 1]_f(\beta)$ with the form

$$(\beta^a + \beta^p T)(v\gamma^c + \gamma^{c+1} W) + pU_3$$

with $T, U_3 \in \mathcal{O}_n$. We then have that a linear combination with coefficients in $\mathbf{Z}_p$ of the desired elements has the form

$$v\beta^a\gamma^c + \beta^p\gamma^c V_1 = u\beta^b + \beta^{p(c+1)} V_2$$

where $u = v\dfrac{\gamma^c}{\beta^{pc}} \in \mathcal{O}_n^\times$ and $V_1, V_2 \in \mathcal{O}_n$. This proves that $P(s)$ is true for all $s$ and hence $G_s(f) = M_s$ for all $s$. □

## 4.2 Formal groups of elliptic curves with supersingular reduction

Let $E/\mathbf{Q}_p$ be an elliptic curve with supersingular reduction and suppose that $a_p = 0$. Let us denote, as in the previous sections, by $\widehat{E}$ the formal group of $E$, i.e. the formal scheme over $\mathbf{Z}_p$ which is the formal completion of the Néron model of $E$ at the identity of its special fiber. Let $L_\infty/\mathbf{Q}_p$ be a ramified $\mathbf{Z}_p$-extension with layers $L_n$. We denote by $\mathrm{Tr}_{n-1}^n : \widehat{E}(L_n) \longrightarrow \widehat{E}(L_{n-1})$ the trace with respect to the group-law $\widehat{E}(X, Y)$. Then the following is the main result of this section.

**Theorem 4.5.** *For $n \geq 0$ there exists $d_n \in \widehat{E}(L_n)$ such that*

1. $\mathrm{Tr}_{n-1}^n\, d_n = -d_{n-2}$
2. $\mathrm{Tr}_0^1\, d_1 = u \cdot d_0$ *with* $u \in \mathbf{Z}_p^\times$.
3. *For $n \geq 1$, $\widehat{E}(L_n)$ is generated by $d_n$ and $d_{n-1}$ as a $\mathbf{Z}_p[\mathrm{Gal}(L_n/\mathbf{Q}_p)]$-module. Also, $d_0$ generates $\widehat{E}(\mathbf{Q}_p)$.*

The proof of this theorem will fill the rest of this section. Let us consider the $\mathbf{Z}_p^\times$-extension $k_\infty$ attached to $L_\infty$ as in the section 4.1 and denote by $\pi$ the generator of the group of universal norms of the extension $k_\infty/\mathbf{Q}_p$ which has positive valuation. We will first construct a sequence of points $c_n \in \widehat{E}(k_n)$ which satisfy the same trace relations. For this we will use Honda-theory as in section 8 of [8] and we will choose a particular representative of the isomorphism class of $\widehat{E}$ whose logarithm has a certain form. More precisely, let $f(X)$ be a "good lift" of Frobeius attached to $\pi$ as in section 4.1 and let

$$\ell(X) := \sum_{k=0}^{\infty} (-1)^k \frac{f^{(2k)}(X)}{p^k} \in \mathbf{Q}_p[[X]],$$

where $f^{(0)}(X) = X$ and if $n \geq 1$ is an integer we set $f^{(n)}(X) := f(f^{(n-1)}(X))$. By Honda theory, if we denote by $G(X, Y) := \ell^{-1}(\ell(X) + \ell(Y))$ then $\widehat{E}$ and $G$

are isomorphic formal groups over $\mathbf{Z}_p$ and the logarithm of $G$ is $\ell(X)$. For the rest of this section we will identify these two formal groups and will write $\widehat{E}$ for $G$. We first have

**Lemma 4.6.** *The formal group $\widehat{E}$ has no $p$-power torsion points in $k_n$ for all $n \geq 0$.*

*Proof.* The proof is the same, modulo the obvious adjustments, as the proof of Proposition 8.8 of [8]. □

**Corollary 4.7.** *The group homomorphism $\ell : \widehat{E}(k_n) \longrightarrow \widehat{\mathbb{G}}_a(k_n)$ is injective.*

*Proof.* This corollary follows immediately from Lemma 4.6 since the kernel of the logarithm of a formal group is composed precisely of the elements of finite order. □

Let $F_f(X,Y)$ be the Lubin-Tate formal group over $\mathbf{Z}_p$ attached to the lift of Frobenius $f(X)$ as in section 4.1 and let us choose a $\pi$-sequence $\{e_n\}_{n\geq 0}$ in $k_\infty$, i.e. $e_n \in F_f[\pi^n] - F_f[\pi^{n-1}]$ such that $f(e_n) = e_{n-1}$ for all $n \geq 1$. Let $\epsilon \in p\mathbf{Z}_p$ be such that $\ell(\epsilon) = \dfrac{p}{p+1}$ and define $c_n \in \widehat{E}(k_n)$ to be $c_n = e_n[+]_{\widehat{E}}\epsilon$ for all $n \geq 0$. The following lemma computes the traces of the $c_n$.

**Lemma 4.8.** *For $n \geq 1$, we have $\mathrm{Tr}^n_{n-1}(c_n) = -c_{n-2}$ where here $\mathrm{Tr}^n_{n-1}$ is the trace from $\widehat{E}(k_n)$ to $\widehat{E}(k_{n-1})$. For $n = 1$, $\mathrm{Tr}^1_0(c_1) = u \cdot c_0$ with $u \in \mathbf{Z}_p^\times$.*

*Proof.* Everything is set up so that the proof follows formally the same steps as the proof of Lemma 8.10 in [8]. Namely, as $\ell$ is injective on $\widehat{E}(k_\infty)$, it is enough to show that the relation holds after applying $\ell$ to both sides of the equality. For $n \geq 2$ we have

$$\begin{aligned}\ell(\mathrm{Tr}^n_{n-1}(c_n)) &= \mathrm{Tr}_{k_n/k_{n-1}}\left(\frac{p}{p+1} + \sum_{k=0}^{\infty}(-1)^k \frac{e_{n-2k}}{p^k}\right) \\ &= \frac{p^2}{p+1} - p + p\sum_{k=1}^{\infty}(-1)^k \frac{e_{n-2k}}{p^k} = -\ell(c_{n-2})\end{aligned}$$

where $e_k = 0$ for $k$ negative. The calculation is similar for $n = 1$. □

**Proposition 4.9.** *We have $\ell(M_n) \subset M_n + k_{n-1}$ and $\ell$ induces an isomorphism*

$$\widehat{E}(k_n)/\widehat{E}(k_{n-1}) \cong \ell(M_n)/\ell(M_{n-1}) \cong M_n/M_{n-1}.$$

*In particular $c_n$ generates $\widehat{E}(k_n)/\widehat{E}(k_{n-1})$ as a $\mathbf{Z}_p[\mathrm{Gal}(k_n/\mathbf{Q}_p)]$-module.*

*Proof.* The proof follows the steps of the proof of Proposition 8.12 of [8]. The main new ingredient is Proposition 4.4. □

**Corollary 4.10.** *For $n \geq 1$, $c_n$ and $c_{n-1}$ generates $\widehat{E}(k_n)$ as a $\mathbf{Z}_p[\mathrm{Gal}(k_n/\mathbf{Q}_p)]$-module.*

*Proof.* This follows easily from Proposition 4.9 and the trace relations satisfied by the $c_n$ (see Lemma 4.8). □

*Proof of Theorem 4.5.* Let $d_n := \mathrm{Tr}_{k_{n+1}/L_n}(c_{n+1}) \in \widehat{E}(L_n)$. Then it is easy to see that $\mathrm{Tr}^n_{n-1}(d_n) = -d_{n-2}$ for $n \geq 2$; so we only have to show that $d_n$ and $d_{n-1}$ generate $\widehat{E}(L_n)$ as a $\mathbf{Z}_p[\mathrm{Gal}(L_n/\mathbf{Q}_p)]$-module for $n \geq 1$. Let us denote by $\Delta$ the torsion subgroup of $\mathbf{Z}_p^\times = \mathrm{Gal}(k_\infty/\mathbf{Q}_p)$. Then we have an isomorphism of $\mathbf{Z}_p[\mathrm{Gal}(k_{n+1}/\mathbf{Q}_p)]$-modules:

$$\widehat{E}(k_{n+1}) = \oplus_{\chi \in \widehat{\Delta}} \widehat{E}(k_{n+1})^\chi$$

where $\widehat{\Delta}$ is the group of characters of $\Delta$ and $\widehat{E}(k_{n+1})^\chi$ is the maximal subgroup of $\widehat{E}(k_{n+1})$ on which $\delta \in \Delta$ acts by multiplication by $\chi(\delta)$. The isomorphism is given by $x \mapsto (x^\chi)_{\chi \in \widehat{\Delta}}$ where $x^\chi := \dfrac{1}{p-1} \displaystyle\sum_{\delta \in \Delta} \chi(\delta) x^\delta$. Since $c_{n+1}$ and $c_n$ generate $\widehat{E}(k_{n+1})$ as a $\mathbf{Z}_p[\mathrm{Gal}(k_{n+1}/\mathbf{Q}_p)]$-module, for every $\chi \in \widehat{\Delta}$, $c^\chi_{n+1}$ and $c^\chi_n$ generate $\widehat{E}(k_{n+1})^\chi$ over the same ring. In particular for $\chi$ equal to the trivial character, we have $\widehat{E}(k_{n+1})^\chi = \widehat{E}(L_n)$, $(p-1)(c^\chi_{n+1}) = d_n$, $(p-1)(c^\chi_n) = d_{n-1}$ and the conclusion follows. □

The following proposition describes the relations that the $d_n$ satisfy. We first introduce some notation that will be used throughout the remainder of the paper. Let $\Phi_n(X) := \displaystyle\sum_{i=0}^{p-1} X^{ip^{n-1}}$ be the $n$-th cyclotomic polynomial, $\xi_n = \Phi_n(1+X)$ and $\omega_n(X) := (X+1)^{p^n} - 1$. Also set,

$$\tilde{\omega}^+_n := \prod_{\substack{1 \leq m \leq n \\ m \text{ even}}} \Phi_m(1+X), \qquad \tilde{\omega}^-_n := \prod_{\substack{1 \leq m \leq n \\ m \text{ odd}}} \Phi_m(1+X),$$

$\omega^+_n = X \cdot \tilde{\omega}^+_n$ and $\omega^-_n = X \cdot \tilde{\omega}^-_n$. Note that $\omega_n = X \cdot \tilde{\omega}^+_n \cdot \tilde{\omega}^-_n$. Finally, set $\Lambda_n = \Lambda/\omega_n\Lambda$.

**Proposition 4.11.** *There is an exact sequence*

$$0 \longrightarrow \widehat{E}(\mathbf{Q}_p) \longrightarrow d_n\Lambda_n \oplus d_{n-1}\Lambda_{n-1} \longrightarrow \widehat{E}(L_n) \longrightarrow 0$$

*where the first map is the diagonal embedding (note that $\widehat{E}(\mathbf{Q}_p) \subseteq d_k\Lambda_k$ for each $k$) and the second map is $(a,b) \mapsto a - b$. Furthermore, $d_n\Lambda_n \cong \Lambda/\omega^\varepsilon_n$ with $\varepsilon = (-1)^n$.*

*Proof.* The exact sequence comes from Proposition 8.13 of [8]. For the second part, we have that

$$\omega^\varepsilon_n d_n = \omega^\varepsilon_{n-2}(\xi_n \cdot d_n) = \omega^\varepsilon_{n-2} \mathrm{Tr}^n_{n-1}(d_n) = -\omega^\varepsilon_{n-2} d_{n-2} = \cdots = \pm X d_0 = 0.$$

Hence, there is a surjective map $\Lambda_n/\omega_n^\varepsilon \longrightarrow d_n\Lambda_n$ obtained by sending 1 to $d_n$. To see that this map is injective, it is enough to note that $\Lambda_n/\omega_n^\varepsilon$ and $d_n\Lambda_n$ are free $\mathbf{Z}_p$-modules of the same rank (which follows from the above exact sequence). □

**Corollary 4.12.** *For $n \geq 0$ and $\varepsilon = (-1)^n$,*

1. $\ker(\mathrm{Tr}_{n-1}^n) \cong \omega_{n-2}^\varepsilon d_n\Lambda_n$.
2. $\mathrm{coker}(\mathrm{Tr}_{n-1}^n)$ *is a $p$-group with $p$-rank equal to $q_n$ where*

$$q_n = \begin{cases} p^{n-1} - p^{n-2} + \cdots + p - 1 & 2|n \\ p^{n-1} - p^{n-2} + \cdots + p^2 - p & 2 \nmid n \end{cases}.$$

*Proof.* By Proposition 4.11, we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widehat{E}(\mathbf{Q}_p) & \longrightarrow & d_n\Lambda_n \oplus d_{n-1}\Lambda_{n-1} & \longrightarrow & \widehat{E}(L_n) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \times p} & & \downarrow & & \downarrow{\scriptstyle \mathrm{Tr}_{n-1}^n} & & \\ 0 & \longrightarrow & \widehat{E}(\mathbf{Q}_p) & \longrightarrow & d_{n-1}\Lambda_{n-1} \oplus d_{n-2}\Lambda_{n-2} & \longrightarrow & \widehat{E}(L_{n-1}) & \longrightarrow & 0 \end{array}$$

where the middle vertical map sends $(d_n, 0)$ to $(0, -d_{n-2})$ and $(0, d_{n-1})$ to $(p \cdot d_{n-1}, 0)$. Then applying the snake lemma and Proposition 4.11 yields the result. □

## 4.3 The plus/minus Perrin-Riou map

We follow closely section 8 of [8] except that we work with a $\mathbf{Z}_p$-extension instead of a $\mathbf{Z}_p^\times$-extension. This produces a certain shift in the numbering but the main arguments are formally the same. Let $T$ be the $p$-adic Tate-module of $E$ considered as a $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-module. The Kummer map $\widehat{E}(L_n) \longrightarrow H^1(L_n, T)$ together with cup product and the Weil pairing induces

$$(\ ,\ )_n : \widehat{E}(L_n) \times H^1(L_n, T) \longrightarrow H^2(L_n, \mathbf{Z}_p(1)) \cong \mathbf{Z}_p.$$

Let $G_n := \mathrm{Gal}(L_n/\mathbf{Q}_p) \cong \mathbf{Z}/p^n\mathbf{Z}$ and for every $x \in \widehat{E}(L_n)$ let us define the morphism $P_{x,n} : H^1(L_n, T) \longrightarrow \mathbf{Z}_p[G_n]$ by $P_{x,n}(z) = \sum_{\sigma \in G_n} (x^\sigma, z)_n \sigma$. Both $H^1(L_n, T)$ and $\mathbf{Z}_p[G_n]$ are naturally $G_n$-modules and $P_{x,n}$ is $G_n$-equivariant for all $x$ and $n$. Moreover, for every $x \in \widehat{E}(L_n)$ and $n \geq 1$ the following diagram

$$\begin{array}{ccc} H^1(L_n, T) & \xrightarrow{P_{x,n}} & \mathbf{Z}_p[G_n] \\ \downarrow & & \downarrow \\ H^1(L_{n-1}, T) & \xrightarrow{P_{\mathrm{Tr}_{n-1}^n(x),n-1}} & \mathbf{Z}_p[G_{n-1}] \end{array}$$

is commutative. Using the sequence of points $\{d_n\}_n$ we consider two subsequences: $d_n^+ = d_n$ if $n$ is even and $d_n^+ = d_{n-1}$ if $n$ is odd and similarly $d_n^- = d_{n-1}$ if $n$ is even and $d_n^- = d_n$ if $n$ is odd. We set $P_n^{\pm} := (-1)^{[\frac{n+1}{2}]} P_{d_n^{\pm},n}$ and define

$$\widehat{E}^+(L_n) := \{P \in \widehat{E}(L_n) \mid \mathrm{Tr}_m^n(P) \in \widehat{E}(L_{m-1}) \text{ for all } 1 \leq m \leq n, m \text{ odd}\};$$

$$\widehat{E}^-(L_n) := \{P \in \widehat{E}(L_n) \mid \mathrm{Tr}_m^n(P) \in \widehat{E}(L_{m-1}) \text{ for all } 1 \leq m \leq n, m \text{ even}\}.$$

**Lemma 4.13.** *$d_n^{\pm}$ generates $\widehat{E}^{\pm}(L_n)$ as a $\mathbf{Z}_p[G_n]$-module.*

*Proof.* The proof is the same as the proof of Proposition 8.13 of [8]. □

We define $H^1_{\pm}(L_n, T) := \left(\widehat{E}(L_n)^{\pm} \otimes \mathbf{Q}_p/\mathbf{Z}_p\right)^{\perp} \subset H^1(L_n, T)$ where we think of $\widehat{E}(L_n)^{\pm} \otimes \mathbf{Q}_p/\mathbf{Z}_p$ as embedded in $H^1(L_n, V/T)$ by the Kummer map with $V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. The orthogonal complement is taken with respect to the Tate pairing $\langle\ ,\ \rangle : H^1(L_n, T) \times H^1(L_n, V/T) \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p$.

**Lemma 4.14.**

1. $\ker(P_n^{\pm}) = H^1_{\pm}(L_n, T)$.
2. *The image of $P_n^{\pm}$ is contained in $\tilde{\omega}_n^{\mp}\Lambda_n$.*

*Proof.* The first part is clear from Lemma 4.13. For the second part, we have that

$$\omega_n^{\pm} P_n^{\pm}(z) = \omega_n^{\pm} \sum_{\sigma \in G_n} \left(\left(d_n^{\pm}\right)^{\sigma}, z\right)_n \sigma = \sum_{\sigma \in G_n} \left(\omega_n^{\pm} \left(d_n^{\pm}\right)^{\sigma}, z\right)_n \sigma = 0$$

by Proposition 4.11. The lemma then follows because any element of $\Lambda_n$ that is killed by $\omega_n^{\pm}$ is divisble by $\tilde{\omega}_n^{\mp}$. □

$\varphi$ a character of
Since $\omega_n = X\tilde{\omega}_n^+\tilde{\omega}_n^-$, we have an isomorphism

$$\Lambda_n^{\pm} := \mathbf{Z}_p[X]/\omega_n^{\pm} \cong \tilde{\omega}_n^{\mp}\Lambda_n.$$

We define $P^{\pm}_{\Lambda,n}$ to be the unique map which makes the following diagram commute.

$$\begin{array}{ccc} H^1(L_n, T) & \xrightarrow{P^{\pm}_{\Lambda,n}} & \Lambda_n^{\pm} \\ \downarrow & & \downarrow \\ \frac{H^1(L_n,T)}{H^1_{\pm}(L_n,T)} & \xrightarrow{P_n^{\pm}} & \Lambda_n \end{array}$$

Here the right vertical map is $\Lambda_n^{\pm} \cong \tilde{\omega}_n^{\mp}\Lambda_n \subseteq \Lambda_n$. The properties of the maps $P^{\pm}_{\Lambda,n}$ are gathered in the following proposition.

**Proposition 4.15.**

1. *For $n \geq 1$,*

$$\begin{array}{ccc} H^1(L_{n+1},T) & \xrightarrow{P^{\pm}_{\Lambda,n+1}} & \Lambda^{\pm}_{n+1} \\ {\scriptstyle \mathrm{cor}_{n+1/n}}\downarrow & & \downarrow \\ H^1(L_n,T) & \xrightarrow{P^{\pm}_{\Lambda,n}} & \Lambda^{\pm}_{n} \end{array} \tag{11}$$

*commutes. (Here the right vertical map is the natural projection.)*

2. *$P^{\pm}_{\Lambda,n}$ is surjective for all $n \geq 1$.*

3. *$P^{\pm}_{\Lambda,n}$ determines an isomorphism $\dfrac{H^1(L_n,T)}{H^1_{\pm}(L_n,T)} \cong \Lambda^{\pm}_n$.*

*Proof.* See the proofs of Proposition 8.22, 8.24 and 8.25 of [8]. □

Diagram (11) allows us to consider the projective limit (with respect to $n$) of the maps $P^{\pm}_{\Lambda,n}$ and we denote this limit by

$$P^{\pm}_{\Lambda} : \mathbf{H}^1(T) := \varprojlim_n (H^1(L_n,T), \mathrm{cor}) \longrightarrow \varprojlim_n \Lambda^{\pm}_n \cong \Lambda.$$

Also, let $\mathbf{H}^1_{\pm}(T) := \varprojlim_n (H^1_{\pm}(L_n,T), \mathrm{cor})$ and we have:

**Proposition 4.16.** *$P^{\pm}_{\Lambda}$ defines an isomorphism $\mathbf{H}^1(T)/\mathbf{H}^1_{\pm}(T) \cong \Lambda$. Furthermore, $\mathbf{H}^1_{\pm}(T)$ is a free $\Lambda$-module of rank 1.*

*Proof.* For the first part, apply part (3) of Proposition 4.15. Then, from the first part, we know that $\mathbf{H}^1_{\pm}(T)$ is a direct summand of $\mathbf{H}^1(T)$ which by [15, Proposition 3.2.1] is a free $\Lambda$-module of rank 2. Therefore, $\mathbf{H}^1_{\pm}(T)$ is a projective $\Lambda$-module and since $\Lambda$ is local, $\mathbf{H}^1_{\pm}(T)$ is free of rank 1. □

Finally, we have the following description of the maps $P^{\pm}_n$ in terms of the dual exponential map of the Galois module $T$.

**Proposition 4.17.** *We have*

$$P^{\pm}_n(z) = \left( \sum_{\sigma \in G_n} \ell(d^{\pm}_n)^{\sigma} \sigma \right) \left( \sum_{\sigma \in G_n} \exp^*_{\omega_E}(z^{\sigma}) \sigma^{-1} \right).$$

*Proof.* See Proposition 8.26 of [8]. □

# 5 The "most basic" case in Iwasawa theory

## 5.1 Algebraic results

In this section, we will be working under the following restrictive global hypothesis. Recall that $p$ is assumed to be odd.

- **Hypothesis G** (for global):
  1. $p \nmid \mathrm{Tam}(E/K)$
  2. $Ш(E/K)[p] = 0$
  3. $E(K)/pE(K) = 0$.

In the good (non-anomalous) ordinary case, this hypothesis implies that both the $\mu$-invariant and $\lambda$-invariant of $E$ vanishes along any $\mathbf{Z}_p$-extension of $K$. For this reason, we refer to the situation in this section as the "most basic" case. Throughout this section we will be assuming (S) and (G) and under these hypotheses we will prove the following theorem.

**Theorem 5.1.** *Assuming (SG), $a_p = 0$ and $p$ odd, we have*

1. *$E(K_n)$ is finite*
2. *$Ш(E/K_n)[p^\infty]^\wedge \cong (\Lambda/(\tilde{\omega}_n^+, \tilde{\omega}_n^-))^d$*
3. *$\mathrm{ord}_p\left(\#Ш(E/K_n)[p^\infty]\right) = d \cdot \sum_{k=0}^{n} q_k$*

*where $d = [K : \mathbf{Q}]$ and $q_k$ is defined in Corollary 4.12.*

**Remark 5.2.** The hypothesis $a_p = 0$ is probably not necessary. See [18] for a proof of this theorem for general $a_p$ (divisible by $p$) when $K = \mathbf{Q}$. However, the condition that $p$ is odd is necessary (see [18, Remark 1.2]).

We begin by computing the structure of $X$ as a $\Lambda$-module. The following well known result does not assume (SG).

**Proposition 5.3.** *When $p$ is supersingular for $E/\mathbf{Q}$,*

$$\mathrm{rk}_\Lambda X = \mathrm{corank}_\Lambda H^1(K_\Sigma/K_\infty, E[p^\infty]) \geq d.$$

*Proof.* The first equality follows from [20, Corollary 5]. The inequality follows from a global Euler characteristic calculation (see [4, Proposition 3]) since

$$\mathrm{corank}_\Lambda H^1(K_\Sigma/K_\infty, E[p^\infty]) - \mathrm{corank}_\Lambda H^2(K_\Sigma/K_\infty, E[p^\infty]) = d.$$

□

**Proposition 5.4.** *Assuming (SG), $X$ is a free $\Lambda$-module of rank $d$.*

*Proof.* Considering Theorem 3.1 with $n = 0$ yields

$$\widehat{E}(K_p) \twoheadrightarrow X_\Gamma \tag{12}$$

since, by (G), $\mathrm{Sel}(E[p^\infty]/K) = 0$ and $p \nmid \mathrm{Tam}(E/K)$. Now, $\mathrm{rk}_{\mathbf{Z}_p} X_\Gamma \geq d$ by Proposition 5.3 and hence (12) is an isomorphism since $\widehat{E}(K_p) \cong \mathbf{Z}_p^d$. By Nakayama's lemma, we can lift (12) to a map $\Lambda^d \twoheadrightarrow X$. Again, by Proposition 5.3, $\mathrm{rk}_\Lambda X \geq d$ and hence this map is an isomorphism. □

**Remark 5.5.** For the remainder of this section we will fix an isomorphism of $X$ with $\Lambda^d$. Such an isomorphism (as constructed in Proposition 5.4) depends in part upon an identification of $\widehat{E}(K_p)$ with $\mathbf{Z}_p^d$. We will now specify this identification. By (S), $K_{\mathfrak{p}_j} \cong \mathbf{Q}_p$ and hence Theorem 4.5 applies to $\widehat{E}(K_{n,\mathfrak{p}_j})$. Set $d_{n,j} = (0, \ldots, d_n, \ldots, 0) \in \widehat{E}(K_{n,p}) = \oplus_{i=1}^d \widehat{E}(K_{n,\mathfrak{p}_i})$ where $d_n \in \widehat{E}(K_{n,\mathfrak{p}_j})$. Then $\{d_{0,j}\}_{j=1}^d$ generates $\widehat{E}(K_p)$ and in what follows we will assume that $\widehat{E}(K_p)$ is identified with $\mathbf{Z}_p^d$ via these generators.

In particular, Theorem 3.1 yields

$$\widehat{E}(K_{n,p}) \xrightarrow{R_n} \Lambda_n^d \longrightarrow X_n \longrightarrow 0 \tag{13}$$

where $\Lambda_n = \Lambda/\omega_n\Lambda$. Furthermore, for $m \leq n$ we have

$$\begin{array}{ccc} \widehat{E}(K_{n,p}) & \xrightarrow{R_n} & \Lambda_n^d \\ {\scriptstyle \mathrm{Tr}_m^n}\downarrow & & \downarrow \\ \widehat{E}(K_{m,p}) & \xrightarrow{R_m} & \Lambda_m^d \end{array} \tag{14}$$

where $\mathrm{Tr}_m^n$ is the trace map and the right vertical map is the natural projection. We postpone checking the commutativity of this diagram until section 6 (see Proposition 6.3).

**Lemma 5.6.** *$\tilde{\omega}_n^{-\varepsilon} | R_n(d_{n,j})$ with $\varepsilon = (-1)^n$.*

*Proof.* By Corollary 4.12, $d_{n,j}$ is killed by $\omega_n^\varepsilon$. Since $R_n$ is a Galois equivariant map, $R_n(d_{n,j})$ is also killed by $\omega_n^\varepsilon$ and is therefore divisible by $\tilde{\omega}_n^{-\varepsilon}$. □

By Lemma 5.6, write

$$R_n(d_{n,j}) = \tilde{\omega}_n^{-\varepsilon} \cdot (u_{1j}, \ldots u_{dj}) \in \Lambda_n^d$$

where $\varepsilon = (-1)^n$.

**Lemma 5.7.** *$\det(u_{ij})$ is a unit in $\Lambda_n$.*

*Proof.* To prove this lemma it is enough to check that $\det(u_{ij}(0))$ is a unit in $\mathbf{Z}_p$. In the case that $n$ is even, we have by diagram (14)

$$R_n(d_{n,j}) \equiv R_0(\mathrm{Tr}_0^n(d_{n,j})) \text{ in } \Lambda_0^d \cong (\mathbf{Z}_p[X]/X)^d.$$

By Theorem 4.5, $\mathrm{Tr}_0^n(d_{n,j}) = \pm p^{\frac{n}{2}} d_{0,j}$. Also by Remark 5.5, we have normalized $R_0$ so that $R_0(d_{0,j}) = (0, \ldots, 1, \ldots, 0)$ where 1 is in the $j$-th coordinate. Therefore, $R_n(d_{n,j})$ evaluated at 0 equals $(0, \ldots, \pm p^{\frac{n}{2}}, \ldots, 0)$.

On the other hand,

$$\begin{aligned} R_n(d_{n,j})(0) &= \tilde{\omega}_n^-(0) \cdot (u_{1j}(0), \ldots, u_{dj}(0)) \\ &= p^{\frac{n}{2}} \cdot (u_{1j}(0), \ldots, u_{dj}(0)). \end{aligned}$$

Therefore,

$$u_{ij}(0) = \begin{cases} 0 & i \neq j \\ \pm 1 & i = j \end{cases} \tag{15}$$

and $\det(u_{ij}(0)) = \pm 1 \in \mathbf{Z}_p^\times$. The case of $n$ odd is proven similarly using the fact that $\mathrm{Tr}_0^1(d_{1,j}) = u \cdot d_{0,j}$ with $u \in \mathbf{Z}_p^\times$. □

Let $I_n = R_n(\widehat{E}(K_{n,p})) \subseteq \Lambda_n^d$. Then by Theorem 4.5, $I_n$ is the ideal of $\Lambda_n^d$ generated by $R_n(d_{n,j})$ and $R_n(d_{n-1,j})$ for $j = 1, \ldots, d$.

**Proposition 5.8.** $\Lambda_n^d / I_n \cong (\Lambda/(\tilde{\omega}_n^+, \tilde{\omega}_n^-))^d$.

*Proof.* Let $\tilde{\omega}_{n,j}^\varepsilon = (0, \ldots, \tilde{\omega}_n^\varepsilon, \ldots, 0)$ where $\tilde{\omega}_n^\varepsilon$ lies in the $j$-th coordinate and let $J_n$ be the ideal generated by $\tilde{\omega}_{n,j}^+$ and $\tilde{\omega}_{n,j}^-$ for $j = 1, \ldots, d$. To prove the proposition, it suffices to show that $I_n = J_n$. By Proposition 5.6, $I_n \subseteq J_n$. Conversely, from (15) in the proof of Lemma 5.7, we have that $(I_n)_\Gamma \cong (J_n)_\Gamma$. Therefore, by Nakayama's lemma we can conclude $I_n = J_n$. □

*Proof of Theorem 5.1.* From (13) and Proposition 5.8,

$$X_n \cong \left(\Lambda/(\tilde{\omega}_n^+, \tilde{\omega}_n^-)\right)^d. \tag{16}$$

An explicit computation (see [9, Lemma 7.1]) shows that

$$\mathrm{ord}_p \,\#\left(\Lambda/(\tilde{\omega}_n^+, \tilde{\omega}_n^-)\right) = \sum_{k=0}^{n} q_k. \tag{17}$$

Therefore $S_n$ is finite and in particular $E(K_n)$ is finite proving part (1). Now since there is no presence of rank, $S_n \cong Ш(E/K_n)[p^\infty]$; this together with (16) yields part (2). Finally, part (3) follows from (17). □

## 5.2 Analytic consequences

We begin with a lemma that converts analytic hypotheses into algebraic ones. The following is a deep lemma that relies heavily upon Kato's Euler system.

**Lemma 5.9.** *If $p$ is an odd supersingular prime for $E/\mathbf{Q}$ such that*

1. $\mathrm{ord}_p\left(\frac{L(E/\mathbf{Q},1)}{\Omega_{E/\mathbf{Q}}}\right) = 0$
2. $G_\mathbf{Q} \longrightarrow \mathrm{Aut}(E[p])$ *is surjective*

*then* $\mathrm{Sel}(E[p^\infty]/\mathbf{Q}) = 0$ *and* $p \nmid \mathrm{Tam}(E/\mathbf{Q})$.

*Proof.* We have that $L(E/\mathbf{Q},1) \neq 0$ and hence from Kato's Euler system [7], $E(\mathbf{Q})$ and $Ш(E/\mathbf{Q})$ are both finite. We must show that $Ш(E/\mathbf{Q})[p^\infty] = 0$ and $p \nmid \mathrm{Tam}(E/\mathbf{Q})$.

The (analytic) $p$-adic $L$-function $L_p^{\mathrm{an}}(E,T) \in \overline{\mathbf{Q}}_p[[T]]$ interpolates special values of $L$-series and in particular

$$L_p^{\mathrm{an}}(E,0) = \left(1 - \frac{1}{\alpha}\right)^2 \frac{L(E/\mathbf{Q},1)}{\Omega_{E/\mathbf{Q}}}$$

where $\alpha$ is a root of $x^2 - a_p x + p$ (see [12, Section 14]).

In [14], Perrin-Riou constructed an algebraic $p$-adic $L$-function $L_p^{\mathrm{alg}}(E,T) \in \overline{\mathbf{Q}}_p[[T]]$ (defined up to a unit in $\Lambda$) with the property that

$$L_p^{\mathrm{alg}}(E,0) \sim \left(1 - \frac{1}{\alpha}\right)^2 \frac{\#Ш(E/\mathbf{Q}) \cdot \mathrm{Tam}(E/\mathbf{Q})}{\#E^{\mathrm{tor}}(\mathbf{Q})}$$

when $\mathrm{Sel}(E[p^\infty]/\mathbf{Q})$ is finite (see also [16, Théorème 2.2.1]).

Kato proved a divisibility between these two $p$-adic $L$-functions under the above assumption on the Galois representation. Namely, we have that

$$L_p^{\mathrm{alg}}(E,T) \mid L_p^{\mathrm{an}}(E,T)$$

in $\mathbf{Z}_p[[T]]$ (see [7, Theorem 12.5] and [16, Théorème 3.1.3]). In particular,

$$\mathrm{ord}_p\left(Ш(E/\mathbf{Q}) \cdot \mathrm{Tam}(E/\mathbf{Q})\right) \leq \mathrm{ord}_p\left(\frac{L(E/\mathbf{Q},1)}{\Omega_{E/\mathbf{Q}}}\right).$$

(Note that $E[p](\mathbf{Q}) = 0$ since $p$ is supersingular.) From the above inequality, the lemma follows immediately since we are assuming that the right hand side is zero. □

The following corollary, originally proven by Kurihara, follows from Theorem 5.1 and Lemma 5.9.

**Corollary 5.10.** *Let $K = \mathbf{Q}$ so that $K_\infty = \mathbf{Q}_\infty$ is the cyclotomic $\mathbf{Z}_p$-extension. Let $E/\mathbf{Q}$ be an elliptic curve and $p$ an odd prime of good reduction with $a_p = 0$. Assume that*

1. $\mathrm{ord}_p\left(\frac{L(E/\mathbf{Q},1)}{\Omega_{E/\mathbf{Q}}}\right) = 0$
2. $G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}(E[p])$ *is surjective.*

*Then the conclusions of Theorem 5.1 hold with $d = 1$.*

*Proof.* First note that $\mathrm{ord}_p\left(\frac{L(E/\mathbf{Q},1)}{\Omega_{E/\mathbf{Q}}}\right) = 0$ implies that $\mathrm{Sel}(E[p^\infty]/\mathbf{Q}) = 0$ and that $p \nmid \mathrm{Tam}(E/\mathbf{Q})$ by Lemma 5.9. Therefore, hypothesis (G) is satisfied. Furthermore, (S) is automatically satisfied when $K = \mathbf{Q}$ and the conclusions of Theorem 5.1 follow. □

**Corollary 5.11.** *Let $K$ be a quadratic extension of $\mathbf{Q}$ and $K_\infty$ any $\mathbf{Z}_p$-extension of $K$. Let $E/\mathbf{Q}$ be an elliptic curve with $p$ an odd prime of good reduction satisfying (S) for $K$ and such that $a_p = 0$. Assume further that*

1. $\mathrm{ord}_p\left(\frac{L(E/K,1)}{\Omega_{E/K}}\right) = 0$
2. $G_K \longrightarrow \mathrm{Aut}(E[p])$ *is surjective.*

*Then the conclusions of Theorem 5.1 hold with $d = 2$.*

*Proof.* Let $E^D$ be the quadratic twist of $E$ corresponding to $K/\mathbf{Q}$. Then $L(E/K,s) = L(E/\mathbf{Q},s)\cdot L(E^D/\mathbf{Q},s)$. In particular, $\mathrm{ord}_p\left(\frac{L(E/K,1)}{\Omega_{E/K}}\right) = 0$ implies that $\mathrm{ord}_p\left(\frac{L(E/\mathbf{Q},1)}{\Omega_{E/\mathbf{Q}}}\right) = 0$ and $\mathrm{ord}_p\left(\frac{L(E^D,1)}{\Omega_{E^D/\mathbf{Q}}}\right) = 0$ since both special values are $p$-integral (see [17, Remark 6.5]). Since $G_K$ surjects onto $\mathrm{Aut}(E[p])$, we have that $G_{\mathbf{Q}}$ surjects onto both $\mathrm{Aut}(E[p])$ and $\mathrm{Aut}(E^D[p])$. Therefore, by Lemma 5.9, we have that $\mathrm{Sel}(E[p^\infty]/\mathbf{Q}) = \mathrm{Sel}(E^D[p^\infty]/\mathbf{Q}) = 0$ and that $p$ does not divide $\mathrm{Tam}(E/\mathbf{Q})\cdot\mathrm{Tam}(E^D/\mathbf{Q})$. From this we can conclude that $\mathrm{Sel}(E[p^\infty]/K) = 0$ and that $p$ does not divide $\mathrm{Tam}(E/K)$. Therefore, hypothesis (G) is satisfied and the conclusions of Theorem 5.1 follow. □

# 6 Algebraic $p$-adic $L$-functions

In this section, we construct algebraic $p$-adic $L$-functions in two different ways. First, we work directly with the points $\{d_n\}$ and Theorem 3.1 to produce two $p$-adic power series as in [13]. However, as in section 5, we first remove certain trivial zeroes to obtain elements of the Iwasawa algebra. Alternatively, we consider plus/minus Selmer groups as in [8] and define algebraic $p$-adic $L$-functions as the characteristic power series of these $\Lambda$-modules. Finally, we show that these two constructions yield the same power series (up to a unit in $\Lambda$). We continue to assume (S) in order to make use of the local results of section 4.

## 6.1 Construction of algebraic $p$-adic $L$-functions via $\{d_n\}$

We begin by generalizing the constructions done in section 5. Assuming (G), it was shown in Proposition 5.4 that $\mathrm{rk}_\Lambda X = d$. In general, this would be true assuming a form of the weak Leopoldt conjecture. We introduce this conjecture as another hypothesis. (See [5] for a formulation of this conjecture and for cases when it is known to be true.)

- **Hypothesis W** (for Weak Leopoldt): $\mathrm{corank}_\Lambda H^2(K_\Sigma/K_\infty, E[p^\infty]) = 0$.

**Proposition 6.1.** *When $p$ is supersingular for $E/\mathbf{Q}$, we have that (W) is equivalent to $\mathrm{rk}_\Lambda X = d$.*

*Proof.* This is clear from Proposition 5.3 and its proof. □

If $Y$ is the $\Lambda$-torsion submodule of $X$, we have

$$0 \longrightarrow Y \longrightarrow X \longrightarrow Z \longrightarrow 0 \tag{18}$$

where $Z$ is torsion free. By Proposition 6.1, embedding $Z$ into its reflexive hull yields a sequence

$$0 \longrightarrow Z \longrightarrow \Lambda^d \longrightarrow H \longrightarrow 0 \tag{19}$$

with $H$ finite. We can then define a map

$$\widehat{E}(K_{n,p}) \longrightarrow \widehat{E}(K_{n,p}) \times B_n \longrightarrow X_{\Gamma_n} \longrightarrow Z_{\Gamma_n} \longrightarrow \Lambda_n^d$$

where the second map comes from Theorem 3.1, the third map comes from (18) and the final map comes from (19). Denote by $Q_n$ the map from $\widehat{E}(K_{n,p})$ to $X_{\Gamma_n}$ and by $R_n$ the map from $\widehat{E}(K_{n,p})$ to $\Lambda_n^d$. These maps satisfy an important compatibility property already exploited in section 5. Before discussing this property, we state a lemma on the functoriality of the snake lemma.

**Lemma 6.2.** *For $i = 1, 2$, let*

$$\begin{array}{ccccccc} & & A_i & \longrightarrow & B_i & \longrightarrow & C_i & \longrightarrow & 0 \\ & & {\scriptstyle a_i}\downarrow & & {\scriptstyle b_i}\downarrow & & {\scriptstyle c_i}\downarrow & & \\ 0 & \longrightarrow & A_i' & \longrightarrow & B_i' & \longrightarrow & C_i' & & \end{array}$$

*be a commutative diagram and assume that there are maps $A_1 \longrightarrow A_2$, $B_1 \longrightarrow B_2$, $C_1 \longrightarrow C_2$ and likewise for $A_i'$, $B_i'$ and $C_i'$ such that all the respective squares commute. Then*

$$\begin{array}{ccc} \ker(c_1) & \xrightarrow{\delta_1} & \operatorname{coker}(a_1) \\ \downarrow & & \downarrow \\ \ker(c_2) & \xrightarrow{\delta_2} & \operatorname{coker}(a_2) \end{array}$$

*commutes where $\delta_i$ is the boundary map coming from the snake lemma.*

*Proof.* This follows from a diagram chase. □

**Proposition 6.3.** *For $m \leq n$, we have that the following diagrams*

$$\begin{array}{ccc} \widehat{E}(K_{n,p}) & \xrightarrow{Q_n} & X_{\Gamma_n} \\ {\scriptstyle \mathrm{Tr}_m^n}\downarrow & & \downarrow \\ \widehat{E}(K_{m,p}) & \xrightarrow{Q_m} & X_{\Gamma_m} \end{array} \qquad \begin{array}{ccc} \widehat{E}(K_{n,p}) & \xrightarrow{R_n} & \Lambda_n^d \\ {\scriptstyle \mathrm{Tr}_m^n}\downarrow & & \downarrow \\ \widehat{E}(K_{m,p}) & \xrightarrow{R_m} & \Lambda_m^d \end{array}$$

*commute.*

*Proof.* Since we have a fixed map $X \longrightarrow \Lambda^d$ defined independent of $n$, the following square

$$\begin{array}{ccc} X_{\Gamma_n} & \longrightarrow & \Lambda_n^d \\ \downarrow & & \downarrow \\ X_{\Gamma_m} & \longrightarrow & \Lambda_m^d \end{array}$$

commutes and therefore, we only need to check the commutativity of the left diagram in the proposition.

We will use the notation of Theorem 3.1. Furthermore, let $\widehat{E}_n = \widehat{E}(K_{n,p})$ and $K_n = \oplus_v \ker(r_{n,v})$. Then, examining the definition of $Q_n^\wedge$ piece-by-piece yields

$$\begin{array}{ccccccccc} S^{\Gamma_m} & \twoheadrightarrow & \mathrm{coker}(s_m) & \overset{\delta_m}{\cong} & K_m \cap \mathrm{im}(\gamma_m) & \subseteq & K_m & \twoheadrightarrow & \mathcal{H}_{m,p} & \cong & \left(\widehat{E}_m\right)^\wedge \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ S^{\Gamma_n} & \twoheadrightarrow & \mathrm{coker}(s_n) & \overset{\delta_n}{\cong} & K_n \cap \mathrm{im}(\gamma_n) & \subseteq & K_n & \twoheadrightarrow & \mathcal{H}_{n,p} & \cong & \left(\widehat{E}_n\right)^\wedge \end{array}$$

where the first horizontal map (for either the top or bottom row) is the natural projection, the second is given by the snake lemma (Proposition 3.2), the third is the natural inclusion, the fourth is the natural projection (applying Proposition 3.3) and the fifth is given by Tate local duality. The first vertical map is the natural inclusion, the second is induced by this inclusion, the third, fourth and fifth maps are induced by restriction and the sixth map is given by the dual of the trace map.

We now check the commutativity of this diagram square-by-square. The first square commutes essentially by definition. The second square commutes by the functoriality of the snake lemma (Lemma 6.2). The third and fourth squares commute because restriction commutes with these natural inclusions and projections. Finally, the commutativity of the last square is an essential property of Tate local duality (see [11, Proposition 4.2]). Dualizing then yields the proposition. □

Since these maps are Galois equivariant, Proposition 5.6 remains valid in this setting. In particular, we can write

$$R_n(d_{n,j}) = \tilde{\omega}_n^{-\varepsilon} \cdot (-1)^{\left[\frac{n+1}{2}\right]} \cdot (u_{1j}^n, \ldots, u_{dj}^n)$$

with $u_{ij}^n \in \Lambda/\omega_n^\varepsilon \Lambda$.

**Lemma 6.4.** *For $n > 1$ and $\varepsilon = (-1)^n$, $u_{ij}^n \equiv u_{ij}^{n-2} \pmod{\omega_{n-2}^\varepsilon}$.*

*Proof.* This lemma follows from Theorem 4.5 and Proposition 6.3. □

From Lemma 6.4, we have that $(u_{ij}^n)$ forms a compatible sequence inside of $\varprojlim_n \Lambda/\omega_n^{-\varepsilon}\Lambda$ for $n$ running through positive integers of a fixed parity. When $n$ is even, denote this sequence by $u_{ij}^+$ and when $n$ is odd by $u_{ij}^-$. Since $\varprojlim_n \Lambda/\omega_n^{\pm}\Lambda \cong$

$\Lambda$, we can consider $u_{ij}^+$ and $u_{ij}^-$ as Iwasawa functions. We are now prepared to define the plus/minus algebraic $p$-adic $L$-functions.

**Definition 6.5.** Let $Y$ be the $\Lambda$-torsion submodule of $X$ and let $t_Y = \mathrm{char}_\Lambda(Y)$. Then set

$$L_p^\pm(E, K_\infty/K, X) := \det(u_{ij}^\pm) \cdot t_Y$$

which is well-defined up to a unit in $\Lambda$.

**Remark 6.6.** Note that $L_p^\pm(E, K_\infty/K, X)$ can be identically zero. This vanishing occurs when $\mathrm{corank}_{\mathbf{Z}_p}(S_n)$ is unbounded (see Corollary 7.11). Furthermore, these coranks can indeed be unbounded. For example, consider the case where $K$ is a quadratic imaginary field and $K_\infty$ is the anticylotomic extension. The recent results of [1] show that if there are Heegner points present then indeed the corank of $S_n$ will grow without bound.

## 6.2 Restricted Selmer groups

As in [8], we define plus/minus Selmer groups by putting harsher local conditions at each $\mathfrak{p}_i$.

**Definition 6.7.** Set

$$\mathrm{Sel}^\pm(E[p^\infty]/K_n) = \ker\left(\mathrm{Sel}(E[p^\infty]/K_n) \longrightarrow \prod_{\mathfrak{p}|p} \frac{E(K_{n,\mathfrak{p}}) \otimes \mathbf{Q}_p/\mathbf{Z}_p}{\widehat{E}^\pm(K_{n,\mathfrak{p}}) \otimes \mathbf{Q}_p/\mathbf{Z}_p}\right)$$

and $\mathrm{Sel}^\pm(E[p^\infty]/K_\infty) = \varinjlim_n \mathrm{Sel}^\pm(E[p^\infty]/K_n)$.

These plus/minus Selmer groups behave like Selmer groups at ordinary primes. In particular, they satisfy a control theorem in the spirit of Mazur's original control theorem.

**Theorem 6.8.** *The natural map*

$$\mathrm{Sel}^\pm(E[p^\infty]/K_n)^{\omega_n^\pm=0} \longrightarrow \mathrm{Sel}^\pm(E[p^\infty]/K_\infty)^{\omega_n^\pm=0}$$

*is injective and has a finite cokernel bounded independent of $n$.*

*Proof.* The proof in [8, Theorem 9.3] translates verbatim over to our situation. □

If $X^\pm(E/K_\infty) = \mathrm{Sel}^\pm(E[p^\infty]/K_\infty)^\wedge$ then $X^\pm(E/K_\infty)$ need not be a torsion $\Lambda$-module. The ranks of these modules will be discussed in section 7.1.

## 6.3 Comparing $\mathrm{Sel}^{\pm}(E[p^\infty]/K_\infty)$ and $L_p^{\pm}(E, K_\infty/K, X)$

As in the ordinary case, when $X^{\pm}(E/K_\infty)$ is a torsion module, its characteristic power series should be considered as an algebraic $p$-adic $L$-function. The following proposition (whose proof will fill the remainder of the section) relates this point of view with that of section 6.1.

**Proposition 6.9.** *Assuming (W),*

$$char_\Lambda X^{\pm}(E/K_\infty) = L_p^{\pm}(E, K_\infty/K, X) \cdot v.$$

*with* $v \in \Lambda^\times$.

Before proving this proposition, we begin with a few lemmas.

**Lemma 6.10.** *For* $\mathfrak{p}|p$ *and* $n \geq 0$,

$$\tilde{\omega}_n^{-\varepsilon} \cdot H^1_\varepsilon(K_{n,\mathfrak{p}}, T) \subseteq \widehat{E}^{\varepsilon}(K_{n,\mathfrak{p}})$$

*with* $\varepsilon = (-1)^n$.

*Proof.* We check this for $n$ even; the case of $n$ odd is similar. We have

$$\frac{H^1_{\pm}(K_{n,\mathfrak{p}}, T)}{\widehat{E}(K_{n,\mathfrak{p}})} \hookrightarrow \frac{H^1(K_{n,\mathfrak{p}}, T)}{H^1_{\mp}(K_{n,\mathfrak{p}}, T)} \cong \Lambda/\omega_n^{\mp}\Lambda$$

where the second map is given by Proposition 4.15. The first map is injective since $z \in H^1_+(K_{n,\mathfrak{p}}, T) \cap H^1_-(K_{n,\mathfrak{p}}, T)$ is orthogonal to $\widehat{E}(K_{n,\mathfrak{p}}) = \widehat{E}^+(K_{n,\mathfrak{p}}) + \widehat{E}^-(K_{n,\mathfrak{p}})$ and hence in $\widehat{E}(K_{n,\mathfrak{p}})$. However, this map is not surjective; its image is killed by $\tilde{\omega}_n^-$ (rather than just $\omega_n^-$) which we now check.

Note that $\frac{H^1(K_{n,\mathfrak{p}},T)}{H^1_{\mp}(K_{n,\mathfrak{p}},T)} \cong \Lambda/\omega_n^{\mp}\Lambda$ is free over $\mathbf{Z}_p$ and hence $\frac{H^1_{\pm}(K_{n,\mathfrak{p}},T)}{\widehat{E}(K_{n,\mathfrak{p}})}$, being a submodule, is also free. Then since $\widehat{E}(K_{n,\mathfrak{p}})$ is free, we can conclude that $H^1_{\pm}(K_{n,\mathfrak{p}}, T)$ is free. Now

$$\mathrm{rk}_{\mathbf{Z}_p} \frac{H^1(K_{n,\mathfrak{p}}, T)}{H^1_+(K_{n,\mathfrak{p}}, T)} = \mathrm{rk}_{\mathbf{Z}_p} \Lambda/\omega_n^+\Lambda = \deg(\omega_n^+) = p^n - p^{n-1} + \cdots + p^2 - p + 1.$$

Hence, since $\mathrm{rk}_{\mathbf{Z}_p} H^1(K_{n,\mathfrak{p}}, T) = 2 \cdot p^n$,

$$\mathrm{rk}_{\mathbf{Z}_p} H^1_+(K_{n,\mathfrak{p}}, T) = 2 \cdot p^n - (p^n - p^{n-1} + \cdots + p^2 - p + 1) = p^n + q_n$$

and therefore $\frac{H^1_+(K_{n,\mathfrak{p}},T)}{\widehat{E}(K_{n,\mathfrak{p}})}$ has $\mathbf{Z}_p$-rank equal to $q_n$.

Now, note that any submodule of $\Lambda/\omega_n^-\Lambda \cong Z_p[X]/\omega_n^-(X)$ of rank $q_n$ is of the form $p^r X\mathbf{Z}_p[X]/\omega_n^-(X)$ and hence is annihilated by $\tilde{\omega}_n^-$. This proves that

$$\tilde{\omega}_n^- \cdot H^1_+(K_{n,\mathfrak{p}}, T) \subseteq \widehat{E}(K_{n,\mathfrak{p}}).$$

Since $\omega_n^+ \cdot \big(\tilde{\omega}_n^- \cdot H^1_+(K_{n,\mathfrak{p}}, T)\big) = \omega_n \cdot H^1_+(K_{n,\mathfrak{p}}, T) = 0$, we further have that $\tilde{\omega}_n^- \cdot H^1_+(K_{n,\mathfrak{p}}, T) \subseteq \widehat{E}^+(K_{n,\mathfrak{p}})$ by the definition of $\widehat{E}^+$; this completes the proof. □

Repeating the arguments of Theorem 3.1 for the plus/minus Selmer groups yields

$$\begin{array}{ccccccc} B_n \times \bigoplus_{\mathfrak{p}|p} H^1_\pm(K_{n,\mathfrak{p}},T) & \xrightarrow{Q_n^\pm} & X_{\Gamma_n} & \longrightarrow & X_n^\pm & \longrightarrow & 0 \\ \uparrow & & \uparrow= & & \uparrow & & \\ B_n \times \widehat{E}(K_{n,p}) & \xrightarrow{Q_n} & X_{\Gamma_n} & \longrightarrow & X_n & \longrightarrow & 0 \end{array} \tag{20}$$

where $X_n^\pm = \mathrm{Sel}^\pm(E[p^\infty]/K_n)^\wedge$. Taking the projective limit of the top line of the above diagram yields

$$\bigoplus_{\mathfrak{p}|p} \mathbf{H}^1_\pm(K_{\infty,\mathfrak{p}},T) \xrightarrow{Q^\pm} X \longrightarrow X^\pm(E/K_\infty) \longrightarrow 0. \tag{21}$$

Let $R^\pm$ be the composition of $Q^\pm$ with the embedding of $X$ into $\Lambda^d$ from (18) and (19) and define $R_n^\pm$ similarly. By Proposition 4.16, $\mathbf{H}^1_\pm(K_{\infty,\mathfrak{p}},T)$ is a free $\Lambda$-module of rank 1.

**Lemma 6.11.** *For each $j$, fix a generator $z_j$ of $\mathbf{H}^1_\pm(K_{\infty,\mathfrak{p}_j},T)$. Then*

$$R^\pm(z_j) = (u_{1j}^\pm,\ldots,u_{dj}^\pm)\cdot v_j^\pm$$

*with $v_j^\pm$ a unit in $\Lambda$.*

*Proof.* Let $\varepsilon = (-1)^n$. We begin by recovering the sequence $\{d_{n,j}\}_n$ (constructed in section 4) from the element $z_j$. Let $z_j^n$ be the image of $z_j$ in $H^1_\pm(K_{n,\mathfrak{p}_j},T)$ and let $d'_{n,j} = (-1)^{\left[\frac{n+1}{2}\right]}\cdot\tilde{\omega}_n^\varepsilon\cdot z_j^n$.

**Claim:** $d'_{n,j} = d_{n,j}\cdot v_j^\varepsilon$ for $v_j^\varepsilon$ a unit in $\Lambda$ (depending only on the parity of $n$).

First note that by Lemma 6.10, $d'_{n,j}$ is in fact an element of $\widehat{E}^\varepsilon(K_{n,\mathfrak{p}_j})$. Furthermore, the $z_j^n$ are compatible under corestriction by construction. Therefore,

$$\mathrm{Tr}^n_{n-2}(d'_{n,j}) = \mathrm{Tr}^n_{n-2}(\tilde{\omega}_n^\varepsilon z_j^n) = p\cdot\tilde{\omega}_{n-2}^\varepsilon z_j^{n-2} = -p\cdot d'_{n-2,j}. \tag{22}$$

Since $\widehat{E}^\varepsilon(K_{n,\mathfrak{p}})$ is cyclic, generated by $d_{n,j}$ (Lemma 4.13), we can write $d'_{n,j} = d_{n,j}\cdot v_{n,j}$ with $v_{n,j}\in\Lambda/\omega_n^\varepsilon\Lambda$. Then (22) implies that $(v_{n,j})_n$ forms a compatible sequence for $n$ of a fixed parity. Call the limiting function in $\varprojlim_n \Lambda/\omega_n^\varepsilon\Lambda \cong \Lambda$ by $v_j^+$ for $n$ even and by $v_j^-$ for $n$ odd. To establish the claim it remains to show that $v_j^\pm$ is a unit.

By [9, Proposition 9.2], $\mathbf{H}^1_\pm(K_{\infty,\mathfrak{p}_j},T)$ surjects onto $H^1_\pm(K_{\mathfrak{p}_j},T)\cong\widehat{E}(K_{\mathfrak{p}_j})$. Therefore, $z_j^0$ (resp. $\mathrm{Tr}^1_0(z_j^1)$) generates $\widehat{E}(K_{\mathfrak{p}_j})$. In particular, $d'_{0,j}$ (resp. $\mathrm{Tr}^1_0(d'_{1,j})$) differs from $d_{0,j}$ (resp. $\mathrm{Tr}^1_0(d_{1,j})$) by a unit in $\mathbf{Z}_p$. Hence, $v_j^\pm(0)\in\mathbf{Z}_p^\times$ and $v_j^\pm$ is a unit in $\Lambda$.

By the claim,

$$\begin{aligned}\tilde{\omega}_n^{\varepsilon} \cdot R_n^{\varepsilon}(z_j^n) &= R_n\left((-1)^{\left[\frac{n+1}{2}\right]} d'_{n,j}\right) = R_n\left((-1)^{\left[\frac{n+1}{2}\right]} d_{n,j}\right) \cdot v_j^{\varepsilon} \\ &= \tilde{\omega}_n^{\varepsilon} \cdot (u_{1j}^n, \ldots, u_{dj}^n) \cdot v_j^{\varepsilon}.\end{aligned}$$

Then cancelling $\tilde{\omega}_n^{\varepsilon}$ and taking limits over $n$ of a fixed parity yields the lemma. □

*Proof of Proposition 6.9.* If $\operatorname{corank}_{\mathbf{Z}_p}(S_n)$ is unbounded we will see by Corollary 7.11 and Corollary 7.8 that our proposition holds with $(0) = (0)$. So we may assume that $\operatorname{corank}_{\mathbf{Z}_p}(S_n)$ is bounded. From (21), we have

$$\begin{aligned}\operatorname{char}_\Lambda X^{\pm}(E/K_\infty) &= \operatorname{char}_\Lambda \left( \frac{X}{Q^{\pm}\left(\bigoplus \mathbf{H}^1_{\pm}(K_{\infty,\mathfrak{p}_j}, T)\right)} \right) \\ &= \operatorname{char}_\Lambda \left( \frac{\Lambda^d}{\{R^{\pm}(z_j)\}_{j=1}^d} \right) \cdot \operatorname{char}_\Lambda Y\end{aligned}$$

since $X/Y \subseteq \Lambda^d$ has finite index. Then by Lemma 6.11, $\operatorname{char}_\Lambda \left( \frac{\Lambda^d}{\{R^{\pm}(z_j)\}_{j=1}^d} \right) = \det(u_{ij}^{\pm}) \cdot v$ with $v = \prod_j v_j^{\pm} \in \Lambda^\times$. Hence, $\operatorname{char}_\Lambda X^{\pm}(E/K_\infty) = \det(u_{ij}^{\pm}) \cdot \operatorname{char}_\Lambda Y \cdot v = L_p^{\pm}(E, K_\infty/K, X) \cdot v$ which completes the proof. □

# 7 Growth of Selmer groups in $\mathbf{Z}_p$-extensions

In this section, we explore the growth of $\operatorname{corank}_{\mathbf{Z}_p}(S_n)$ as $n$ varies. We describe this growth in terms of the $\Lambda$-ranks of $X^+(E/K_\infty)$ and $X^-(E/K_\infty)$. When $\operatorname{corank}_{\mathbf{Z}_p}(S_n)$ is bounded, we compute the growth of $Ш(E/K_n)[p^\infty]$ in terms of the $\mu$ and $\lambda$-invariants of $L_p^{\pm}(E, K_\infty/K, X)$ as in [16]. Throughout this section, we will be assuming (S).

## 7.1 Corank of Selmer groups

Let $r^{\pm} = \operatorname{rk}_\Lambda X^{\pm}(E/K_\infty) = \operatorname{corank}_\Lambda \operatorname{Sel}^{\pm}(E[p^\infty]/K_\infty)$.

**Proposition 7.1.** *We have*

$$\operatorname{corank}_{\mathbf{Z}_p}(S_n) = r^{\varepsilon} \cdot q_n + r^{-\varepsilon} \cdot q_{n-1} + O(1)$$

*where $\varepsilon = (-1)^n$. (Here, and in what follows, the $O(1)$ term depends upon $E$ and upon $K_\infty/K$, but not upon $n$.)*

**Remark 7.2.** Note that if $r^+ = r^-$ then $\operatorname{corank}_{\mathbf{Z}_p} S_n = r^{\pm} \cdot p^n + \mathrm{O}(1)$ since $q_n + q_{n-1} = p^n - 1$. In the ordinary case such growth formulas always have this form. However, in the supersingular case, one should have situations where $r^+ \neq r^-$. Namely, if $K$ is a quadratic imaginary extension of $\mathbf{Q}$, $K_\infty$ is the

anti-cyclotomic $\mathbf{Z}_p$-extension and $E$ has CM by $K$, then conjecturally $r^{\varepsilon} = 1$ and $r^{-\varepsilon} = 0$ where $\varepsilon$ is minus the sign of the functional equation for $E$. (See [6, pg. 247])

Before proving Proposition 7.1, we begin with a definition and some lemmas.

**Definition 7.3.** For $L$ a finite extension of $\mathbf{Q}$, let

$$\mathrm{Sel}^0(E[p^\infty]/L) = \ker\left(\mathrm{Sel}(E[p^\infty]/L) \longrightarrow \prod_{\mathfrak{p}|p} E(L_\mathfrak{p}) \otimes \mathbf{Q}_p/\mathbf{Z}_p\right);$$

$$\mathrm{Sel}^1(E[p^\infty]/L) = \ker\left(\mathrm{Sel}(E[p^\infty]/L) \longrightarrow \prod_{\mathfrak{p}|p} \frac{E(L_\mathfrak{p}) \otimes \mathbf{Q}_p/\mathbf{Z}_p}{E(\mathbf{Q}) \otimes \mathbf{Q}_p/\mathbf{Z}_p}\right).$$

To ease notation, let $S_n^{\pm} = \mathrm{Sel}^{\pm}(E[p^\infty]/K_n)$, $S_n^0 = \mathrm{Sel}^0(E[p^\infty]/K_n)$, $S_n^1 = \mathrm{Sel}^1(E[p^\infty]/K_n)$ and $X^{\pm} = X^{\pm}(E/K_\infty)$.

**Lemma 7.4.** *We have*

1. *For any $\Lambda_n$-module $M$, the map $M^{\omega_n^{\varepsilon}=0} + M^{\tilde{\omega}_n^{-\varepsilon}=0} \longrightarrow M$ is surjective and has a finite kernel.*
2. *$(S_n^{\varepsilon})^{\tilde{\omega}_n^{-\varepsilon}=0} \subseteq S_n^1$.*
3. *The map $S_{n-1}^{-\varepsilon} + S_n^1 \longrightarrow S_n^{-\varepsilon}$ has finite cokernel and its kernel is contained in $S_n^1$.*
4. *The map $S_n^+ + S_n^- \longrightarrow S_n$ has finite cokernel and its kernel is contained in $S_n^1$.*

*Proof.* Part (1) follows from the fact that $(\omega_n^{\varepsilon}, \tilde{\omega}_n^{-\varepsilon})/(\omega_n)$ is finite. To see part (2), note that if $\sigma \in S_n^{\varepsilon}$ is killed by $\tilde{\omega}_n^{-\varepsilon}$, then the restriction of $\sigma$ to any $\mathfrak{p}$ over $p$ will lie in

$$\left(E^+(K_{n,\mathfrak{p}}) \otimes \mathbf{Q}_p/\mathbf{Z}_p\right) \cap \left(E^-(K_{n,\mathfrak{p}}) \otimes \mathbf{Q}_p/\mathbf{Z}_p\right) = E(K_\mathfrak{p}) \otimes \mathbf{Q}_p/\mathbf{Z}_p.$$

Part (3) follows similarly. Part (4) is [8, Proposition 10.1]. □

**Lemma 7.5.** *Assuming (W),* $\mathrm{corank}_{\mathbf{Z}_p} S_n^1$ *is bounded independent of $n$.*

*Proof.* Since $\mathrm{coker}\left(S_n^0 \longrightarrow S_n^1\right)$ has $\mathbf{Z}_p$-rank bounded by $d$, it suffices to check that $\mathrm{corank}_{\mathbf{Z}_p} S_n^0$ is bounded. By Theorem 3.1, we have that

$$\mathrm{rk}_{\mathbf{Z}_p} S_n(T) - \mathrm{rk}_{\mathbf{Z}_p} S_{n,\Sigma}(T) + \mathrm{rk}_{\mathbf{Z}_p} X_{\Gamma_n} = \mathrm{rk}_{\mathbf{Z}_p} \widehat{E}(K_{n,p}) + \mathrm{rk}_{\mathbf{Z}_p} X_n.$$

By (W), $\mathrm{rk}_\Lambda X = d$ and hence $\mathrm{rk}_{\mathbf{Z}_p} X_{\Gamma_n} = d \cdot p^n + \mathrm{O}(1)$. Furthermore, we have that

$$\mathrm{rk}_{\mathbf{Z}_p} S_n(T) = \mathrm{rk}_{\mathbf{Z}_p} X_n, \quad \mathrm{rk}_{\mathbf{Z}_p} S_{n,\Sigma}(T) = \mathrm{rk}_{\mathbf{Z}_p} S_n^0 \quad \text{and} \quad \mathrm{rk}_{\mathbf{Z}_p} \widehat{E}(K_{n,p}) = d \cdot p^n.$$

Hence, $\mathrm{corank}_{\mathbf{Z}_p} S_n^0$ is $\mathrm{O}(1)$ (i.e. bounded). □

**Lemma 7.6.** *Assuming (W), for $\varepsilon = (-1)^n$,*

$$\operatorname{corank}_{\mathbf{Z}_p} (S_n^{\varepsilon})^{\omega_n^{\varepsilon}=0} + \operatorname{corank}_{\mathbf{Z}_p} \left(S_{n-1}^{-\varepsilon}\right)^{\omega_n^{-\varepsilon}=0} = \operatorname{corank}_{\mathbf{Z}_p} S_n + O(1).$$

*Proof.* By Lemma 7.5 and part (4) of Lemma 7.4,

$$\operatorname{corank}_{\mathbf{Z}_p} S_n^{\varepsilon} + \operatorname{corank}_{\mathbf{Z}_p} S_n^{-\varepsilon} = \operatorname{corank}_{\mathbf{Z}_p} S_n + \mathrm{O}(1).$$

By part (1) and part (2) of Lemma 7.4 and by Lemma 7.5,

$$\operatorname{corank}_{\mathbf{Z}_p} (S_n^{\varepsilon})^{\omega_n^{\varepsilon}=0} \operatorname{corank}_{\mathbf{Z}_p} \left(S_n^{-\varepsilon}\right)^{\omega_n^{-\varepsilon}=0} = \operatorname{corank}_{\mathbf{Z}_p} S_n + \mathrm{O}(1).$$

Finally, by Lemma 7.5 and part (3) of Lemma 7.4,

$$\operatorname{corank}_{\mathbf{Z}_p} (S_n^{\varepsilon})^{\omega_n^{\varepsilon}=0} \operatorname{corank}_{\mathbf{Z}_p} \left(S_{n-1}^{-\varepsilon}\right)^{\omega_n^{-\varepsilon}=0} = \operatorname{corank}_{\mathbf{Z}_p} S_n + \mathrm{O}(1).$$

□

*Proof of Proposition 7.1.* For any $m$, by Theorem 6.8,

$$\begin{aligned} \operatorname{corank}_{\mathbf{Z}_p} (S_m^{\varepsilon})^{\omega_m^{\varepsilon}=0} &= \operatorname{rk}_{\mathbf{Z}_p}(X^{\varepsilon}/\omega_m^{\varepsilon} X^{\varepsilon}) + \mathrm{O}(1) \\ &= r^{\varepsilon} \cdot \operatorname{rk}_{\mathbf{Z}_p} (\Lambda/\omega_m^{\varepsilon}\Lambda) + \mathrm{O}(1) \\ &= r^{\varepsilon} \cdot q_m + \mathrm{O}(1). \end{aligned}$$

Taking $m = n$ and $n-1$, together with Lemma 7.6, yields the proposition. □

When $\operatorname{corank}_{\mathbf{Z}_p} S_n$ is bounded, we will see that $X^+$ and $X^-$ are $\Lambda$-torsion. We introduce this condition as another hypothesis.

- **Hypothesis B** (for bounded): $\operatorname{corank}_{\mathbf{Z}_p}(S_n)$ is bounded.

**Lemma 7.7.** *(B) implies (W).*

*Proof.* Let $r = \operatorname{rk}_{\Lambda} X$. By Proposition 5.3 it suffices to check that $r = d$. We have that $\operatorname{rk}_{\mathbf{Z}_p} \widehat{E}(K_{n,p}) = dp^n$ and by the theory of $\Lambda$-modules, $\operatorname{rk}_{\mathbf{Z}_p} X_{\Gamma_n}$ grows like $rp^n$. Then from Theorem 3.1 and (B), we can conclude $r = d$ completing the proof. □

**Corollary 7.8.** *Hypothesis (B) holds if and only if $X^+$ and $X^-$ are torsion $\Lambda$-module.*

*Proof.* If $X^+$ or $X^-$ are not torsion then by Theorem 6.8, (B) must fail. Conversely, if (B) holds then (W) holds. Hence, by Proposition 7.1, $r^+ = r^- = 0$ and $X^{\pm}$ is torsion. □

## 7.2 $p$-cyclotomic zeroes of $L_p^{\pm}(E, K_\infty/K, X)$

We now relate certain zeroes of the $p$-adic $L$-function $L_p^{\pm}(E, K_\infty/K, X)$ to the corank of $S_n$. Denote by $\zeta_n$ a primitive $p^n$-th root of unity and let $\xi_n = \Phi_n(1+X)$.

**Lemma 7.9.** *Let $u_j = (u_{1j}, \ldots, u_{dj}) \in \Lambda^d$ for $j = 1, \ldots, d$. Then we have $(\Lambda/\xi_n)^d/(u_1, \ldots, u_d)$ is finite if and only if $\det(u_{ij}(\zeta_n - 1)) \neq 0$. When this occurs*

$$\mathrm{ord}_p\left(\#\frac{(\Lambda/\xi_n)^d}{(u_1, \ldots, u_d)}\right) = \mu(f)\cdot(p^n - p^{n-1}) + \lambda(f)$$

*where $f = \det(u_{ij})$ and $n$ is sufficiently large.*

*Proof.* Set $u_j(\zeta_n - 1) = (u_{1j}(\zeta_n - 1), \ldots, u_{dj}(\zeta_n - 1))$ and then

$$\frac{(\Lambda/\xi_n)^d}{(u_1, \ldots, u_d)} \cong \frac{\mathbf{Z}_p[\mu_{p^n}]^d}{(u_1(\zeta_n - 1), \ldots, u_d(\zeta_n - 1))}.$$

By linear algebra, the left hand side is finite if and only if $\det(u_{ij}(\zeta_n - 1)) \neq 0$. Furthermore, when these groups are finite, they have size $(p^n - p^{n-1}) \cdot \mathrm{ord}_p(\det(u_{ij}(\zeta_n - 1)))$ since $p$ is totally ramified in $\mathbf{Z}_p[\mu_{p^n}]$. Our result then follows since for any non-zero $g \in \Lambda$,

$$\mathrm{ord}_p(g(\zeta_n - 1)) = \mu(g) + \frac{\lambda(g)}{(p^n - p^{n-1})}$$

for $n$ large enough. □

**Proposition 7.10.** *We have that*

1. *$L_p^+(E, K_\infty/K, 0) \neq 0$ and $L_p^-(E, K_\infty/K, 0) \neq 0$ if and only if $S_0$ is finite.*
2. *For $n > 1$, $L_p^{\varepsilon}(E, K_\infty/K, \zeta_n - 1) \neq 0$ for $\varepsilon = (-1)^n$ if and only if $S_n/S_{n-1}$ is finite.*

*Proof.* We prove this for even $n > 1$; the other cases follow similarly. Consider the diagram

$$\begin{array}{ccccccc} \widehat{E}(K_{n,p}) & \xrightarrow{Q_n} & X_{\Gamma_n} & \longrightarrow & X_n & \longrightarrow & 0 \\ {\scriptstyle \mathrm{Tr}^n_{n-1}}\downarrow & & \downarrow{\scriptstyle \pi_n} & & \downarrow & & \\ \widehat{E}(K_{n-1,p}) & \xrightarrow{Q_{n-1}} & X_{\Gamma_{n-1}} & \longrightarrow & X_{n-1} & \longrightarrow & 0 \end{array} \tag{23}$$

Then $S_n/S_{n-1}$ is finite if and only if $\ker(\pi_n)/Q_n(\ker(\mathrm{Tr}^n_{n-1}))$ is finite by Corollary 4.12. We have that $\ker(\pi_n) \cong \omega_{n-1}X/\omega_n X$ and from (18)

$$0 \longrightarrow \frac{\omega_{n-1}Y}{\omega_n Y} \longrightarrow \frac{\omega_{n-1}X}{\omega_n X} \longrightarrow \frac{\omega_{n-1}Z}{\omega_n Z} \longrightarrow 0. \tag{24}$$

The map $R_n$ restricted to $\ker(\mathrm{Tr}^n_{n-1})$ is given by the composite map

$$\ker(\mathrm{Tr}^n_{n-1}) \xrightarrow{Q_n} \frac{\omega_{n-1}X}{\omega_n X} \longrightarrow \frac{\omega_{n-1}Z}{\omega_n Z} \longrightarrow \left(\frac{\omega_{n-1}\Lambda}{\omega_n\Lambda}\right)^d. \tag{25}$$

Now by Corollary 4.12, $\{\omega^+_{n-2}d_{n,j}\}_{j=1}^d$ generates $\ker(\mathrm{Tr}^n_{n-1})$ and we have that $R_n(\omega^+_{n-2}d_{n,j}) = \omega_{n-1}\cdot(u^n_{1j},\dots,u^n_{dj})$. Set $u^n_j = (u^n_{1j},\dots,u^n_{dj}) \in (\Lambda/\xi_n)^d$.

First we consider the case where $t_Y(\zeta_n - 1) = 0$. Then by definition $L^+_p(E, K_\infty/K, \zeta_n - 1) = 0$ and we need to check that $S_n/S_{n-1}$ is infinite. Since $t_Y(\zeta_n - 1) = 0$, we have that $\omega_{n-1}Y/\omega_n Y$ is infinite. Then by Proposition 6.1 and (24)

$$\mathrm{rk}_{\mathbf{Z}_p}(\omega_n X/\omega_{n-1}X) > d\cdot(p^n - p^{n-1}).$$

But $\mathrm{rk}_{\mathbf{Z}_p}\left(\ker(\mathrm{Tr}^n_{n-1})\right) = d\cdot(p^n - p^{n-1})$ and hence $S_n/S_{n-1}$ is infinite from (23).

So we may assume that $t_Y(\zeta_n - 1) \neq 0$. Then $L^+_p(E, K_\infty/K, \zeta_n - 1) \neq 0$ is equivalent to $\det(u^n_{ij}(\zeta_n - 1)) \neq 0$ which by Lemma 7.9 is equivalent to $(\Lambda/\xi_n)^d/(u^n_1,\dots,u^n_d)$ being finite. Since the last two maps in (25) have finite kernel and cokernel, these last statements are equivalent to

$$\frac{\omega_n X/\omega_{n-1}X}{(Q_n(d_{n,1}),\dots,Q_n(d_{n,d}))} = \frac{\ker(\pi_n)}{Q_n(\ker(\mathrm{Tr}^n_{n-1}))} \text{ being finite.}$$

Then by (23), this is equivalent to $S_n/S_{n-1}$ being finite completing the proof. □

**Corollary 7.11.** *$L^+_p(E, K_\infty/K, X) \neq 0$ and $L^-_p(E, K_\infty/K, X) \neq 0$ if and only if $\mathrm{corank}_{\mathbf{Z}_p}(S_n)$ is bounded.*

*Proof.* The result follows from Proposition 7.10 and the fact that a non-zero element of $\Lambda$ has finitely many zeroes. □

## 7.3 Case of bounded rank

Throughout this subsection, we will assume (B) and obtain formulas describing the growth of $S_n$ along $K_\infty/K$.

**Definition 7.12.** Assuming (B) (so that $L^\pm_p(E, K_\infty/K, X)$ is non-zero) define

$$\lambda^\pm = \lambda^\pm_E(K_\infty/K) = \lambda(L^\pm_p(E, K_\infty/K, X))$$

and

$$\mu^\pm = \mu^\pm_E(K_\infty/K) = \mu(L^\pm_p(E, K_\infty/K, X)).$$

We begin with a general lemma about the "growth" of torsion $\Lambda$-modules.

**Lemma 7.13.** *If $Y$ is a torsion $\Lambda$-module then for $n$ large enough $\omega_{n-1}Y/\omega_n Y$ is finite of size $\mu(Y)\cdot(p^n - p^{n-1}) + \lambda(Y) - \mathrm{rk}_{\mathbf{Z}_p}(Y_{\Gamma_n})$.*

*Proof.* By the structure theory of $\Lambda$-modules, we may assume that $Y$ is of the form $\Lambda/f^e$ with $f$ an irreducible polynomial. (Note that any finite groups that appear are killed by $\omega_n$ for $n$ large enough.) If $\gcd(f,\omega_n)=1$ then

$$\frac{\omega_{n-1}Y}{\omega_n Y}\cong\frac{Y}{\xi_n Y}\cong\frac{\Lambda}{(f^e,\xi_n)}\cong\frac{\mathbf{Z}_p[\mu_{p^n}]}{f^e(\zeta_n-1)}.$$

Now

$$\begin{aligned}\operatorname{ord}_p\left(\#\frac{\mathbf{Z}_p[\mu_{p^n}]}{f^e(\zeta_n-1)}\right)&=(p^n-p^{n-1})\cdot\operatorname{ord}_p(f^e(\zeta_n-1))\\&=(p^n-p^{n-1})\cdot\mu(f^e)+\lambda(f^e)\end{aligned}$$

which implies the lemma since $\operatorname{rk}_{\mathbf{Z}_p}(Y_{\Gamma_n})=0$.

If $f=\xi_k$ for some $k\le n$ then

$$\frac{\omega_{n-1}Y}{\omega_n Y}\cong\frac{\Lambda}{(\xi_k^{e-1},\xi_n)}\cong\frac{\mathbf{Z}_p[\mu_{p^n}]}{\xi_k^{e-1}(\zeta_n-1)}$$

and the lemma follows since $\operatorname{rk}_{\mathbf{Z}_p}(Y_{\Gamma_n})=\deg(\xi_k)$. □

The following duality theorem will be needed in what follows. Let

$$S_n^0(T)=\operatorname{Sel}^0(T_pE/K_n)=\ker\left(S_n(T)\longrightarrow\prod_{\mathfrak{p}|p}E(K_{n,\mathfrak{p}})\otimes\mathbf{Z}_p\right)$$

so that $S_{n,\Sigma}(T)\subseteq S_n^0(T)\subseteq S_n(T)$.

**Theorem 7.14.** *Let $Y$ be the $\Lambda$-torsion submodule of $X$. Then assuming (W), $Y$ is pseudo-isomorphic to $\operatorname{Sel}_p^0(E[p^\infty]/K_\infty)^\wedge$. In particular, $\operatorname{rk}_{\mathbf{Z}_p}Y_{\Gamma_n}=\operatorname{rk}_{\mathbf{Z}_p}S_n^0(T)=\operatorname{rk}_{\mathbf{Z}_p}S_{n,\Sigma}(T)$.*

*Proof.* The first statement is Corollary 2.5 in [24]. For the second statement, let $S_\infty^0=\operatorname{Sel}_p^0(E[p^\infty]/K_\infty)$ and $S_n^0=\operatorname{Sel}_p^0(E[p^\infty]/K_n)$. Then by [9, Remark 4.4], $S_n^0$ and $\left(S_\infty^0\right)^{\Gamma_n}$ differ only by finite groups. Therefore,

$$\operatorname{rk}_{\mathbf{Z}_p}Y_{\Gamma_n}=\operatorname{corank}_{\mathbf{Z}_p}\left(S_\infty^0\right)^{\Gamma_n}=\operatorname{corank}_{\mathbf{Z}_p}S_n^0=\operatorname{rk}_{\mathbf{Z}_p}S_n^0(T).$$

Since, $E(K_{n,v})\otimes\mathbf{Z}_p$ is finite for $v\nmid p$, we have that $\operatorname{rk}_{\mathbf{Z}_p}S_n^0(T)=\operatorname{rk}_{\mathbf{Z}_p}S_{n,\Sigma}(T)$ completing the proof. □

**Theorem 7.15.** *Assuming (B), we have that*

$$\operatorname{ord}_p\left(\#(S_n/S_{n-1})\right)=\begin{cases}\mu^+\cdot(p^n-p^{n-1})+(\lambda^+-s)\cdot n+d\cdot q_n & 2|n\\ \mu^-\cdot(p^n-p^{n-1})+(\lambda^--s)\cdot n+d\cdot q_n & 2\nmid n\end{cases}$$

*where $s$ is the stable value of $\operatorname{corank}_{\mathbf{Z}_p}S_k$ and $n$ is sufficiently large.*

*Proof.* Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{S_n(T)}{S_{n,\Sigma}(T)} & \longrightarrow & B_n \times \widehat{E}(K_{n,p}) & \xrightarrow{Q_n} & X_{\Gamma_n} & \longrightarrow & X_n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \frac{S_{n-1}(T)}{S_{n-1,\Sigma}(T)} & \longrightarrow & B_{n-1} \times \widehat{E}(K_{n-1,p}) & \xrightarrow{Q_{n-1}} & X_{\Gamma_{n-1}} & \longrightarrow & X_{n-1} & \longrightarrow & 0 \end{array}$$

defined by Theorem 3.1. For $n$ large enough, $S_n(T), S_{n,\Sigma}(T)$ and $B_n$ stabilize and the vertical maps in the above diagram between these groups become multiplication by $p$.

We will break the above diagram into two pieces; namely

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{S_n(T)}{S_{n,\Sigma}(T)} & \longrightarrow & B_n \times \widehat{E}(K_{n,p}) & \longrightarrow & M_n & \longrightarrow & 0 \\ & & \cdot p \downarrow & & \cdot p \times \mathrm{Tr}_{n-1}^n \downarrow & & \downarrow m_n & & \\ 0 & \longrightarrow & \frac{S_{n-1}(T)}{S_{n-1,\Sigma}(T)} & \longrightarrow & B_{n-1} \times \widehat{E}(K_{n-1,p}) & \longrightarrow & M_{n-1} & \longrightarrow & 0 \end{array} \tag{26}$$

and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_n & \xrightarrow{Q_n} & X_{\Gamma_n} & \longrightarrow & X_n & \longrightarrow & 0 \\ & & m_n \downarrow & & \downarrow & & \downarrow \pi_n & & \\ 0 & \longrightarrow & M_{n-1} & \xrightarrow{Q_{n-1}} & X_{\Gamma_{n-1}} & \longrightarrow & X_{n-1} & \longrightarrow & 0 \end{array} \tag{27}$$

where $M_n$ is defined by the above diagrams. If $s_0 = \mathrm{rk}_{\mathbf{Z}_p} S_{n,\Sigma}(T)$ and $h = \mathrm{rk}_{\mathbf{F}_p} B_n/pB_n$ then applying the snake lemma to (26) yields

$$\begin{aligned} 0 \longrightarrow & (\mathbf{Z}/p\mathbf{Z})^h \times \ker(\mathrm{Tr}_{n-1}^n) \longrightarrow \ker(m_n) \longrightarrow (\mathbf{Z}/p\mathbf{Z})^{s-s_0} \longrightarrow \\ & (\mathbf{Z}/p\mathbf{Z})^h \times \mathrm{coker}(\mathrm{Tr}_{n-1}^n) \longrightarrow \mathrm{coker}(m_n) \longrightarrow 0. \end{aligned}$$

By Corollary 4.12, $\mathrm{coker}(\mathrm{Tr}_{n-1}^n) \cong (\mathbf{Z}/p\mathbf{Z})^{dq_n}$ and therefore we have that

$$\ker(m_n) \cong \ker(\mathrm{Tr}_{n-1}^n) \times (\mathbf{Z}/p\mathbf{Z})^{h+a} \tag{28}$$

and

$$\mathrm{coker}(m_n) \cong (\mathbf{Z}/p\mathbf{Z})^{dq_n+h-s+s_0+a} \tag{29}$$

for some $a$ between 0 and $s - s_0$. Applying the snake lemma to (27) yields

$$0 \longrightarrow \ker(m_n) \longrightarrow \frac{\omega_{n-1}X}{\omega_n X} \longrightarrow (S_n/S_{n-1})^\wedge \longrightarrow \mathrm{coker}(m_n) \longrightarrow 0. \tag{30}$$

For $n$ large enough, $S_n/S_{n-1}$ and $\frac{\omega_{n-1}Y}{\omega_n Y}$ are both finite and

$$\begin{aligned} \left[\frac{\omega_{n-1}X}{\omega_n X} : \ker(\mathrm{Tr}_{n-1}^n)\right] &= \#\left(\frac{\omega_{n-1}Y}{\omega_n Y}\right) \cdot \left[\frac{\omega_{n-1}Z}{\omega_n Z} : \ker(\mathrm{Tr}_{n-1}^n)\right] \\ &= \#\left(\frac{\omega_{n-1}Y}{\omega_n Y}\right) \cdot \left[\frac{\omega_{n-1}\Lambda}{\omega_n \Lambda} : \ker(\mathrm{Tr}_{n-1}^n)\right] \\ &= \#\left(\frac{\omega_{n-1}Y}{\omega_n Y}\right) \cdot \#\left(\frac{(\Lambda/\xi_n)^d}{(u_1^n, \ldots, u_d^n)}\right). \end{aligned}$$

Again, for $n$ large enough, $L_p^{\pm}(E, K_\infty/K, \zeta_n - 1) \neq 0$ and hence $\det(u_{ij}^n(\zeta_n - 1)) \neq 0$. Also, by Lemma 7.9,

$$\mathrm{ord}_p\left(\#\frac{(\Lambda/\xi_n)^d}{(u_1^n, \ldots, u_d^n)}\right) = (\mu^\varepsilon - \mu_t)\cdot(p^n - p^{n-1}) + \lambda^\varepsilon - \lambda_t \tag{31}$$

where $\lambda_t = \lambda(t_Y)$, $\mu_t = \mu(t_Y)$ and $\varepsilon = (-1)^n$. Then, by Lemma 7.13, we have that

$$\mathrm{ord}_p\left(\#\frac{\omega_{n-1}Y}{\omega_n Y}\right) = \mu_t \cdot (p^n - p^{n-1}) + \lambda_t - \mathrm{rk}_{\mathbf{Z}_p}(Y_{\Gamma_n})$$

for $n$ large enough. Thus,

$$\mathrm{ord}_p\left[\frac{\omega_{n-1}X}{\omega_n X} : \ker(\mathrm{Tr}_{n-1}^n)\right] = \mu^\varepsilon \cdot (p^n - p^{n-1}) + \lambda^\varepsilon - \mathrm{rk}_{\mathbf{Z}_p}(Y_{\Gamma_n}).$$

Returning to (30), we can compute

$$\begin{aligned}
\mathrm{ord}_p\left(\#S_n/S_{n-1}\right) &= \mathrm{ord}_p\left[\frac{\omega_{n-1}X}{\omega_n X} : \ker(m_n)\right] + \mathrm{ord}_p(\#\,\mathrm{coker}(m_n)) \\
&= -a - h + \mathrm{ord}_p\left[\frac{\omega_{n-1}X}{\omega_n X} : \ker(\mathrm{Tr}_{n-1}^n)\right] + \mathrm{ord}_p(\#\,\mathrm{coker}(m_n)) \\
&= \mu^\varepsilon \cdot (p^n - p^{n-1}) + \lambda^\varepsilon - \mathrm{rk}_{\mathbf{Z}_p}(Y_{\Gamma_n}) + dq_n - s + s_0
\end{aligned}$$

Finally, from Theorem 7.14, we have that $s_0 = \mathrm{rk}_{\mathbf{Z}_p}(Y_{\Gamma_n})$ which completes the proof of the theorem. □

# References


[1] C. Cornut, Mazur's conjecture on higher Heegner points, Invent. Math. **148** (2002), no. 3, 495–523.

[2] R. Greenberg, Introduction to Iwasawa theory for elliptic curves, in *Arithmetic algebraic geometry (Park City, UT, 1999)*, 407–464, Amer. Math. Soc., Providence, RI, 2001.

[3] R. Greenberg, Iwasawa theory for elliptic curves, in *Arithmetic theory of elliptic curves (Cetraro, 1997)*, 51–144, Lecture Notes in Math., 1716, Springer, Berlin, 1999.

[4] R. Greenberg, Iwasawa theory for $p$-adic representations, in *Algebraic number theory*, Adv. Stud. Pure Math., 17, Academic Press, Boston, MA, 1989.

[5] R. Greenberg, Iwasawa theory for $p$-adic representations II, preprint.

[6] R. Greenberg, On the Birch and Swinnerton-Dyer conjecture, Invent. Math. **72** (1983), 241–265.

[7] K. Kato, $p$-adic Hodge theory and values of zeta functions of modular forms, preprint.

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

[9] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, Invent. Math. **149** (2002), 195–224.

[10] M. Hazewinkel, On norm maps for one dimensional formal groups. III, Duke Math. J. **44** (1977), no. 2, 305–314.

[11] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Invent. Math. **18** (1972), 183–266.

[12] B. Mazur, J. Tate and J. Teitelbaum, On $p$-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math. **84** (1986), no. 1, 1–48.

[13] B. Perrin-Riou, Théorie d'Iwasawa $p$-adique locale et globale. (French) [Local and global $p$-adic Iwasawa theory], Invent. Math. **99** (1990), no. 2, 247–292.

[14] B. Perrin-Riou, Fonctions $L$ $p$-adiques d'une courbe elliptique et points rationnels [$p$-adic $L$-functions of an elliptic curve and rational points] Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 945–995.

[15] B. Perrin-Riou, Théorie d'Iwasawa des représentations $p$-adiques sur un corps local [Iwasawa theory of $p$-adic representations over a local field], Invent. Math. **115** (1994), no. 1, 81–161.

[16] B. Perrin-Riou, Arithmétique des courbes elliptiques á réduction supersingulière en $p$, Experiment. Math. **12** (2003), no. 2, 155–186.

[17] R. Pollack, On the $p$-adic $L$-function of a modular form at a supersingular prime, Duke Math. J. **118** (2003), no. 3, 523–558.

[18] R. Pollack, An algebraic version of a theorem of Kurihara, preprint.

[19] K. Rubin, Euler systems and modular elliptic curves, in *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, 351–367, Cambridge Univ. Press, Cambridge, 1998.

[20] P. Schneider, $p$-adic height pairings. II, Invent. Math. **79** (1985), no. 2, 329–374.

[21] J. H. Silverman, *The arithmetic of elliptic curves*, Corrected reprint of the 1986 original, Springer, New York, 1992.

[22] J. Tate, Duality theorems in Galois cohomology over number fields, in *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, 288–295, Inst. Mittag-Leffler, Djursholm, 1963.

[23] V. Vatsal, Uniform distribution of Heegner points, Invent. Math. **148** (2002), no. 1, 1–46.

[24] K. Wingberg, Duality theorems for abelian varieties over $\mathbf{Z}_p$-extensions, in *Algebraic number theory*, 471–492, Adv. Stud. Pure Math., 17, Academic Press, Boston, MA, 1989.