Non-commutative Iwasawa theory of elliptic curves at primes of multiplicative reduction.

Chern-Yang LEE
Emmanuel College

This dissertation is submitted for the degree of
Doctor of Philosophy at the
University of Cambridge
April 2010

Declaration

This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements.

Dedicated to Sek-Khuan Lee and Nga-Fong Toh

Abstract

Let E be an elliptic curve defined over the rationals $\mathbb{Q}$, and p be a prime at least 5 where E has multiplicative reduction. This thesis studies the Iwasawa theory of E over certain false Tate curve extensions F_∞, with Galois group $G = Gal(F_\infty/\mathbb{Q})$. I show how the p^∞-Selmer group of E over F_∞ controls the p^∞-Selmer rank growth within the false Tate curve extension, and how it is connected to the root numbers of E twisted by absolutely irreducible orthogonal Artin representations of G, and investigate the parity conjecture for twisted modules.

Title:
Non-commutative Iwasawa theory of elliptic curves at primes of multiplicative reduction.

Author:
Chern-Yang LEE

Introduction

The Iwasawa main conjectures for elliptic curves provide a scope to study Birch and Swinnerton-Dyer conjecture. For a fix prime p, on the algebraic side, one studies the structure of the Iwasawa module $X_p(E/F_\infty)$, which is the Pontryagin dual of the p^∞-Selmer group of the elliptic curve E over a p-adic Lie extension F_∞ of the base number field F over which E is defined. On the analytic side, one expects the existence of a p-adic L-function, interpolating the special values of complex L-functions. Main conjecture asserts certain coincidence of both the algebraic module and the p-adic L-function.

There have been quite a number of cases studied by many experts, in either the algebraic modules or the p-adic L-functions. There seems to have a common level of difference when the prime p varies by its reduction type for E, (assuming naively that E has the same reduction type at each place of F above p), or when the p-adic Lie extension F_∞ varies. Out of the reduction types, good ordinary reduction has been most studied along with many different p-adic Lie extensions, for instance when $F_\infty = F^{cyc}/F$ by Mazur [20], $F_\infty = F(E_{p^\infty})$ by Coates-Fukaya-Kato-Sujatha-Venjakob [4] and $F_\infty =$ 'False Tate curve extensions' by Coates-Fukaya-Kato-Sujatha [3].

Let G denote the Galois group of the p-adic Lie extension F_∞/F and Λ denote the corresponding Iwasawa algebra. Mazur conjectured that the Selmer module $X_p(E/F^{cyc})$ is Λ-torsion when E has good ordinary reduction over places of F above p. This is proved in some of the cases of F, or under other assumptions. It is further expected that $X_p(E/F_\infty)$ is Λ-torsion for many other p-adic Lie extensions. However, when the p-adic Lie extension is not abelian, for instance when $F_\infty = F(E_{p^\infty})$ with E an elliptic curve without complex multiplication, being Λ-torsion alone is not sufficient to formulate a main conjecture.

In [4], the authors introduce a stronger assumption, called $\mathfrak{M}_H(G)$-Conjecture, asserting that the algebraic module $X_p(E/F_\infty)$ should belong to the category $\mathfrak{M}_H(G)$. Equivalently, it means $Y_p(E/F_\infty)$, the quotient module of $X_p(E/F_\infty)$ by its p-primary part, is finitely generated over the Iwasawa algebra of H, where H is the subgroup of G which fixes F^{cyc}. This $\mathfrak{M}_H(G)$-Conjecture allows one to attach a characteristic element to the module and go further to formulate the main conjecture.

In [3], the alliance took the belief of $\mathfrak{M}_H(G)$-Conjecture over to study Iwasawa Theory for E over certain False Tate curve extension F_∞/F, which is a non-commutative p-adic Lie group of dimension 2, where E is any elliptic curve defined over any number field F that has good ordinary reduction over all places of F above the odd prime p. The field F_∞ is defined from an element $m \in F^\times$, with certain constraints relating to the reductions of E. By $\mathfrak{M}_H(G)$-Conjecture, they define an algebraic invariant τ being the rank of $Y_p(E/F_\infty)$ over the Iwasawa algebra of H_K, where H_K is the subgroup of $G = Gal(F_\infty/F)$ which fixes $F(\mu_{p^\infty})$. This τ seems to have a lot of control over the arithmetics of E over the intermediate fields. When τ is odd, it guarantees and give lower bounds for the Selmer rank growth in both the cyclotomic direction and radical direction. When $\tau = 1$, the corresponding bounds are hit and one can decide the Selmer rank of the elliptic curve over infinitely many intermediate number fields. The authors also consider the root number of the elliptic curve E twisted by all irreducible orthogonal Artin representations of G and show their connection to τ and prove a parity conjecture of the twisted modules.

In this thesis, I study the parallel results as [3] under the setting of a triple (E, p, m), where E is an elliptic curve defined over $F = \mathbb{Q}$, having semistable reduction at all prime divisors of the integer $m > 1$. The main difference is that I assume E has multiplicative reduction at the odd prime $p \geq 5$, instead of good ordinary reduction. These assumptions are made in Section 1.1, which is mentioned as assumptions on (E, p, m) in several places throughout the thesis.

In chapter 2, I start by introducing the all-important $\mathfrak{M}_H(G)$-Conjecture and some direct consequences from it and compute the $\mathbb{Z}_p$-coranks of several modules under this Conjecture. These computations will lead to a formula to obtain

the marvelous but 'conjectural' value τ.

In chapter 3, I have a thorough investigation over the $\bar{\mathbb{Q}}_p$-irreducible Artin representations which factors through $\mathbb{Q}(\mu_{p^n}, \sqrt[p^n]{m})$. I use V.Dokchitser's formula [8] to compute the root numbers of the elliptic curve twisted by these Artin-representations. By Greenberg[9]-Guo[10], these root numbers are again controlled by the parity of τ from the formula established in chapter 2.

In chapter 4, we once again relate the value τ to λ_n, the λ-invariant of the finitely generated torsion module $X_p(E/L_n^{cyc})$ where $L_n = \mathbb{Q}(\sqrt[p^n]{m})$ for $n \geq 1$ via two approaches in computing the homological rank of $Y_p(E/F_\infty)$. By Greenberg-Guo, this relation leads to the control of growth of p^∞-Selmer ranks within the False Tate curve tower by the value τ. I give an assertion on when the parity conjecture of twisted modules holds.

Acknowledgements

Above all, I would like to express my gratitude to my supervisor Prof. John Coates, for always being my largest source of support, confidence and encouragements throughout the years that I have been in Cambridge. He never fails in motivating me when it is most needed. His advice and guidance are very encouraging and beneficial to me. I appreciate his patience in correcting me numerous times when I had not understood well enough. I am particularly grateful that John gave extremely careful readings on my manuscripts and pointed out my errors and room of improvements.

Apart from the general guidance of my supervisor, the work in this thesis was greatly assisted by the the following advice from other mathematicians. First, I would like to thank Christian Wuthrich for referring me to Jones' paper [14] which leads to computing the λ-invariant of the p^∞-Selmer group of an elliptic curve over $\mathbb{Q}(\mu_{p^\infty})$. Christian taught me SAGE by providing me some relevant computations as examples, and has been very responsive to my questions by email. I would like to thank Tim Dokchitser for providing me his Magma command in computing the Hasse-Weil L-value of an elliptic curve over a number field and numerous troubleshooting and help with my calculations in Magma. Also, I am grateful to Tom Fisher for introducing me a Pari-GP command by Denis Simon which searches rational points of infinite order on an elliptic curve over a number field, which successfully led me to the examples given at the end of the thesis.

I would like to dedicate this thesis to my dearest parents, Sek-Khuan and Nga-Fong, not only for being the main financial support of my PhD life, but also for their confidence in me in pursuing my dream. I would like to add here my appreciation of the love and patience by Choonpei, who from being my girlfriend till becoming my wife, taking very good care of me on daily basis, and sharing my joy during the process of the writing up.

I am grateful to have some moments free of financial burdens with the very generous funds by Cambridge Commonwealth Trusts and Emmanuel College. I would like to thank a very special person, Dato Seri Joseph Chong, for sponsoring my whole undergraduate studies in Peking University and my Part III course

in the University of Cambridge.

I would like to thank the Department of Pure Mathematics and Mathematical Statistics for providing such a wonderful academic environment and the departmental administrator Sally Lowe for solving every administration problem. Finally, I wish to thank the Chinese Educational Body in Malaysia and my secondary school, Chong Hwa High School Kluang for providing me the best education in Malaysia!

Contents

Chapter 1

Setting and Background

1.1 The False Tate Curve Extension

Let p be a fixed odd prime. We denote by μ_{p^n} the group of p^n-th roots of unity, and μ_{p^∞} the group of p-power roots of unity.

Definition:. *For any number field L, we denote by L^{cyc} the p-cyclotomic extension of L and Γ_L the Galois group $Gal(L^{cyc}/L)$. More precisely, it is the unique $\mathbb{Z}_p$-extension of L which is contained in $L(\mu_{p^\infty})$.*

Definition:. *For the fixed prime p, and any positive integer $m \overset{def}{=} \prod {q_i}^{r_i}$, where q_i are distinct primes with $p \nmid r_i$, we introduce the notations*

$$F_n \overset{def}{=} \mathbb{Q}(\mu_{p^n}, \sqrt[p^n]{m}) \quad n \geq 0, \tag{1.1}$$

and we call the union

$$F_\infty \overset{def}{=} \bigcup_{n \geq 0} F_n \tag{1.2}$$

a false Tate curve extension over $\mathbb{Q}$. It is clearly a Galois extension of $\mathbb{Q}$.

Let E be an elliptic curve. In this paper, I shall study the Iwasawa Theory within the false Tate curve extension $F_\infty/\mathbb{Q}$ with the following assumptions on the triple (E, p, m), with prime decomposition $m = \prod {q_i}^{r_i}$.

Assumption on (E, p, m) :

1. E is defined over $\mathbb{Q}$,
2. $p \geq 5$,
3. E has (split or non-split) multiplicative reduction at p,
4. E has semi-stable reduction at all primes q_i dividing m.

Let us introduce more notations corresponding to the false Tate curve extension F_∞. For each $n \geq 0$, F_n is the composite of two subfields

$$K_n \stackrel{\text{def}}{=} \mathbb{Q}(\mu_{p^n}) \quad \textit{and} \quad L_n \stackrel{\text{def}}{=} \mathbb{Q}(\sqrt[p^n]{m}),$$

and we denote their respective unions by

$$K_\infty \stackrel{\text{def}}{=} \bigcup_n K_n \quad \textit{and} \quad L_\infty \stackrel{\text{def}}{=} \bigcup_n L_n.$$

I shall use the simpler notation $K \stackrel{\text{def}}{=} K_1$, and denote the following composite fields by

$$L'_n \stackrel{\text{def}}{=} KL_n \quad \textit{and} \quad L'_\infty \stackrel{\text{def}}{=} KL_\infty.$$

We denote by G the Galois group $Gal(F_\infty/\mathbb{Q})$. For any number field L contained in F_∞, we denote by $G_L \leq G$ the open subgroup which fixes L and $H_L \leq G$ the closed subgroup which fixes L^{cyc}, and simply by $H \stackrel{\text{def}}{=} H_\mathbb{Q}$. These groups are compact p-adic Lie groups.

1.2 Iwasawa algebras and their modules

Definition:. *For any compact p-adic Lie group $\mathcal{G}$, we define the Iwasawa algebra of $\mathcal{G}$ by*

$$\Lambda(\mathcal{G}) \stackrel{def}{=} \varprojlim_U \mathbb{Z}_p[\mathcal{G}/U] \tag{1.3}$$

where U runs through the open normal subgroups of $\mathcal{G}$ and the inverse limit is taken with respect to the canonical projective maps. In particular, for any

number field L, we denote the Iwasawa algebra of Γ_L *as*

$$\Lambda(\Gamma_L) \stackrel{def}{=} \varprojlim_n \mathbb{Z}_p[\Gamma_L/\Gamma_L^{p^n}] \tag{1.4}$$

where $\Gamma_L^{p^n}$ *runs through the open normal subgroups of* Γ_L *and the inverse limit is taken with respect to the canonical projective maps.*

If the compact p-adic Lie group $\mathcal{G}$ is pro-p, the Iwasawa algebra $\Lambda(\mathcal{G})$ is a local ring, with the unique maximal ideal the kernel of the augmentation map $\Lambda(\mathcal{G}) \longrightarrow \mathbb{F}_p$. If $\mathcal{G}$ in addition has no nontrivial element of order p, the Iwasawa algebra $\Lambda(\mathcal{G})$ is Noetherian and contains no nontrivial zero divisors.

The main purpose of this section is to introduce the structure theorem of finitely generated $\Lambda(\Gamma)$-torsion modules, where Γ denotes any compact p-adic Lie group isomorphic to $\mathbb{Z}_p$.

Let us denote by $\Lambda \stackrel{\text{def}}{=} Z_p[[T]]$, the ring of power series of one variable with coefficients in $\mathbb{Z}_p$. It is endowed with a complete topology described below:

The group ring $\mathbb{Z}_p[T]$ has a group topology defined on it, induced by principal ideals $\left((T+1)^{p^n}-1\right)$, $n \geq 0$ being a base of neighbourhoods of $0 \in \mathbb{Z}_p[T]$. Λ is simply the completion of this group ring under this topology, i.e:

$$\Lambda \cong \varprojlim_n \mathbb{Z}_p[T]/\left((T+1)^{p^n}-1\right).$$

Proposition 1.2.1. *We have a non-canonical isomorphism of algebras*

$$\Lambda(\Gamma) \cong \Lambda$$

induced by $\gamma \mapsto 1+T$*, where* γ *is any chosen topological generator of* Γ.

Definition:. *A* Λ*-module is said to be torsion if for each element of the module, there is a non-zero element in* Λ *annihilating it.*

Definition:. *Let* M*,* M' *be two finitely generated* Λ*-modules. We say* M *is*

pseudo isomorphic to M' and denote $M \overset{pseudo}{\sim} M'$ if there is a Λ-modules homomorphism $M \longrightarrow M'$ with finite kernel and cokernel.

This relation is an equivalence relation among finitely generated Λ-torsion modules.

Definition:. *A non-constant polynomial*

$$f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in \mathbb{Z}_p[T]$$

is called distinguished if $p \mid a_i$ for all $0 \leq i \leq n-1$.

The ring (or algebra) Λ is a unique factorization domain, with p and irreducible distinguished polynomials as the only irreducible elements, up to multiplication by a unit in Λ.

Theorem 1.2.1. *Structure Theorem [29, Theorem 13.12]*
Let M be a finitely generated Λ-module. Then

$$M \overset{pseudo}{\sim} \Lambda^r \oplus \left(\oplus_{i=1}^{s} \Lambda/(p^{n_i})\right) \oplus \left(\oplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\right), \tag{1.5}$$

where r, s, t, n_i, m_j are non-negative integers , and $f_j(T)$ is distinguished and irreducible.

Hence there's the direct corollary

Corollary 1.2.1. *Let M be a finitely generated Λ-torsion module. Then*

$$M \overset{pseudo}{\sim} \left(\oplus_{i=1}^{s} \Lambda/(p^{n_i})\right) \oplus \left(\oplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\right), \tag{1.6}$$

where s, t, n_i, m_j are non-negative integers, and $f_j(T)$ is distinguished and irreducible.

Definition:. *For any finitely generated Λ-torsion module M, with a pseudoiso-*

morphism given as in (1.6), we define an μ-invariant and a λ-invariant to it:

$$\mu_{\Lambda(\Gamma)}(M) \stackrel{def}{=} \sum_{i=1}^{s} n_i,$$

$$\lambda_{\Lambda(\Gamma)}(M) \stackrel{def}{=} \sum_{j=1}^{t} m_j \cdot deg(f_j).$$

A finitely generated $\Lambda(\Gamma)$-torsion module M is also a finitely generated $\mathbb{Z}_p$-module if and only if it has vanishing μ-invariant. In this case, its λ-invariant is just the $\mathbb{Z}_p$-rank of M.

For any H which is a pro-p p-adic Lie group without non-trivial elements of finite order, the Iwasawa algebra $\Lambda(H)$ has no non-trivial zero divisors and therefore admits a skew field of fractions, denote as $Q_\Lambda(H)$. In this paper, we will come across some abelian cases when $H \cong \mathbb{Z}_p$.

Definition:. *Let H be a pro-p p-adic Lie group without non-trivial elements of finite order. For any finitely generated $\Lambda(H)$-module M, we define*

$$rank_{\Lambda(H)} M \stackrel{def}{=} dim_{Q_\Lambda(H)}(Q_\Lambda(H) \otimes_{\Lambda(H)} M), \tag{1.7}$$

as the $\Lambda(H)$-rank of M.

In the case when $H \cong \mathbb{Z}_p$, M is $\Lambda(\mathbb{Z}_p)$-torsion if and only if it has zero $\Lambda(\mathbb{Z}_p)$-rank.

Definition:. *For any compact p-adic Lie group $\mathcal{G}$, for $i \geq 0$, we define the i-th cohomology group of $\mathcal{G}$ with coefficients in a left $\Lambda(\mathcal{G})$-module M as the image of the i-th right derived functor of $Hom_{\Lambda(\mathcal{G})}(\mathbb{Z}_p, *)$ of M, and denote it by $H^i(\mathcal{G}, M)$. Similarly, we define the i-th homology group of $\mathcal{G}$ with coefficients in a right $\Lambda(\mathcal{G})$-module M as the image of the i-th left derived functor of $\left(* \otimes_{\Lambda(\mathcal{G})} \mathbb{Z}_p\right)$ of M, and denote it by $H_i(\mathcal{G}, M)$.*

Definition:. *If there exists a natural number r such that $H_i(\mathcal{G}, M) = 0$ for all integers $i > r$ and every finitely generated $\Lambda(\mathcal{G})$-module M, we say that $\Lambda(\mathcal{G})$*

has finite p-homological dimension and denote the smallest such r by $hd_p(\mathcal{G})$ *and call it the p-homological dimension of* $\mathcal{G}$*. As we shall see later, "dually" we can define the same for* $cd_p(\mathcal{G})$*, the p-cohomological dimension of* $\mathcal{G}$ *as the smallest r such that* $H^i(\mathcal{G}, M) = 0$ *for all integer* $i > r$ *and every discrete p-primary* $\Lambda(\mathcal{G})$*-module M.*

For a compact p-adic Lie group $\mathcal{G}$ having no nontrivial element of order p, it has finite p-(co)homological dimension, equaling to the dimension of $\mathcal{G}$ as a p-adic Lie group. See [18] and [25].

I shall prove the following two propositions together, they are both due to Howson [13].

Proposition 1.2.2. *Let M denote a finitely generated* $\Lambda(G)$*-module, where G is a p-adic Lie group having no element of order p. Then*

i *For each* $i \geq 0$*,* $H_i(G, M)$ *is a finitely generated* $\mathbb{Z}_p$*-module;*

ii $\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}\big(H_i(G, M)\big)$ *is finite.*

Proposition 1.2.3 (Howson)**.** *[13]*
Let M denote a finitely generated $\Lambda(H)$*-module, where H is a pro-p p-adic Lie group having no element of order p. Then*

$$rank_{\Lambda(H)}M = \sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}\big(H_i(H, M)\big). \tag{1.8}$$

Proof. For both the cases G and H, since they have no non-trivial p-torsion elements, they both have finite p-homological dimensions. and hence the alternating sums appeared in the proposition are just sums of finite terms. Hence, it reduces to show $H_i(G, M)$ and $H_i(H, M)$ are finitely generated $\mathbb{Z}_p$-modules for each $i \geq 0$. We prove the latter situation first. Since M is a finitely generated $\Lambda(H)$-module, it is a quotient module of a finitely generated free $\Lambda(H)$-module. Hence we have an exact sequence of $\Lambda(H)$-modules

$$0 \longrightarrow M' \longrightarrow \Lambda(H)^{n_0} \longrightarrow M \longrightarrow 0. \tag{1.9}$$

Since H is pro-p and have no elements of order p other than the trivial element, $\Lambda(H)$ is a Noetherian ring. M' being a submodule of a finitely generated module over a Noetherian ring, is finitely generated. Taking the H-homology of the short exact sequence above, we obtain a long exact sequence of $\mathbb{Z}_p$-modules

$$\cdots \longrightarrow H_{i+1}(H, \Lambda(H)^{n_0}) \longrightarrow H_{i+1}(H, M) \longrightarrow H_i(H, M') \longrightarrow H_i(H, \Lambda(H)^{n_0}) \longrightarrow \cdots \tag{1.10}$$

$$\cdots \longrightarrow H_1(H, \Lambda(H)^{n_0}) \longrightarrow H_1(H, M) \longrightarrow M'_H \longrightarrow \left(\Lambda(H)^{n_0}\right)_H \longrightarrow M_H \longrightarrow 0. \tag{1.11}$$

The right end of eq(1.11) shows that $H_0(H, M) = M_H$ is a finitely generated $\mathbb{Z}_p$-module since $\left(\Lambda(H)^{n_0}\right)_H \cong \mathbb{Z}_p^{n_0}$. Since M' is a finitely generated $\Lambda(H)$-module as well, the same argument deduces $H_0(H, M')$ is a finitely generated $\mathbb{Z}_p$-module. For $\Lambda(H)^{n_0}$ is a free $\Lambda(H)$-module, its higher homology groups are vanishing, that is

$$H_i(H, \Lambda(H)^{n_0}) = 0$$

for $i \geq 1$. Therefore the exact sequences eq(1.11) and eq(1.10) become

$$0 \longrightarrow H_{i+1}(H, M) \longrightarrow H_i(H, M') \longrightarrow 0, \quad for\ i \geq 1, \tag{1.12}$$

$$0 \longrightarrow H_1(H, M) \longrightarrow H_0(H, M') \longrightarrow \mathbb{Z}_p^{n_0} \longrightarrow H_0(H, M) \longrightarrow 0. \tag{1.13}$$

From the latter exact sequence, $H_1(H, M)$ must be a finitely generated $\mathbb{Z}_p$-module as so are the rest of the terms. The same arguments, when applied to M', deduce that $H_1(H, M')$ is a finitely generated $\mathbb{Z}_p$-module. The exact sequence eq(1.12) provides an inductive way to 'climb' up the homology degree by one to inductively show that $H_i(H, M)$ is finitely generated over $\mathbb{Z}_p$, via the parallel result for both M and M' in the preceding case.

Now for the case of G, there exists an open normal subgroup which is pro-p. Let us denote this pro-p subgroup by H. By the Hochschild-Serre spectral sequence, we have

$$H_p(G/H, H_q(H, M)) \Rightarrow H_{p+q}(G, M) \tag{1.14}$$

and hence $H_i(G, M)$ are finitely generated over $\mathbb{Z}_p$ by the fact that $H_i(H, M)$ are and the quotient group G/H is finite.

Since $\Lambda(H)$ is a local ring, a $\Lambda(H)$-module is projective if and only if it is free. On the other hand, $\Lambda(H)$ has finite global dimension, hence there exists a pro-

jective (and hence free) resolution of M of finite length

$$0 \longrightarrow \Lambda(H)^{n_l} \longrightarrow \cdots \longrightarrow \Lambda(H)^{n_1} \longrightarrow \Lambda(H)^{n_0} \longrightarrow M \longrightarrow 0. \tag{1.15}$$

Left-tensor this exact sequence by $\Lambda_{\mathbb{Q}}(H)$, the skew field of fractions of $\Lambda(H)$, which is a flat module, we get an exact sequence of finitely generated vector spaces over $\Lambda_{\mathbb{Q}}(H)$ and hence the alternating sum of their dimensions would be zero along this exact sequence. This yields

$$\begin{aligned} rank_{\Lambda(H)}M &= \sum_{i=0}^{l}(-1)^i dim_{\Lambda_{\mathbb{Q}}(H)}(\Lambda_{\mathbb{Q}}(H) \otimes_{\Lambda(H)} \Lambda(H)^{n_i}) \\ &= \sum_{i=0}^{l}(-1)^i n_i. \end{aligned} \tag{1.16}$$

On the other hand, the alternating sum of the values $\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}H_i(H,\star)$ is zero along any long exact sequence of finitely generated $\Lambda(H)$-modules. This yields

$$\begin{aligned} \sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}H_i(H,M) &= \sum_{k=0}^{l}(-1)^k \sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}H_i(H,\Lambda(H)^{n_k}) \\ &= \sum_{k=0}^{l}(-1)^k rank_{\mathbb{Z}_p}H_0(H,\Lambda(H)^{n_k}) \\ &= \sum_{k=0}^{l}(-1)^k n_k, \end{aligned} \tag{1.17}$$

by the fact that the higher homology groups of a free module vanish as pointed before. Hence the formula (1.8) is proved. □

1.3 Selmer Groups and Fundamental Diagram

In this section, we want to obtain a fundamental diagram involving the p^∞-Selmer groups $Sel_p(E/F_\infty)$ and $Sel_p(E/K_\infty)$ where F_∞ and K_∞ are as given in Section 1.1. Before this, I shall define the p^∞-Selmer groups of E over arbitrary algebraic extension of the defining field of E. I shall first define it over number fields.

Throughout this section, k always denotes a number field, that is, a field containing $\mathbb{Q}$, with degree $[k:\mathbb{Q}] < \infty$. Let $\overline{k}$ denote any fixed separable closure of k. We denote by k_v the completion of k at the place v.

Assume that E is an elliptic curve defined over the number field k.

Definition:. *For any abelian group A, and n a positive integer, we denote by A_n the subgroup consisting of all n-torsion elements, by A_{tors} the torsion subgroup of A, by $A(p)$ or A_{p^∞} the p-primary subgroup of A for any prime p. Furthermore, when A is a G-module for any topological group G, let $H^i(G,A)$ denote the i-th cohomological group, defined with continuous cochains. For any field F, we use the notation $H^i(F,A) \stackrel{def}{=} H^i(Gal(\overline{F}/F),A)$ for $\overline{F}$ a separable closure of F and A a Galois module.*

The multiplication by n map of the elliptic curve induces the exact sequence of $Gal(\overline{k}/k)$-modules:

$$0 \longrightarrow E_n \longrightarrow E(\overline{k}) \xrightarrow{[n]} E(\overline{k}) \longrightarrow 0$$

where E_n denotes the kernel of the multiplication by n map. Taking the $Gal(\overline{k}/k)$-cohomology of this short exact sequence yields a long exact sequence:

$$0 \longrightarrow E_n(k) \longrightarrow E(k) \xrightarrow{[n]} E(k) \longrightarrow H^1(k,E_n) \longrightarrow H^1(k,E) \xrightarrow{[n]} H^1(k,E)$$

which provides the short exact sequence:

$$0 \longrightarrow \frac{E(k)}{[n]E(k)} \longrightarrow H^1(k,E_n) \longrightarrow H^1(k,E)_n \longrightarrow 0$$

For any place v of k, we can view E as defined over the completion field k_v. Similarly, we can do exactly the same as before and obtain

$$0 \longrightarrow \frac{E(k_v)}{[n]E(k_v)} \longrightarrow H^1(k_v,E_n) \longrightarrow H^1(k_v,E)_n \longrightarrow 0$$

Taking the inductive limit over all $n \geq 1$, which is an exact functor, to these short exact sequences, we obtain the following commutative diagram with exact

rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(k)\otimes\mathbb{Q}/\mathbb{Z} & \xrightarrow{\kappa} & H^1(k,E_{tors}) & \xrightarrow{\lambda} & H^1(k,E) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E(k_v)\otimes\mathbb{Q}/\mathbb{Z} & \xrightarrow{\prod\kappa_v} & \prod_v H^1(k_v,E_{tors}) & \xrightarrow{\prod\lambda_v} & \prod_v H^1(k_v,E) & \longrightarrow & 0 \end{array} \tag{1.18}$$

where direct product runs over all places v of k. The left vertical map is just the canonical embedding into each component. The middle and right vertical maps are restriction maps into each v-component.

Definition:. *The Tate-Shafarevich group of E over k, $Ш(E/k)$ is defined to be the kernel of the right vertical map in diagram (1.18), which is*

$$Ш(E/k) = ker\Big(H^1(k,E) \longrightarrow \prod_v H^1(k_v,E)\Big), \tag{1.19}$$

of which v runs over all places of k in the product $\prod_v$ above.

It is conjectured that over number field k, the group $Ш(E/k)$ is finite.

Definition:. *The Selmer group of E over k, $Sel(E/k)$ is defined to be the preimage of $Ш(E/k)$ under the surjection λ. By the exactness of the second row of the commutative diagram (1.18), we can equivalently give its definition as:*

$$Sel(E/k) = ker\Big(H^1(k,E_{tors}) \longrightarrow \prod_v H^1(k_v,E)\Big). \tag{1.20}$$

where v runs over all places of k in the product $\prod_v$.

Definition:. *Let $Sel_p(E/k)$ denote the p-primary subgroup of the Selmer group for E over k, or briefly the p^∞-Selmer group for E over k. This is by definition, the p-primary subgroup of (1.20), which is*

$$Sel_p(E/k) = ker\Big(H^1(k,E_{p^\infty}) \to \prod_v H^1(k_v,E)_{p^\infty}\Big) \tag{1.21}$$

where v runs over all places of k. We endow these p-primary groups $Sel_p(E/k) \subseteq H^1(k, E_{p^\infty})$ with discrete topology and hence they are equipped with discrete $\mathbb{Z}_p$-module structures.

Combined with the commutative diagram (1.18), we obtain the following exact sequence:

$$0 \longrightarrow E(k) \otimes \mathbb{Q}/\mathbb{Z} \longrightarrow Sel(E/k) \longrightarrow Ш(E/k) \longrightarrow 0, \tag{1.22}$$

and its p-primary analogue:

$$0 \longrightarrow E(k) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow Sel_p(E/k) \longrightarrow Ш(E/k)(p) \longrightarrow 0. \tag{1.23}$$

Now I would want to extend these definitions from over a number field to over any general algebraic extension.

Let us fix the following notations:

Definition:. *Let L denote any algebraic extension of k, which could be of infinite degree over k, and w denote a place of L. We write L_w to be the union of the completion at w of all number fields contained in L.*

With this notion of L_w, all of the above leading to the commutative diagram eq(1.18) still holds for L and L_w in place of k and k_v respectively. Thus, we can define $Ш(E/L)$, $Sel(E/L)$ and $Sel_p(E/L)$ in the same fashion as above with k and k_v replaced by L and L_w respectively. We endow too to $Sel_p(E/L)$ a discrete $\mathbb{Z}_p$-module structure. Equivalently, $Ш(E/L)$, $Sel(E/L)$ and $Sel_p(E/L)$ are just the direct limits of $Ш(E/k')$, $Sel(E/k')$ and $Sel_p(E/k')$ respectively, where the limits are taken with respect to restriction maps, with k' running over all the subfields of L which are finite extensions over k. Thus, the exact sequences eq(1.22) and eq(1.23) hold also for k being replaced by L.

Let S be a finite set of non-Archimedean places of k containing

i all places of k above the chosen prime p,

ii all places of k at which E has bad reduction.

Denote k_S the maximal extension of k which is unramified outside $S \cup S_\infty$, where S_∞ is the set of all Archimedean places of k. Denote $G_S(L) \overset{\text{def}}{=} Gal(k_S/L)$ for any intermediate field L, $k \subset L \subset k_S$ and $S(L)$ the set of places of L above S.

Given any non-Archimedean place v of k, such that E attains good reduction $\tilde{E}$ modulo v, denote by $\overline{k_v}$ a separable closure of the field of completion k_v, by $\overline{\mathbf{k}_v}$ a separable closure of the residue field $\mathbf{k}_v$, by $\hat{E}$ the formal group associated to the elliptic curve E/k_v, by $\overline{\mathcal{M}}$ the maximal ideal of the ring of integers of $\overline{k_v}$. By classical theorem of elliptic curve, we have short exact sequence

$$0 \longrightarrow \hat{E}(\overline{\mathcal{M}}) \longrightarrow E(\overline{k_v}) \longrightarrow \tilde{E}(\overline{\mathbf{k}_v}) \longrightarrow 0.$$

The formal group $\hat{E}(\overline{\mathcal{M}})$ contains no non-trivial p-primary part for any prime p coprime to the characteristic of $\mathbf{k}_v$. Hence, as long as the good reduction prime v does not divide p, we have

$$E(\overline{k_v})_{p^\infty} \cong \tilde{E}(\overline{\mathbf{k}_v})_{p^\infty}$$

and thus v is unramified over $k(E_{p^\infty})$ and hence $k(E_{p^\infty}) \subset k_S$.

So. we get for any intermediate field L, $k \subset L \subset k_S$, the isomorphism

$$Sel_p(E/L) \cong Ker\Big(H^1(G_S(L), E_{p^\infty}) \to \bigoplus_{v \in S \cup S_\infty} J_v(L)\Big) \tag{1.24}$$

where $J_v(L) \overset{\text{def}}{=} \bigoplus_{w|v} H^1\left(L_w, E(\overline{L_w})\right)_{p^\infty}$ with w runs over all places (finitely many) of L above v, when $[L:k] < \infty$. When $[L:k] = \infty$, we define

$$J_v(L) \overset{\text{def}}{=} \varinjlim_{[L':k]<\infty} \bigoplus_{w'|v} H^1\left(L'_{w'}, E(\overline{L'_{w'}})\right)_{p^\infty},$$

with w' runs over all places (finitely many) of L' where the direct limit are taken over all subfields L' of L which is of finite degree over k. Since we are assuming p is an odd prime, $J_v(L)$ is trivial for any archimedean place v of k, hence we may omit S_∞ in the direct sum in the isomorphism above.

Hence, in our settings made in Section 1.1, taking $L = K_\infty$ and F_∞, we

obtain the following commutative diagram, with exact rows:-

$$\begin{array}{ccccccc} 0 & \longrightarrow & Sel_p(E/F_\infty)^{H_K} & \longrightarrow & H^1(G_S(F_\infty), E_{p^\infty})^{H_K} & \longrightarrow & \oplus_{v\in S} J_v(F_\infty)^{H_K} \\ & & \uparrow{\scriptstyle r_{K_\infty}} & & \uparrow{\scriptstyle res_{K_\infty}} & & \uparrow{\scriptstyle \oplus_{v\in S} h_v} \\ 0 & \longrightarrow & Sel_p(E/K_\infty) & \longrightarrow & H^1(G_S(K_\infty), E_{p^\infty}) & \longrightarrow & \oplus_{v\in S} J_v(K_\infty) \end{array} \tag{1.25}$$

where the right upward map is just the restriction map. In order that $F_\infty \subset K_S$ such that the notation $G_S(F_\infty)$ makes sense, we require S to contain all the places of K that ramify over F_∞. In particular, we can just let $S = S(K) = S_p \cup S_{bad} \cup S_{ram}$, where S_p denotes the singleton of unique prime of K above p, S_{bad} denotes the set of primes of K where E has bad reduction, and S_{ram} denotes the set of primes of K dividing m, where m is the positive integer which defines $F_\infty = \mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{m})$.

1.4 Pontryagin Duality and $\mathbb{Z}_p$-coranks

Definition:. *Let M and T be two topological spaces. For each compact subset $U \subset M$ and open subset $V \subset T$, construct a subset*

$$h(U,V) \overset{def}{=} \{h \in \mathcal{C}(M,T) \mid h(U) \subset V\}$$

where $\mathcal{C}(M,T)$ consists of all continuous map from M to T.

$$\{h(U,V) \mid U \subset M \text{ is compact}, V \subset T \text{ is open.}\}$$

forms a topological base for $\mathcal{C}(M,T)$ and we call this the compact-open topology.

Definition:. *Give the p-primary group $\mathbb{Q}_p/\mathbb{Z}_p$ the discrete topology and view it as a discrete Z_p-module. Hence, it is locally compact and Hausdorff. For any topological Z_p-module M, we denote the Z_p-module of all continuous Z_p-homomorphisms by*

$$\hat{M} \overset{def}{=} Hom_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p) \tag{1.26}$$

and call it the Pontryagin dual of M. We shall always endow $\hat{M}$ with the induced

compact-open topology. When M is a profinite, or equivalently compact and totally disconnected, (or discrete torsion respectively), $\mathbb{Z}_p$-module, $\hat{M}$ is discrete torsion (or profinite respectively) as a topological $\mathbb{Z}_p$-module.

Pontryagin duality is a reflexive contravariant functor between the category of discrete torsion $\mathbb{Z}_p$-modules and the category of profinite $\mathbb{Z}_p$-modules.

Definition:. *We say a discrete torsion Z_p-module, M, is cofinitely generated as a Z_p-module if its Pontryagin dual $\hat{M}$ is a finitely generated $\mathbb{Z}_p$-module. We can then define its Z_p-corank as the Z_p-rank of its Pontryagin dual and denote the value by $corank_{\mathbb{Z}_p} M$.*

Let L denote an arbitrary algebraic extension of the base field k, of which the elliptic curve E is defined over.

Definition:. *Let $Sel_p(E/L)$ be the p^∞-Selmer group of E over L, denote by*

$$X_p(E/L) \overset{def}{=} Hom_{\mathbb{Z}_p}\left(Sel_p(E/L), \mathbb{Q}_p/\mathbb{Z}_p\right) \tag{1.27}$$

its Pontryagin dual. It is a compact $\mathbb{Z}_p$-module. Moreover, when L/k is Galois, then the Galois group $Gal(L/k)$ acts continuously from the left on $H^1(L, E_{p^\infty})$, and hence $Sel_p(E/L)$ is equipped as a discrete left $\mathbb{Z}_p[Gal(L/k)]$-module. We shall endow its Pontryagin dual $X_p(E/L)$ a left $\mathbb{Z}_p[Gal(L/k)]$-module structure induce by the following definition:

$$(\sigma f)(s) = \sigma(f(\sigma^{-1}s))$$

for any $\sigma \in Gal(L/k)$, $f \in X_p(E/L)$ and $s \in Sel_p(E/L)$. In addition, when L/k is a p-adic Lie extension, then the same expression in (1.27) gives $X_p(E/L)$ a $\Lambda\big(Gal(L/k)\big)$-module structure, where $\Lambda\big(Gal(L/k)\big)$ is the Iwasawa algebra which is define in the same fashion as (1.3).

Proposition 1.4.1. *Assume that L is a finite extension of the base field k, then $H^1(G_S(L), E_{p^\infty})$ is a cofinitely generated Z_p-module. In particular, $Sel_p(E/L)$ is a cofinitely generated Z_p-module. Moreover, for any number fields extension*

$k \subseteq L \subseteq L'$, *we have*

$$corank_{\mathbb{Z}_p} Sel_p(E/L) \leq corank_{\mathbb{Z}_p} Sel_p(E/L'). \tag{1.28}$$

Proof. By Nakayama lemma, it is sufficient to check the finiteness of

$$H^1(\widehat{G_S(L)}, E_{p^\infty})/p\big(H^1(\widehat{G_S(L)}, E_{p^\infty})\big) = Coker\big(H^1(\widehat{G_S(L)}, E_{p^\infty}) \xrightarrow{p} H^1(\widehat{G_S(L)}, E_{p^\infty})\big).$$

This is the Pontryagin dual of

$$\big(H^1(G_S(L), E_{p^\infty})\big)_p = Ker\big(H^1(G_S(L), E_{p^\infty}) \xrightarrow{p} H^1(G_S(L), E_{p^\infty})\big).$$

Taking the $G_S(L)$-invariants from the short exact sequence

$$0 \longrightarrow E_p \longrightarrow E_{p^\infty} \xrightarrow{p} E_{p^\infty} \longrightarrow 0$$

yields a long exact sequence which contains

$$H^1(G_S(L), E_p) \longrightarrow H^1(G_S(L), E_{p^\infty}) \xrightarrow{p} H^1(G_S(L), E_{p^\infty}).$$

By its exactness, we get that $\big(H^1(G_S(L), E_{p^\infty})\big)_p$ is the homomorphic image of the finite group $H^1(G_S(L), E_p)$ and hence is finite.
For the second argument, it is sufficient to show that the kernel of the induced restriction map $Sel_p(E/L) \longrightarrow Sel_p(E/L')$ is finite. Indeed, this kernel injects into the kernel of the restriction map

$$H^1(G_S(L), E_{p^\infty}) \xrightarrow{r_{L'/L}} H^1(G_S(L'), E_{p^\infty}).$$

When L' is Galois over L, $ker(r_{L'/L}) = H^1(Gal(L'/L), E(L')_{p^\infty})$ is clearly finite. When L' is not Galois over L, take its Galois closure $L'' \in k_S$, then $ker(r_{L'/L}) \subset ker(r_{L''/L})$ where the latter is finite since L'' is Galois over L.

□

Looking at the short exact sequence (1.23)

$$0 \longrightarrow E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow Sel_p(E/L) \longrightarrow Ш(E/L)(p) \longrightarrow 0.$$

Hence, the $\mathbb{Z}_p$-corank of $Sel_p(E/L)$ is an upper bound of the Mordell-Weil rank of E over L. Since conjecturally $Ш(E/L)(p)$ is finite, the $\mathbb{Z}_p$-corank of $Sel_p(E/L)$ should actually reflect the Mordell-Weil rank over L.

However, when L is an infinite extension of k, $Sel_p(E/L)$ is not in general a cofinitely generated Z_p-module. For instance when $L = k^{cyc}$ is the p-cyclotomic extension of k, we shall later see in Lemma 2.1.2 that $Sel_p(E/k^{cyc})$ is a co-finitely generated $\Lambda(\Gamma_k)$-module. Even if its $\Lambda(\Gamma_k)$-corank vanishes, we can observe from (1.6) that the positivity of the μ-invariant of its Pontryagin dual would prevent $Sel_p(E/k^{cyc})$ from being a cofinitely generated $\mathbb{Z}_p$-module.

Chapter 2

The Category $\mathfrak{M}_H(G)$

2.1 Mazur Conjecture

Within this section, k always denotes an arbitrary number field, i.e a finite extension of $\mathbb{Q}$.

In this section, I will mainly state some results and conjectures regarding the $\Lambda(\Gamma_k)$-rank of the compact profinite group $X_p(E/k^{cyc})$, where p is a rational prime and E is an elliptic curve defined over number field k.

Lemma 2.1.1. *Nakayama [1, p.2,Theorem]*
Let Λ be a compact topological ring with 1 and let I be a (left) ideal with $I^n \to 0$ in Λ. For M any compact profinite (left) Λ-module, $IM = M$ implies $M = 0$.

As a consequence of Nakayama lemma, if M/IM is a finitely generated $\mathbb{Z}_p$-module, then M is a finitely generated Λ-module.

Lemma 2.1.2. *[19, Theorem 4.5 (a)]*
For any prime p, $X_p(E/k^{cyc})$ is a finitely generated $\Lambda(\Gamma_k)$-module.

We shall see later that the nullity of the $\Lambda(\Gamma_k)$-rank of $X_p(E/k^{cyc})$ depends crucially on the reduction type of the primes of k above the prime p.

Theorem 2.1.1. *Mazur Control Theorem [20, c.f Proposition 6.4]*
For a fixed odd prime p, and a number field k, denote by $\Gamma_n \overset{def}{=} \Gamma_k^{p^n}$ the open

subgroup of $\Gamma_k = Gal(k^{cyc}/k)$ *of index* p^n*, for each integer* $n \geq 0$*, and let* k_n *denote the subfield of* k^{cyc}*, fixed by* Γ_n*. Suppose* E *is an elliptic curve defined over* k*, with good ordinary reduction at all primes of* k *lying above* p*, then the restriction map*

$$Sel_p(E/k_n) \xrightarrow{\bar{r}_{k_n}} Sel_p(E/k^{cyc})^{\Gamma_n} \tag{2.1}$$

has finite kernel and cokernel, for $n \geq 0$ *and moreover, the kernels and cokernels are of bounded order when* n *varies.*

Mazur conjectured the following statement [20]

Conjecture 2.1.1. *(Mazur)*
If p *is a prime such that* E/k *has potentially good ordinary reduction or potentially multiplicative reduction at all primes of* k *above* p*, then* $Sel_p(E/k^{cyc})$ *is* $\Lambda(\Gamma_k)$*-cotorsion.*

The same argument fails for any potentially good supersingular reduction places above p, due at prior to Konovalov [15] and later to Schneider.

Theorem 2.1.2. *[24, Corollary 5]*

$$corank_{\Lambda(\Gamma_k)} Sel_p(E/k^{cyc}) \geq r(E,k)$$

where

$$r(E,k) \stackrel{def}{=} \sum_{pss} [k_v : \mathbb{Q}_p]$$

which the sum $\sum_{pss}$ *runs over each place* v *of* k *above* p *at where* E *has potentially supersingular reduction.*

Schneider conjectured that

Conjecture 2.1.2. *The equality always holds in the theorem above.*

Under our assumption on (E, p, m) in Section 1.1, we expect the validity of another stronger conjecture, namely Conjecture 2.2.1 introduced in the following section, which will implies the validity of Mazur's Conjecture for every

intermediate number field $\mathbb{Q} \subseteq k \subset F_\infty$.

2.2 The category $\mathfrak{M}_H(G)$

Assume from now on that we are working over the False Tate curve extension introduced in Section 1.1 and recall the notations $G \stackrel{\text{def}}{=} Gal(F_\infty/\mathbb{Q})$, $H \stackrel{\text{def}}{=} Gal(F_\infty/\mathbb{Q}^{cyc})$. We recall that we are assuming in particular that E has multiplicative reduction at p. For any $\Lambda(G)$-module M, $M(p)$ denotes its submodule consisting of all elements of p-power order.

Definition:. *Let $\mathfrak{M}_H(G)$ denote the category of all finitely generated $\Lambda(G)$-modules M, such that $M/M(p)$ is finitely generated over $\Lambda(H)$.*

Throughout this paper, I will assume the validity of the following conjecture made in [4]. .

Conjecture 2.2.1. *Under the assumption made on (E, p, m) in Section 1.1, $X_p(E/F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$.*

We first derive some direct consequences from this conjecture. Write L an arbitrary number field contained in F_∞, and denote

$$H_L \stackrel{\text{def}}{=} Gal(F_\infty/L^{cyc}),$$

$$\Gamma_L \stackrel{\text{def}}{=} Gal(L^{cyc}/L),$$

$$Y_p(E/F_\infty) \stackrel{\text{def}}{=} X_p(E/F_\infty)/X_p(E/F_\infty)(p),$$

$$Y_p(E/L^{cyc}) \stackrel{\text{def}}{=} X_p(E/L^{cyc})/X_p(E/L^{cyc})(p).$$

Now, $X_p(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$ means that $Y_p(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module. Since $[H : H_L]$ is finite, $\Lambda(H)$ is a finitely generated $\Lambda(H_L)$-module. Hence $Y_p(E/F_\infty)$ is also a finitely generated $\Lambda(H_L)$-module. Therefore

$$Y_p(E/F_\infty)_{H_L} \text{ is finitely generated over } \mathbb{Z}_p$$

Observing from the following commutative diagram with exact rows,

$$\begin{array}{ccccc} X_p(E/F_\infty)_{H_L} & \longrightarrow & Y_p(E/F_\infty)_{H_L} & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \\ X_p(E/L^{cyc}) & \longrightarrow & Y_p(E/L^{cyc}) & \longrightarrow & 0 \end{array} \tag{2.2}$$

the cokernel of the first vertical map is Pontryagin dual to the kernel of the restriction map

$$r_{L^{cyc}} : Sel_p(E/L^{cyc}) \longrightarrow Sel_p(E/F_\infty)^{H_L}$$

which is a subgroup of

$$ker(r_{L^{cyc}}) \subseteq H^1\left(H_L, E_{p^\infty}(F_\infty)\right) \cong E_{p^\infty}(F_\infty)_{H_L}$$

where the isomorphism is due to the Poincare duality, whenever H_L is pro-p, i.e. when $\mu_p \subset L$. Finally, we see its finiteness since $E_{p^\infty}(F_\infty)$ is cofinitely generated over $\mathbb{Z}_p$ and $E_{p^\infty}(F_\infty)^{H_L} = E_{p^\infty}(L^{cyc})$ is finite by Ribet's Theorem [22, Theorem 1.1]. Hence, for any intermediate field L containing μ_p, both the vertical maps in the commutative diagram (2.2) above have finite cokernels, and

Consequence 1: $Y_p(E/L^{cyc})$ is finitely generated over $\mathbb{Z}_p$.

Consequence 2: $X_p(E/L^{cyc})$ is $\Lambda(\Gamma_L)$-torsion.

In fact, these two consequences hold for any intermediate number field $L \subset F_\infty$. Indeed, they hold for $L' \overset{\text{def}}{=} L(\mu_p)$. Write $\Delta_L \overset{\text{def}}{=} Gal(L'^{cyc}/L^{cyc})$ which is a finite group of order coprime to p. Therefore the restriction map induces an isomorphism

$$Sel_p(E/L^{cyc}) \cong Sel_p(E/L'^{cyc})^{\Delta_L}$$

$Y_p(E/L'^{cyc})$ is finitely generated over $\mathbb{Z}_p$ and so is $Y_p(E/L'^{cyc})_{\Delta_L}$ and hence $Y_p(E/L^{cyc})$. Similarly, $X_p(E/L'^{cyc})$ is $\Lambda(\Gamma_{L'})$-torsion, and so is $X_p(E/L'^{cyc})_{\Delta_L} \cong X_p(E/L^{cyc})$ with the same group action by Γ_L and $\Gamma_{L'}$, so we obtain Consequence 2 for L.

The validity of Conjecture 2.2.1 is essential to define the $\Lambda(H_K)$-rank of $Y_p(E/F_\infty)$, which will play a large part in the rest of this thesis.

2.3 Computation of the $\mathbb{Z}_p$-coranks of some modules

In the rest of this chapter, we suppose the triple (E, p, m) satisfies the assumption made in Section 1.1 and shall always assume the validity of Conjecture 2.2.1. Let L denote any subfield of F_∞ with $[L : \mathbb{Q}] < \infty$. From the consequences in section 2.2, we deduce that $X_p(E/L^{cyc})$ is $\Lambda(\Gamma_L)$-torsion and its λ-invariant is

$$\lambda_{\Lambda(\Gamma_L)}(X_p(E/L^{cyc})) \stackrel{\text{def}}{=} dim_{\mathbb{Q}_p}(X_p(E/L^{cyc}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p).$$

In the rest of this chapter, for simplicity, we shall assume further that the subfield L contains $K \stackrel{\text{def}}{=} \mathbb{Q}(\mu_p)$ as this implies that $H_L \cong \mathbb{Z}_p$. For instance when $L = K$ and $L = F_n$ for $n \geq 1$. The other cases for instance when $L = L_n$ for $n \geq 0$ will be treated separately in Section 4.3 and we shall see then the results are very identical.

For simplicity, we shall assume that $S = S(K) = S_{ram} \cup S_{bad} \cup S_p$ as given at the end of Section 1.3. Now, I would want to rewrite the fundamental diagram (1.25) by replacing S by $S(L^{cyc})$ in the direct sum. Recall that there are only finitely many primes of K^{cyc} above each rational prime and $[L : K] < \infty$, $S(L^{cyc})$ is again a finite set.

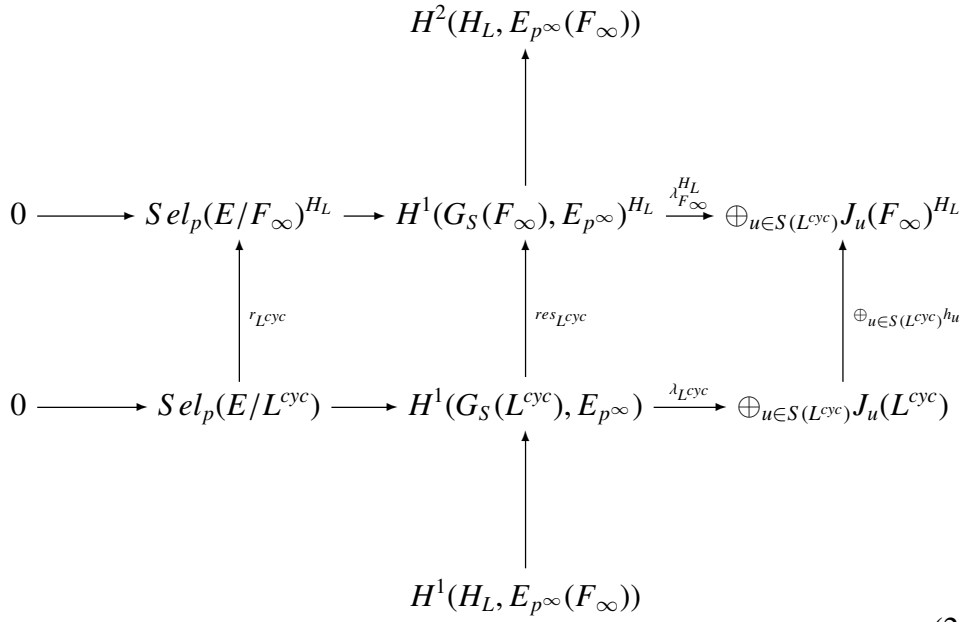
Let us denote for any place u of L^{cyc},

$$J_u(F_\infty) \stackrel{\text{def}}{=} \varinjlim_{\substack{[L':L^{cyc}]<\infty \\ L' \subset F_\infty}} \bigoplus_{w'|u} H^1\left(L'_{w'}, E(\overline{L'_{w'}})\right)_{p^\infty},$$

where the limit is taken via restriction map, and

$$J_u(L^{cyc}) \stackrel{\text{def}}{=} H^1\left(L^{cyc}_u, E(\overline{L^{cyc}_u})\right)_{p^\infty},$$

we have



(2.3)

where the vertical upward sequence is the inflation-restriction exact sequence. This doesn't make any difference since $J_v(L^{cyc}) = \oplus_{u|v} J_u(L^{cyc})$, $J_v(F_\infty) = \oplus_{u|v} J_u(F_\infty)$, and $h_v = \oplus_{u|v} h_u$, where u always denotes a place of L^{cyc} and v denotes a place of K

We shall be interested at the difference between the "$\mathbb{Z}_p$-coranks" of the two terms on the left and for this, we need to apply snake lemma. We may check the surjectivity of $\lambda_{L^{cyc}}$ by the theorem below, which does not depend on the settings and assumptions made at the beginning of this section.

Theorem 2.3.1. *(Hachimori and Venjakob) [12, Theorem 7.2]*
For E an elliptic curve defined over number field k and any odd prime p, assume $G = Gal(F/k)$ is a pro-p, p-adic Lie group with no p-torsion and $E(F)_{p^\infty}$ is finite. If $X_p(E/F)$ is $\Lambda(G)$-torsion, then we have

1. $H^2(G_S(F), E_{p^\infty}) = 0$
2. $H^1(G_S(F), E_{p^\infty}) \xrightarrow{\lambda_F} \oplus_{v\in S} J_v(F)$ *is surjective*

here S is a set of primes of k containing all the primes above p, all places at where E has bad reduction and primes which are ramified in F/k.

Proof. By Poitou-Tate global duality, we have the exact sequence

$$0 \longrightarrow Sel_p(E/F) \longrightarrow H^1(G_S(F), E_{p^\infty}) \xrightarrow{\lambda_F} \bigoplus_{v\in S} J_v(F) \longrightarrow \widehat{R_p(E/F)} \longrightarrow H^2(G_S(F), E_{p^\infty}) \longrightarrow 0 \quad (2.4)$$

where $\widehat{*}$ denotes the Pontryagin dual of $*$, and

$$R_p(E/F) \stackrel{\text{def}}{=} \varprojlim_{n,M} Sel(E_{p^n}/M)$$

where the inverse limit is taken with respect to corestriction maps (c.f for instance [21, page 232] for the definition), and the maps induced by "multiplication by p" maps $E_{p^{n+1}} \longrightarrow E_{p^n}$.
Here,

$$Sel(E_{p^n}/M) \stackrel{\text{def}}{=} ker\left(H^1(G_S(M), E_{p^n}) \longrightarrow \bigoplus_{v\in S} J_v(M)\right).$$

Since $G \stackrel{\text{def}}{=} Gal(F/k)$ is a pro-p infinite group and $E(F)_{p^\infty}$ is finite, we have

$$\varprojlim_{M} E(M)_{p^\infty} = 0$$

with M runs over the finite extensions of k, contained in F. Therefore,

$$0 \longrightarrow R_p(E/F) \longrightarrow \varprojlim_{M} Hom_{\mathbb{Z}_p}(\widehat{Sel_p(E/M)}, \mathbb{Z}_p)$$

follows from taking inverse limit with respect to corestriction maps from the short exact sequence

$$0 \longrightarrow E(M)_{p^\infty} \longrightarrow \varprojlim_{n} Sel(E_{p^n}/M) \longrightarrow Hom_{\mathbb{Z}_p}(\widehat{Sel_p(E/M)}, \mathbb{Z}_p) \longrightarrow 0$$

Further, we see that from the restriction map

$$res_M : Sel_p(E/M) \longrightarrow Sel_p(E/F)^{Gal(F/M)}$$

we have exact sequence

$$0 \to \varprojlim_{M} Hom_{\mathbb{Z}_p}(\widehat{(ker(res_M))}, \mathbb{Z}_p)$$
$$\to \varprojlim_{M} Hom_{\mathbb{Z}_p}(\widehat{(Sel_p(E/M))}, \mathbb{Z}_p)$$
$$\to \varprojlim_{M} Hom_{\mathbb{Z}_p}(\widehat{(Sel_p(E/F))}_{Gal(F/M)}, \mathbb{Z}_p) \quad (2.5)$$

and $E(F)_{p^\infty}$ is finite again implies $ker(res_M) \subset H^1(Gal(F/M), E(F)_{p^\infty})$ is finite and hence the vanishing of the first term of this exact sequence (2.5), and thus

$$R_p(E/F) \text{ is a submodule of } \varprojlim_{M} Hom_{\mathbb{Z}_p}(\widehat{(Sel_p(E/F))}_{Gal(F/M)}, \mathbb{Z}_p)$$

of which the latter is isomorphic to

$$\varprojlim_{M} Hom_{\Lambda(G)}(\widehat{Sel_p(E/F)}, \mathbb{Z}_p[G/Gal(F/M)]) \cong Hom_{\Lambda(G)}(\widehat{Sel_p(E/F)}, \Lambda(G))$$

via

$$f \mapsto \left(x \in \widehat{Sel_p(E/F)} \mapsto \sum_{\sigma \in G/Gal(F/M)} f(\sigma^{-1}x)\sigma \in \mathbb{Z}_p[G/Gal(F/M)] \right)$$

and this last term $Hom_{\Lambda(G)}(\widehat{Sel_p(E/F)}, \Lambda(G)) = 0$, and hence $R_p(E/F) = 0$, when $X_p(E/F)$ is $\Lambda(G)$-torsion. Hence two statements of this theorem follow from the exact sequence (2.4).

□

There are two other facts which hold regardless of the settings and validity of Conjecture 2.2.1, and will be very useful for further computations.

Theorem 2.3.2. *(Ribet)*
For A an abelian variety defined over a number field k. Let k^∞ be the compositum of $k(\mu_{p^\infty})$ for all rational primes p. The torsion subgroup of $A(k^\infty)$ is finite.

Proof. See [22, Theorem 1.1].

□

Lemma 2.3.1. *(Hachimori-Matsuno)*
Let $K_\mathfrak{q}$ be a finite extension of $\mathbb{Q}_q$, containing μ_p, with $p \neq q$ are distinct primes, p is odd. For any elliptic curve E defined over $K_\mathfrak{q}$, we have

1. *If E has good reduction over $K_\mathfrak{q}^{cyc} \overset{def}{=} K_\mathfrak{q}(\mu_{p^\infty})$, then*

$$E(K_\mathfrak{q}^{cyc})_{p^\infty} \cong \begin{cases} E_{p^\infty} & \text{if } E(K_\mathfrak{q})_{p^\infty} \neq 0, \\ 0 & \text{if } E(K_\mathfrak{q})_{p^\infty} = 0. \end{cases}$$

2. *If E has split multiplicative reduction over $K_\mathfrak{q}^{cyc}$, then E has split multiplicative reduction over $K_\mathfrak{q}$ and*

$$E(K_\mathfrak{q}^{cyc}) \cong K_\mathfrak{q}^{cyc*}/g^{\mathbb{Z}}$$

as $Gal(K_\mathfrak{q}^{cyc}/K_\mathfrak{q})$-modules for some $g \in K_\mathfrak{q}$, and

$$E(K_\mathfrak{q}^{cyc})_{p^\infty} \cong < \mu_{p^\infty}, g^{1/p^n} > /g^{\mathbb{Z}}$$

as $Gal(K_\mathfrak{q}^{cyc}/K_\mathfrak{q})$-submodules, for some integer $n \geq 0$ such that $g^{1/p^n} \in K_\mathfrak{q}^{cyc}$ but $g^{1/p^{n+1}} \notin K_\mathfrak{q}^{cyc}$.

3. *If E has non-split multiplicative reduction over $K_\mathfrak{q}^{cyc}$, then*

$$E(K_\mathfrak{q}^{cyc})_{p^\infty} = 0.$$

Proof. See [11, Proposition 5.1]

□

Let us resume the settings and assumptions from the beginning of this section from now on.

Corollary 2.3.1. *Assuming Conjecture 2.2.1, we have*

1. *$H^2(G_S(L^{cyc}), E_{p^\infty}) = 0$*
2. *$H^1(G_S(L^{cyc}), E_{p^\infty}) \xrightarrow{\lambda_{L^{cyc}}} \oplus_{u \in S(L^{cyc})} J_u(L^{cyc})$ is surjective*

Proof. This is merely a check of the validity of the criterions of the theorem of Hachimori and Venjakob in the settings as given in section 1.1. The elliptic

curve E is defined over $\mathbb{Q}$ and hence over L. Also, $\Gamma_L \overset{\text{def}}{=} Gal(L^{cyc}/L) \cong \mathbb{Z}_p$ is a pro-p, p-adic Lie group without p-torsion and $E(L^{cyc})_{p^\infty}$ is finite by Ribet's theorem. Lastly, $X_p(E/L^{cyc})$ is $\Lambda(\Gamma_L)$-torsion by the validity of Conjecture 2.2.1.

□

Corollary 2.3.2. *Assuming Conjecture 2.2.1, the co-finitely generated $\Lambda(\Gamma_L)$-module $Sel_p(E/F_\infty)^{H_L}$ is cotorsion over $\Lambda(\Gamma_L)$ and*

$$\lambda_{\Lambda(\Gamma_L)}\big(X_p(E/F_\infty)_{H_L}\big) = \lambda_{\Lambda(\Gamma_L)}\big(X_p(E/L^{cyc})\big) + \sum_{u\in S(L^{cyc})} corank_{\mathbb{Z}_p} ker(h_u). \quad (2.6)$$

Proof. By snake lemma, we have an exact sequence

$$0 \to ker(r_{L^{cyc}}) \to H^1(H_L, E_{p^\infty}(F_\infty)) \to \oplus_{u\in S(L^{cyc})} ker(h_u) \to coker(r_{L^{cyc}}) \to H^2(H_L, E_{p^\infty}(F_\infty)) = 0.$$

The nullity on the right is due to $H_L \cong \mathbb{Z}_p$ having p-cohomological dimension 1. Since $E_{p^\infty}(F_\infty)$ is co-finitely generated over $\mathbb{Z}_p$, by Poincare duality, $H^1(H_L, E_{p^\infty}(F_\infty)) \cong (E_{p^\infty}(F_\infty))_{H_L}$ has vanishing $\mathbb{Z}_p$-corank since $(E_{p^\infty}(F_\infty))^{H_L} = E_{p^\infty}(L^{cyc})$ is finite again by Ribet's theorem. Hence we proved this corollary by assuming the next proposition and the deeply ramified theorem later, which show each $ker(h_u)$ has finite $\mathbb{Z}_p$-corank.

□

Let S_{good}, S_{ns}, S_s denote the set of good, non-split multiplicative, split multiplicative reduction primes of E over K respectively. The notation $S_*(L^{cyc})$ means the set of places of L^{cyc} above S_*, for $* = p$, bad, $good$, s, ns, and ram. It is clear to see that $S_*(L^{cyc})$ is the set of $*$-reduction primes of E over L^{cyc} for $* =$ bad, $good$, s or ns, because $Gal(L^{cyc}/K)$ is a pro-p group and $p \geq 5$, hence the reduction type doesn't change within this pro-p extension L^{cyc}/K.

Proposition 2.3.1. *For $u \in S(L^{cyc}) - S_p(L^{cyc})$,*

1. *If $u \notin S_{ram}(L^{cyc})$, then*

$$ker(h_u) = 0.$$

2. *If* $u \in S_{ram}(L^{cyc}) \cap S_{ns}(L^{cyc})$, *then*

$$ker(h_u) = 0.$$

3. *If* $u \in S_{ram}(L^{cyc}) \cap S_{s}(L^{cyc})$, *then*

$$ker(h_u) \cong \mathbb{Q}_p/\mathbb{Z}_p \oplus A_u,$$

where A_u *is some abelian group of finite order.*

4. *If* $u \in S_{ram}(L^{cyc}) \cap S_{good}(L^{cyc})$, *then*

   (a) *if* $E(L_u^{cyc})_{p^\infty} = 0$, *then*

   $$ker(h_u) = 0,$$

   (b) *if* $E(L_u^{cyc})_{p^\infty} \neq 0$, *then*

   $$ker(h_u) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2.$$

Proof. Let $H_{L,u}$ be the decomposition subgroup of H_L at w, a place of F_∞ above u. For $u \in S(L^{cyc})$,

$$J_u(L^{cyc}) \xrightarrow{h_u} J_u(F_\infty)^{H_L}$$

has kernel

$$ker(h_u) = H^1(H_{L,u}, E(F_{\infty,w}))_{p^\infty}.$$

When $u \notin S_p(L^{cyc})$, by Lutz's Theorem $E(L_u^{cyc}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p = 0$, hence

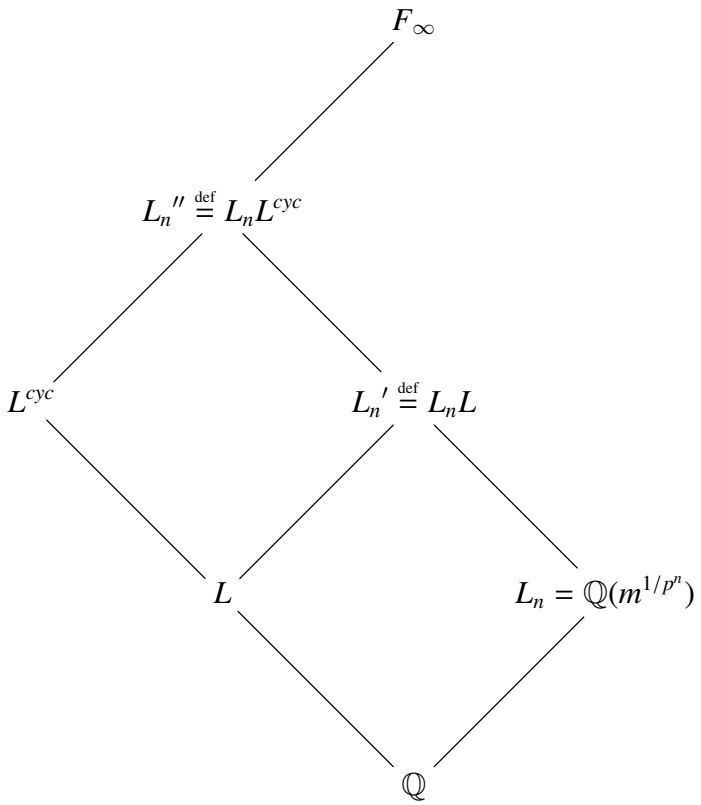
$$ker(h_u) \cong H^1(H_{L,u}, E(F_{\infty,w})_{p^\infty})$$

by Kummer Theory.

- When $u \in S(L^{cyc}) - S_{ram}(L^{cyc}) - S_p(L^{cyc})$,
  u is unramified over F_∞/L^{cyc}
  $\Rightarrow u$ splits completely over F_∞/L^{cyc}
  $\Rightarrow H_{L,u} = 0$

$\Rightarrow ker(h_u) = 0$

- When $u \in S_{ram}(L^{cyc}) - S_p(L^{cyc})$,
  then w is the unique prime of F_∞ above u. Look at the tower of fields below:-



Write q_i the rational prime lying below w, this is a prime divisor of m which is distinct from p. For each $n \geq 0$, write u'', u' and u_L the prime of L_n'', L_n' and L respectively, which lies below w. Since the triple (E, p, m) satisfies the assumption made in Section 1.1, according to the final statement in the assumption, E does not have additive reduction at u, u_n'', u_n' and u_L.

In order to understand $E(F_{\infty,w})_{p^\infty}$, we apply the theorem of Hachimori-Matsuno, quoted as Lemma 2.3.1 above, with $K_{\mathfrak{q}} = L'_{n,u'_n}$ for all $n \geq 0$. Noticing that since $\mu_p \subset L$ by assumption, we have $\mu_p \subset L'_{n,u'_n}$ and $L''_{n,u''_n} = L'_{n,u'_n}(\mu_{p^\infty})$

– When E has non-split multiplicative reduction at u, then
E has non-split multiplicative reduction at u''_n and u'_n since L''_n/L^{cyc} and L''_n/L'_n are pro-p extension and p is odd for all $n \geq 0$. By part(3) of Lemma 2.3.1, we see

$$E(L''_{n,u''_n})_{p^\infty} = 0$$

for all $n \geq 0$, and hence

$$E(F_{\infty,w})_{p^\infty} = 0$$

and finally

$$ker(h_u) = 0.$$

– When E has good reduction at u, then
E has good reduction at q_i by semistability and the assumption that E has no additive reduction at q_i. Furthermore,

  * if $E(L_u^{cyc})_{p^\infty} = 0$, then

$$E(L_{u_L})_{p^\infty} = 0.$$

Since u_L is totally ramified in L'_n for all $n \geq 0$, L'_{n,u'_n} and L_{u_L} have the same residue field, denoted by l. Since l has finite characteristic coprime to p, write $\tilde{E}$ the reduction of E modulo u_L, we have

$$E(L_{u_L})_{p^\infty} \cong \tilde{E}(l)_{p^\infty} \cong E(L'_{n,u'_n})_{p^\infty}$$

and hence for all $n \geq 0$,

$$E(L'_{n,u'_n})_{p^\infty} = 0$$

and by part(1) of Lemma 2.3.1,

$$E(L''_{n,u''_n})_{p^\infty} = 0.$$

Therefore, we have again

$$E(F_{\infty,w})_{p^\infty} = 0$$

and

$$ker(h_u) = 0.$$

∗ if $E(L_u^{cyc})_{p^\infty} \neq 0$, then
by part(1) of Lemma 2.3.1, we have

$$E(F_{\infty,w})_{p^\infty} = E(L''_{n,u''_n})_{p^\infty} = E(L_u^{cyc})_{p^\infty} = E_{p^\infty} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2$$

as $H_{L,u} = Gal(F_{\infty,w}/L_u^{cyc})$-modules with trivial action. Therefore,

$$ker(h_u) \cong H^1(H_{L,u}, E(F_{\infty,w})_{p^\infty}) = Hom(H_{L,u}, E(F_{\infty,w})_{p^\infty}) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2.$$

– When E has split multiplicative reduction at u, then
for all $n \geq 0$, E has split multiplicative reduction at u''_n. By

$$E(L''_{n,u''_n})_{p^\infty} \cong \mathbb{Q}_p/\mathbb{Z}_p \oplus \text{finite group}$$

and since by Poincare duality,

$$H^1(H_{L,u}, E(F_{\infty,w})_{p^\infty}) \cong (E(F_{\infty,w})_{p^\infty})_{H_{L,u}}$$

the statement follows since

$$(E(F_{\infty,w})_{p^\infty})^{H_{L,u}} = E(L_u^{cyc})_{p^\infty} \cong \mathbb{Q}_p/\mathbb{Z}_p \oplus \text{finite group}$$

by part(2) of Lemma 2.3.1 again.

□

2.4 Deeply Ramified Theorem

In this section, we continue assuming the same settings as the previous section. We have given the description of $ker(h_u)$ for all $u \in S(L^{cyc}) - S_p(L^{cyc})$. The main purpose of this section is to complete the description of $ker(h_u)$ when $u \in S_p(L^{cyc})$. Let us denote by $\mathfrak{p}$ a place of L^{cyc} above p, by $\tilde{p}$ a place of F_∞ above $\mathfrak{p}$ and denote by $H_{L,\mathfrak{p}}$ the corresponding decomposition group.

Theorem 2.4.1. *For any $\mathfrak{p} \in S_p(L^{cyc})$, we have*

$$corank_{\mathbb{Z}_p} ker(h_\mathfrak{p}) = \begin{cases} 1 & \text{if } E \text{ has split multiplicative reduction at } p, \\ 0 & \text{if } E \text{ has non-split multiplicative reduction at } p. \end{cases} \tag{2.7}$$

This result is just a simple consequence of Coates-Greenberg [5, Proposition 4.3] and Greenberg [9, Section 3]. We recall the proof.

Let $h_\mathfrak{p}$ be the map

$$J_\mathfrak{p}(L^{cyc}) = H^1(L^{cyc}_\mathfrak{p}, E)_{p^\infty} \xrightarrow{h_\mathfrak{p}} H^1(F_{\infty,\tilde{p}}, E)^{H_L}_{p^\infty} = J_\mathfrak{p}(F_\infty)^{H_L}. \tag{2.8}$$

Using the local Kummer exact sequence,

$$0 \longrightarrow E(\mathcal{F}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\kappa_\mathcal{F}} H^1(\mathcal{F}, E_{p^\infty}) \longrightarrow H^1(\mathcal{F}, E)_{p^\infty} \longrightarrow 0$$

for any local field $\mathcal{F}$, we can rewrite the map $h_\mathfrak{p}$ in (2.8) as

$$H^1(L^{cyc}_\mathfrak{p}, E_{p^\infty})/Im(\kappa_{L^{cyc}_\mathfrak{p}}) \xrightarrow{h_\mathfrak{p}} \left(H^1(F_{\infty,\tilde{p}}, E_{p^\infty})/Im(\kappa_{F_{\infty,\tilde{p}}})\right)^{H_L} \tag{2.9}$$

Throughout this section, we shall be dealing with the case where $\mathcal{F}$ is an algebraic extension of $\mathbb{Q}_p$, for the particular fixed odd prime p.

We shall use a very important theorem by Coates-Greenberg about deeply ramified extensions to eventually show the main theorem of this section.

For an elliptic curve E of semistable reduction over local field $\mathcal{F}$, and let $\widehat{E}$

be the formal group over $\mathcal{O}_{\mathcal{F}}$ attached to the minimal model of E over $\mathcal{F}$. We have an $G_{\mathcal{F}}$-invariant submodule

$$\mathcal{C} \stackrel{\text{def}}{=} \widehat{E}(\overline{\mathcal{M}_{\mathcal{F}}})_{p^\infty} \subseteq E_{p^\infty}$$

where $\overline{\mathcal{M}_{\mathcal{F}}}$ denotes the maximal ideal of the ring of integers of a separable closure of the local field $\mathcal{F}$. Hence, we obtain a short exact sequence of $G_{\mathcal{F}}$-modules

$$0 \longrightarrow \mathcal{C} \longrightarrow E_{p^\infty} \longrightarrow \mathcal{D} \longrightarrow 0$$

where $\mathcal{D}$ denotes $E_{p^\infty}/\mathcal{C}$. This deduces a long exact sequence

$$\cdots \longrightarrow H^1(\mathcal{F}, \mathcal{C}) \xrightarrow{\lambda_{\mathcal{F}}} H^1(\mathcal{F}, E_{p^\infty}) \xrightarrow{\pi_{\mathcal{F}}} H^1(\mathcal{F}, \mathcal{D}) \longrightarrow \cdots \tag{2.10}$$

Theorem 2.4.2. *(Coates-Greenberg)*
Assume that E is defined over local field F, a finite extension of $\mathbb{Q}_p$. Then for any deeply ramified extension $\mathcal{F}/F$, we have

$$Im(\kappa_{\mathcal{F}}) = Im(\lambda_{\mathcal{F}}).$$

Proof. See [5, Proposition 4.3].

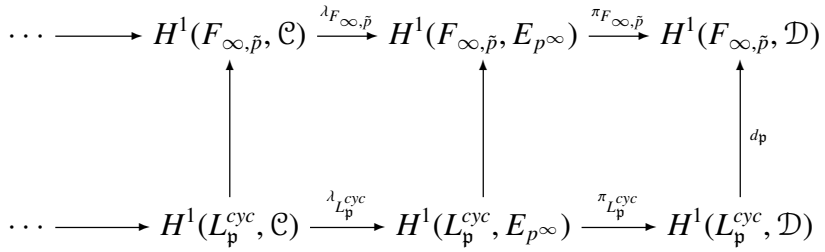
□

Proof of Theorem 2.4.1. Since $\mathcal{F} = F_\infty$, L^{cyc} are deeply ramified extensions over $\mathbb{Q}_p$, by the theorem of Coates-Greenberg, we have

$$Im(\pi_{L^{cyc}_{\mathfrak{p}}}) \xrightarrow{h_{\mathfrak{p}}} Im(\pi_{F_{\infty,\tilde{p}}})^{H_L}$$

which is actually the restricted map of $d_{\mathfrak{p}}$ which lives in the commutative dia-

gram below:-



Hence, we have identified the following

$$\begin{aligned} ker(h_{\mathfrak{p}}) &\cong Im(\pi_{L_{\mathfrak{p}}^{cyc}}) \cap ker(d_{\mathfrak{p}}) \\ &= ker(d_{\mathfrak{p}}) \end{aligned} \tag{2.11}$$

as $\pi_{L_{\mathfrak{p}}^{cyc}}$ is surjective since $G_{L_{\mathfrak{p}}^{cyc}}$ has p-cohomological dimension 1.
From the knowledge about Tate curves,

- when E has split multiplicative reduction at p, we have

  $$\mathcal{C} \cong \mu_{p^\infty}$$

  as $G_{\mathbb{Q}_p}$-modules and

  $$\mathcal{D} \cong \mathbb{Q}_p/\mathbb{Z}_p$$

  as $G_{\mathbb{Q}_p}$-modules with trivial action. So

  $$ker(d_{\mathfrak{p}}) \cong Hom(H_{L,\mathfrak{p}}, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Q}_p/\mathbb{Z}_p$$

  as groups, and the theorem follows in this case.

- when E has non-split multiplicative reduction at p, we have

$$\mathcal{C} \cong \mu_{p^\infty} \otimes \phi$$

as $G_{\mathbb{Q}_p}$-modules and

$$\mathcal{D} \cong \mathbb{Q}_p/\mathbb{Z}_p \otimes \phi$$

as $G_{\mathbb{Q}_p}$-modules with ϕ the unramified non-trivial quadratic character of $G_{\mathbb{Q}_p}$. Since $F_{\infty,\tilde{p}}/\mathbb{Q}_p$ is totally ramified, we have

$$\mathcal{D}^{G_{F_{\infty,\tilde{p}}}} = 0$$

and hence

$$ker(d_{\mathfrak{p}}) = 0.$$

□

2.5 Subconclusion

We continue to assume that the triple (E, p, m) satisfies the assumptions made in Section 1.1 and that $Y_p(E/F_\infty)$ is finitely generated over $\Lambda(H)$. Again, write L to denote any subfield of F_∞ which is a finite extension over $K = \mathbb{Q}(\mu_p)$. Recall that in this case, H_L is always isomorphic to $\mathbb{Z}_p$. We shall apply the results here in later chapters for $L = K$ and F_n for $n \geq 1$.

Proposition 2.5.1. *We have*

$$rank_{\Lambda(H_L)} Y_p(E/F_\infty) = \lambda_{\Lambda(\Gamma_L)} \left(X_p(E/F_\infty)_{H_L} \right) \tag{2.12}$$

Proof. Considering $cd_p(H_L) = 1$, Howson's formula (1.8) gives

$$rank_{\Lambda(H_L)} Y_p(E/F_\infty) = rank_{\mathbb{Z}_p} Y_p(E/F_\infty)_{H_L} - rank_{\mathbb{Z}_p} H_1\left(H_L, Y_p(E/F_\infty)\right) \tag{2.13}$$

On the other hand, we have an exact sequence

$$0 \to H_1(H_L, X_p(E/F_\infty)(p)) \to H_1(H_L, X_p(E/F_\infty)) \to H_1(H_L, Y_p(E/F_\infty)) \to$$
$$H_0(H_L, X_p(E/F_\infty)(p)) \to H_0(H_L, X_p(E/F_\infty)) \to H_0(H_L, Y_p(E/F_\infty)) \to 0.$$

Since $H_i(H_L, X_p(E/F_\infty)(p))$ being p-primary for $i = 0, 1$, we conclude that

$$rank_{\mathbb{Z}_p} H_i(H_L, Y_p(E/F_\infty)) = \lambda_{\Lambda(\Gamma_L)} H_i(H_L, X_p(E/F_\infty))$$

for $i = 0, 1$ and the proof is complete once we prove the following lemma.

□

Lemma 2.5.1. *We have*

$$H^1\left(H_L, Sel_p(E/F_\infty)\right) = 0 \tag{2.14}$$

Proof. By definition, we have

$$0 \longrightarrow Sel_p(E/F_\infty) \longrightarrow H^1(G_S(F_\infty), E_{p^\infty}) \xrightarrow{\lambda_{F_\infty}} \bigoplus_{v \in S} J_v(F_\infty)$$

and hence we have our target module lies in the long exact sequence

$$0 \longrightarrow Sel_p(E/F_\infty)^{H_L} \longrightarrow H^1(G_S(F_\infty), E_{p^\infty})^{H_L} \xrightarrow{\rho_{F_\infty}} \left(Im(\lambda_{F_\infty})\right)^{H_L}$$
$$\longrightarrow H^1(H_L, Sel_p(E/F_\infty)) \longrightarrow H^1(H_L, H^1(G_S(F_\infty), E_{p^\infty})) \tag{2.15}$$

So, it suffices to show

1. $H^1(G_S(F_\infty), E_{p^\infty})^{H_L} \xrightarrow{\rho_{F_\infty}} (Im\lambda_{F_\infty})^{H_L}$ is surjective
2. $H^1(H_L, H^1(G_S(F_\infty), E_{p^\infty})) = 0$

For 1, clearly,

$$Im(\lambda_{F_\infty})^{H_L} \subseteq \left(\bigoplus_{v \in S} J_v(F_\infty) \right)^{H_L}$$

Corollary 2.3.1 says that $\lambda_{L^{cyc}}$ is surjective, also,

$$coker(\oplus_{u \in S(L^{cyc})} h_u) \subseteq \oplus_{w \in S(F_\infty)} H^2(H_{L,u}, E(F_{\infty,w}))_{p^\infty} = 0$$

since the p-cohomological dimension of $H_{L,u}$

$$cd_p(H_{L,u}) \leqslant 1$$

by the commutativity of the fundamental diagram eq(2.3),

$$H^1(G_S(F_\infty), E_{p^\infty})^{H_L} \xrightarrow{\lambda_{F_\infty}^{H_L}} (\oplus_{v\in S} J_v(F_\infty))^{H_L}$$

is surjective, hence so is ρ_{F_∞}.
For 2, using the Hochschild-Serre spectral sequence,

$$H^2(G_S(L^{cyc}), E_{p^\infty}) \longrightarrow H^1(H_L, H^1(G_S(F_\infty), E_{p^\infty})) \longrightarrow H^3(H_L, E_{p^\infty}(F_\infty))$$

is exact. The first term $H^2(G_S(L^{cyc}), E_{p^\infty}) = 0$ due to Corollary 2.3.1. The last term $H^3(H_L, E_{p^\infty}(F_\infty)) = 0$ since $cd_p(H_L) = 1$. Hence, $H^1(H_L, H^1(G_S(F_\infty), E_{p^\infty})) = 0$.

□

We have

Proposition 2.5.2.

$$rank_{\Lambda(H_L)} Y_p(E/F_\infty) = \lambda_{\Lambda(\Gamma_L)}\left(\widehat{Sel_p(E/L^{cyc})}\right) + \sum_{u\in S(L^{cyc})} corank_{\mathbb{Z}_p} ker(h_u). \quad (2.16)$$

Proof. This is just the association of eq(2.6) and eq(2.12). □

Chapter 3

Root Number Computations

3.1 Root Numbers

The aim of this section is to give the definition of root numbers, more particularly the root numbers of the representations attached to elliptic curves and their twists by self-dual representations. I shall outline these definitions with the acknowledgement of various facts without repeating the technical proofs, which can mostly be found in Rohrlich's paper [23] and Deligne's paper [6].

Definition:. *Let E be an elliptic curve defined over a number field K. We define the global root number as*

$$w(E) = \prod_v w(E/K_v),$$

where $w(E/K_v)$ is the local root number and the product runs through all places v of K. If ρ is a self-dual representation of $Gal(\bar{K}/K)$, we define the twisted global root numbers similarly as

$$w(E,\rho) = \prod_v w(E/K_v,\rho_v),$$

where ρ_v denote the restricted representation of ρ to a pre-fixed decomposition subgroup $Gal(\bar{K}_v/K_v)$ for each place v of K.

Hence, it is down to defining the local root numbers $w(E/K_v)$ and $w(E/K_v,\rho_v)$ for all places v of K. Let F denote the local field K_v. By abuse of notation, we still write the twisted local root number as $w(E/F,\rho)$, without the subindex v

to ρ, with understanding that ρ means here its restriction to $Gal(\bar{F}/F)$, which can be identified as a subgroup of $Gal(\bar{K}/K)$ by choosing a place $\bar{v}$ of $\bar{K}$ above v. The choice of $\bar{v}$ will determined the subgroup $Gal(\bar{F}/F)$ up to conjugation and hence the isomorphic class of ρ is determined independent of the choice of place. The definition of the local root numbers will be given separately in the case where either F is Archimedean or non-Archimedean.

When F is non-Archimedean: Let F be a finite extension of $\mathbb{Q}_p$, and denote by $\bar{F}$ a algebraic closure of F. We denote by $\mathcal{O}_F$ the ring of integers in F, and π_F a fixed local parameter of F. We shall also fix a $\Phi \in Gal(\bar{F}/F)$ which acts as the inverse of the Frobenius in the residue fields, and call Φ the geometric Frobenius.

Definition: (Weil groups and Weil-Deligne groups)**.** *The Weil group of F, denoted by $W_F \stackrel{def}{=} W(\bar{F}/F)$ is the subgroup of $Gal(\bar{F}/F)$ generated by the inertia subgroup $I \stackrel{def}{=} I_F$ and the geometric Frobenius Φ. The Weil-Deligne group of F, denoted by W'_F, is defined to be the group:*

$$W'_F \stackrel{def}{=} \mathbb{C} \rtimes W_F$$

where W_F the Weil group of F acts on $\mathbb{C}$ by

$$gzg^{-1} = \omega_F(g)z, \quad g \in W_F, \ z \in \mathbb{C}$$

where $\omega_F : W_F \longrightarrow \mathbb{C}^\times$ is the unramified character, which sends Φ to the reciprocal of the order of the residue field of F.
The Weil group W_F is equipped with a topology satisfying:-

1. The subgroup I_F is open in W_F,
2. The relative topology on I_F coincides to the one from $Gal(\bar{F}/F)$,
3. Left multiplication by Φ is a homeomorphism.

The topology of the Weil-Deligne group W'_F is regarded as the product topology of the Cartesian product of W_F and $\mathbb{C}$.

Definition:. *A representation $\rho' = (\rho, N)$ of W'_F is a continuous homomorphism*

$$\rho' : W'_F \longrightarrow GL(V)$$

where V is a finite dimensional vector space over $\mathbb{C}$, such that $\rho' \mid_{\mathbb{C}}$ is analytic. Here, the correspondent pair (ρ, N) is given by

$$(\rho, N) = (\rho' \mid_{W_F}, (log\rho'(z))/z)$$

for any $z \in \mathbb{C}^{\times}$. Conversely, given any ρ a representation of W_F on V, that is a continuous homomorphism from W_F to $GL(V)$, and N any nilpotent endomorphism on V, satisfying

$$\rho(g)N\rho(g)^{-1} = \omega_F(g)N$$

for all $g \in W_F$, then ρ' can be recovered by

$$\rho'(gz) = \rho(g)exp(zN)$$

where $z \in \mathbb{C}$.

In [23, section 4], Rohrlich explains a recipe to obtain $\mathbb{C}$ representations of Weil-Deligne group from l-adic Galois representations. Let l be a rational prime different from p and choose a nontrivial character $t_l : I \longrightarrow \mathbb{Q}_l$. The recipe is from the following:-

Proposition 3.1.1. *[23, p.131] Let $\tau_l : Gal(\bar{F}/F) \longrightarrow GL(V_l)$ be an l-adic representation, where V_l is a finite dimensional vector space over $\mathbb{Q}_l$.*

1. *There is a unique nilpotent endomorphism N_l of V_l such that*

$$\tau_l(i) = exp(t_l(i)N_l)$$

   for i in some open subgroup of I and furthermore, $\tau_l(g)N_l\tau_l(g)^{-1} = \omega_F(g)N_l$ for all $g \in W_F$.

2. *The map $\sigma_l : W_F \longrightarrow GL(V_l)$ defined by sending $g = \Phi^m i$ with $m \in \mathbb{Z}$ and $i \in I$ to $\tau_l(g)exp(-t_l(i)N_l)$, is a homomorphism which is trivial on an open subgroup of I.*

3. *$\sigma_l(g)N_l\sigma_l(g)^{-1} = \omega_F(g)N_l$ for all $g \in W_F$.*

4. *Pick an embedding $\iota : \mathbb{Q}_l \hookrightarrow \mathbb{C}$ and consider the extension of scalars of the vector space V_l via ι, we can associate N_l and σ_l from 1 and 2 above canonically to $N_{l,\iota}$ and $\sigma_{l,\iota}$ as endomorphism and representation on $V_l \otimes_\iota \mathbb{C}$ respectively, and the isomorphic class of the representation $\sigma'_{l,\iota} = (\sigma_{l,\iota}, N_{l,\iota})$ is independent on the choice of Φ and t_l.*

Definition:. *Suppose that E is an elliptic curve defined over F, pick l a prime different from p and an embedding $\iota : \mathbb{Q}_l \hookrightarrow \mathbb{C}$. Let $\tau_{E/F,l} : Gal(\bar{F}/F) \longrightarrow GL((T_l(E) \otimes \mathbb{Q}_l)^*)$ be the contragredient of the natural Galois representation on the Tate-module $T_l(E) \otimes \mathbb{Q}_l$. Denote by $\sigma'_{E/F,l,\iota} = (\sigma_{E/F,l,\iota}, N_{E/K,l,\iota})$ the associated $\mathbb{C}$-representation of W'_F defined by the recipe above. The isomorphic class of $\sigma'_{E/F,l,\iota}$ is independent of the choice of l and ι and hence we shall just denote by $\sigma'_{E/F}$ as we will only be interested in the isomorphic classes of representations from now on.*

We shall define the ϵ-factor of any representation $\rho' = (\rho, N)$ of the Weil-Deligne group W'_F, which at last will lead to the definition of root number. This definition goes very deep into a theorem of Langlands [17] regarding the existence of a function ϵ.

For any non-trivial additive character $\psi : F \longrightarrow \mathbb{C}^\times$, let $n_F(\psi)$ denote the largest integer n such that $\psi(\pi_F^{-n}\mathcal{O}_F) = 1$. For any quasicharacter $\chi : F^\times \longrightarrow \mathbb{C}^\times$, denote $a_F(\chi)$ as 0 if $\chi(\mathcal{O}_F^\times) = 1$ or otherwise the smallest integer m such that $\chi(U_{F,m}) = 1$, where $U_{F,m}$ is the subgroup of units in F that are congruent to 1 modulo π_F^m. By fixing a Haar measure dx_F on F, we can define

Definition: (Local ϵ-factors for quasicharacter χ)**.** *Let c denote any element of $F^\times$ with valuation equals to $n_F(\psi) + a_F(\chi)$. Then we define*

$$\epsilon(\chi, \psi, dx_F) \overset{def}{=} \begin{cases} \frac{\chi(c)}{\omega_F(c)} \times \int_{\mathcal{O}_F} dx_F & if\ \chi\ is\ unramified \\ \int_{c^{-1}\mathcal{O}_F^\times} \chi^{-1}(x)\psi(x)dx_F & if\ \chi\ is\ ramified. \end{cases} \tag{3.1}$$

We can identify any quasicharacter $\chi : F^\times \longrightarrow \mathbb{C}^\times$ with a one dimensional representation of the Weil group W_F, since any of the latter must factor through the abelian quotient W_F^{ab} which is isomorphic to $F^\times$ via the Artin reciprocity map.

We shall need a corollary of Brauer Induction Theorem and an existence theorem due to Langlands and Deligne [6] to generalize the definition above to arbitrary virtual $\mathbb{C}$-representations of Weil group.

Proposition 3.1.2. *[23, Corollary 2 of Section 2] Let ρ be a representation of W_F and denote by $[\rho]$ its class in the Grothendieck group of virtual representations. Then we have*

$$[\rho] = (dim\rho) \cdot [\mathbf{1}_F] + \sum_{(L,\chi,\chi')} c_{L,\chi,\chi'}[Ind_F^L(\chi - \chi')] \tag{3.2}$$

where the sum runs over triples with L all finite extensions of F in $\bar{F}$, χ and χ' all quasicharacters of $L^\times$, with almost all $c_{L,\chi,\chi'} \in \mathbb{Z}$ are zero. Here, the notation $[Ind_F^L(\chi - \chi')]$ denotes the class $[Ind_F^L\chi] - [Ind_F^L\chi']$ and $\mathbf{1}_F$ denotes the trivial quasicharacter of W_F.

Theorem 3.1.1. *There exists a unique function $\epsilon(\star, \star, \star)$ satisfying the following*

i

$$\epsilon(\rho_2, \psi, dx_F) = \epsilon(\rho_1, \psi, dx_F) \cdot \epsilon(\rho_3, \psi, dx_F)$$

for any short exact sequence $0 \to \rho_1 \to \rho_2 \to \rho_3 \to 0$ of representations of the Weil group W_F.

ii *For any finite extension L of F in $\bar{F}$, and any Haar measure dx_L of L,*

$$\frac{\epsilon(Ind_F^L\rho, \psi, dx_F)}{\epsilon(\rho, \psi \circ tr_{L/F}, dx_L)} = \left(\frac{\epsilon(Ind_F^L\mathbf{1}_L, \psi, dx_F)}{\epsilon(\mathbf{1}_L, \psi \circ tr_{L/F}, dx_L)}\right)^{dim\rho}$$

for any virtual representation ρ of Weil group $W_L = W_F \cap Gal(\bar{F}/L)$, where $\mathbf{1}_L$ denotes the trivial quasicharacter of W_L and $tr_{L/F}$ is the trace map from L to F.

iii *For any finite extension L of F in $\bar{F}$, the ϵ-factor of any quasicharacter χ of $L^\times$, $\epsilon(\chi, \psi_L, dx_L)$ is given by the formula in (3.1) with all the factors considered as defined with respect to field L.*

This theorem of Langlands in fact holds for all local fields, including the Archimedean fields $\mathbb{R}$ and $\mathbb{C}$. The only difference when dealing with Archimedean fields is on the criterion iii, which appoints the values of the ϵ for quasicharacter differently. See below (3.7) and (3.9).

We can now explicitly give a formula for $\epsilon(\rho, \psi, dx_F)$ as a result of this theorem.

Definition: (Local ϵ-factors for representations of Weil groups)**.** *Let ρ be as given in the proposition above (3.2), we define its ϵ-factor as the one which exists as described in the Theorem above. Namely,*

$$\epsilon(\rho, \psi, dx_F) \stackrel{def}{=} \epsilon(\mathbf{1}_F, \psi, dx_F)^{dim\rho} \cdot \prod_{(L,\chi,\chi')} \left(\frac{\epsilon(\chi, \psi \circ tr_{L/F}, dx_L)}{\epsilon(\chi', \psi \circ tr_{L/F}, dx_L)} \right)^{c_{L,\chi,\chi'}} \tag{3.3}$$

where each term on the right hand side is given in (3.1).

Definition: (Local ϵ-factors for representations of Weil-Deligne group)**.** *The local ϵ-factor of $\rho' = (\rho, N)$ is defined by*

$$\epsilon(\rho', \psi, dx) \stackrel{def}{=} \epsilon(\rho, \psi, dx)\delta(\rho')$$

where

$$\delta(\rho') := det\left(-\Phi \mid V^I/V_N^I\right)$$

with $V_N^I = V^I \cap ker(N)$.

A representation ρ' of W_F' is called essentially symplectic if there exists a $\rho' \otimes \omega_F^k$-invariant bilinear non-degenerate symplectic form on V for certain real number k.

The representation $\sigma'_{E/F}$ that defined earlier is essentially symplectic. For the dual of the Weil-pairing, which is symplectic, is W_F'-invariant under the representation $\sigma'_{E/F} \otimes \omega_F^{1/2}$. [23, c.f section 16] .

Definition: (Local root numbers). *The root number of $\rho' = (\rho, N)$ is defined as*

$$w_F(\rho', \psi) = \frac{\epsilon(\rho', \psi, dx_F)}{|\ \epsilon(\rho', \psi, dx_F)\ |}.$$

This value is independent on the choice of the Haar measure dx_F on F, and furthermore independent on the choice of the additive character ψ, if ρ' is essentially symplectic, and we shall simplify the notation by just $w_F(\rho')$ and in this case, it takes value ± 1.

Definition: (Local root numbers for elliptic curves). *The (local) root number for an elliptic curve E defined over a non-Archimedean local field F is*

$$w(E/F) \stackrel{def}{=} w_F(\sigma'_{E/F}).$$

For any orthogonal $\mathbb{C}$-representation ρ of $Gal(\bar{F}/F)$, we can also define the twisted (local) root number, which is again independent of the choice of the additive character ψ by

$$w(E/F, \rho) \stackrel{def}{=} w_F(\sigma'_{E/F} \otimes \rho).$$

When F is Archimedean: Let F be $\mathbb{R}$ or $\mathbb{C}$ here.

Definition: (Weil groups and Weil-Deligne groups). *When $F = \mathbb{C}$, we define its Weil-Deligne group $W'_{\mathbb{C}}$ and its Weil group $W_{\mathbb{C}}$ as*

$$W'_{\mathbb{C}} = W_{\mathbb{C}} \stackrel{def}{=} \mathbb{C}^\times;$$

when $F = \mathbb{R}$, we define its Weil-Deligne group $W'_{\mathbb{R}}$ and its Weil group $W_{\mathbb{R}}$ as

$$W'_{\mathbb{R}} = W_{\mathbb{R}} \stackrel{def}{=} \mathbb{C}^\times \cup J\mathbb{C}^\times,$$

where $J^2 = -1$, and $JzJ^{-1} = \bar{z}$ for all $z \in \mathbb{C}^\times$.

Definition:. *When E is an elliptic curve defined over $\mathbb{C}$, we define a representation*

$$\sigma'_{E/\mathbb{C}} = \sigma_{E/\mathbb{C}} : W'_{\mathbb{C}} \longrightarrow GL(\mathbb{C}^2)$$
$$z \mapsto \begin{pmatrix} 1/z & 0 \\ 0 & 1/\bar{z} \end{pmatrix};$$

when E is an elliptic curve defined over $\mathbb{R}$, we define a representation

$$\sigma'_{E/\mathbb{R}} = \sigma_{E/\mathbb{R}} : W'_{\mathbb{R}} \longrightarrow GL(\mathbb{C}^2)$$
$$z \mapsto \begin{pmatrix} 1/z & 0 \\ 0 & 1/\bar{z} \end{pmatrix}$$
$$Jz \mapsto \begin{pmatrix} 0 & 1/z \\ -1/\bar{z} & 0 \end{pmatrix}$$

for $z \in \mathbb{C}^\times$.

Definition:. *Let*

$$\psi_{\mathbb{R},y}(x) = e^{2\pi i y x}, \tag{3.4}$$

$$\psi_{\mathbb{C},y}(z) = e^{2\pi i \cdot tr_{\mathbb{C}/\mathbb{R}}(yz)} \tag{3.5}$$

be additive characters on $\mathbb{R}$ and $\mathbb{C}$ respectively, with $y \in \mathbb{R}^\times$ and $y \in \mathbb{C}^\times$ respectively, and let $d_{\mathbb{R}}$ denote the Lebesgue measure on $\mathbb{R}$ and $d_{\mathbb{C}}$ the twice Lebesgue measure on $\mathbb{C}$.

In contrast to the non-Archimedean case (3.1), we can define the ϵ-factor for quasicharacter of W_F where F is $\mathbb{R}$ or $\mathbb{C}$. Firstly, it is easily seen that in both cases, we have canonical isomorphisms $F^\times \cong W_F^{ab}$. Hence we can identify any quasi-character of $F^\times$ with an isomorphic class of one-dimensional representations of the Weil-group W_F.

Definition: (Local ϵ-factors of Archimedean fields)**.** *When $F = \mathbb{R}$, all the quasi-characters $\chi_{m,r}$ of $\mathbb{R}^\times$ are parameterized by a pair $(m, r) \in \{0, 1\} \times \mathbb{C}$, given as*

$$\chi_{m,r}(x) \overset{def}{=} (sgnx)^m |x|^r \tag{3.6}$$

and we define

$$\epsilon(\chi_{m,r}, \psi_{\mathbb{R},y}, d_{\mathbb{R}}) \overset{def}{=} (i \cdot sgny)^m |y|^r \tag{3.7}$$

where $y \in \mathbb{R}^\times$ as appeared in (3.4).

When $F = \mathbb{C}$, all the quasi-characters $\chi_{\iota,m,r}$ of $\mathbb{C}^\times$ are parameterized by a triple $(\iota, m, r) \in \{$identity, complex conjugation$\} \times \mathbb{N} \times \mathbb{C}$, given as

$$\chi_{\iota,m,r}(z) \overset{def}{=} \iota(z)^m |z\bar{z}|^r \tag{3.8}$$

and we define

$$\epsilon(\chi_{\iota,m,r}, \psi_{\mathbb{C},y}, d_{\mathbb{C}}) \overset{def}{=} (i \cdot \iota(y))^m |y\bar{y}|^r \tag{3.9}$$

where $y \in \mathbb{C}^\times$ as appeared in (3.5).

According to the remark after Theorem 3.1.1, when we replace criterion iii by (3.7) and (3.9), we can define a unique function $\epsilon(\star, \psi_{F,y}, d_F)$ for every virtual representation of the Weil-group (or equivalently the Weil-Deligne group) W_F, where F is $\mathbb{R}$ and $\mathbb{C}$, in view of the corollary of the Brauer Theorem stated earlier. Finally, we can define the local root numbers $w(\star, \psi_{F,y})$ for every virtual representation of W'_F exactly the same as the non-Archimedean case. Similarly, when ρ' is essentially symplectic, $w(\rho', \psi_{F,y})$ takes value ± 1 and is independent of the choice of $y \in F^\times$. The Weil group W_F is of no difference to the Weil-Deligne group W'_F when F is Archimedean, and hence the notation $\rho' = (\rho, N)$ will always mean $N = 0$ and $\rho' = \rho$ in this case.

Proposition 3.1.3. *We have*

(i) $w(E/\mathbb{C}) \overset{def}{=} w(\sigma_{E/\mathbb{C}}) = -1$

(ii) $w(E/\mathbb{R}) \overset{def}{=} w(\sigma_{E/\mathbb{R}}) = -1$

(iii) $w(E/\mathbb{C}, \rho) \overset{def}{=} w(\sigma_{E/\mathbb{C}} \otimes \rho) = (-1)^{dim\rho}$

(iv) $w(E/\mathbb{R}, \rho) \overset{def}{=} w(\sigma_{E/\mathbb{R}} \otimes \rho) = (-1)^{dim\rho}$

for any elliptic curve E defined over $\mathbb{C}$ and any self-dual representation ρ of $W_{\mathbb{C}}$ and $W_{\mathbb{R}}$ in (iii) and (iv) respectively.

We conclude this section by quoting a formula by V.Dokchitser, of which I shall apply to compute certain root numbers in next chapter.

Theorem 3.1.2. *(V.Dokchitser)*
Let E be an elliptic curve defined over $\mathbb{Q}$, and ρ an Artin representation which is self-dual. Let S_{add} and S_{multi} be the set of rational primes at where E has additive reduction and multiplicative reduction respectively. If ρ is unramified at all places of S_{add}, then

$$w(E,\rho) = w(E)^{dim\rho}\cdot(-1)^{dim\rho^-}\cdot\prod_{p\in S_{multi}} s_p^{dim\rho - dim\rho^{I_p}}\cdot det(\Phi_p|\rho^{I_p})\cdot\prod_{p\in S_{add}} det(\Phi_p|\rho)^{N_p(E)}$$

where ρ^- denotes the eigenspace of $\rho(\tau)$ of eigenvalue -1, where τ is the complex conjugation, and the conductor of E has prime factorization $\prod_p p^{N_p(E)}$. Here Φ_p is an geometric Frobenius element, I_p is the corresponding inertia subgroup and

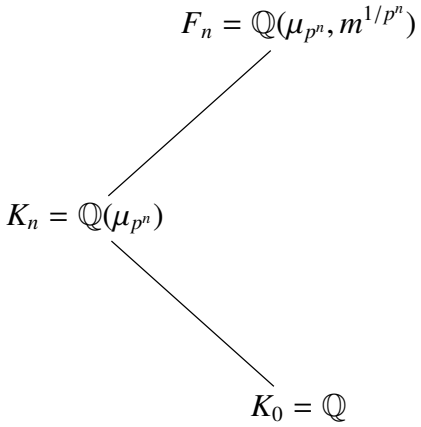
$$s_p = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction at } p, \\ 1 & \text{if } E \text{ has non-split multiplicative reduction at } p. \end{cases}$$

Proof. See [8].

□

3.2 Computations of Root Numbers

Recall the tower of fields:-



and we denote $N_n \stackrel{\text{def}}{=} Gal(F_n/K_n)$, $G_n \stackrel{\text{def}}{=} Gal(F_n/\mathbb{Q})$ and $H_n \stackrel{\text{def}}{=} Gal(K_n/\mathbb{Q})$.

Using external semi-direct product

$$G_n = N_n \rtimes_{\varphi_n} H_n$$

where

$$\begin{array}{rccc} \varphi_n : & H_n & \longrightarrow & Aut(N_n) \\ & h & \mapsto & (n \mapsto n_h \cdot n \cdot n_h^{-1}) \end{array}$$

where $n_h \in G_n$ is a lifting of h.

Definition:. *Let*

$$\rho_{\chi_n} \overset{def}{=} Ind_{\mathbb{Q}}^{K_n} \chi_n,$$

where χ_n denotes any character of exact order p^n of the Galois group $Gal(F_n/K_n)$.

We will have deeper discussions on these Artin representations ρ_{χ_n} in Section 3.4. We shall see, in Proposition 3.4.1 that ρ_{χ_n} are self dual and we shall assume this fact in this section.

Throughout this section, we shall assume again that (E, p, m) satisfies the assumptions made in Section 1.1. It is clear to see that the criteria in Theorem 3.1.2 are met for $\rho = \rho_K \overset{\text{def}}{=} Ind_{\mathbb{Q}}^{K} 1$ and ρ_{χ_n}, since they are unramified outside $p \cdot m$ and by the assumption, E has semistable reduction at all the prime divisors of $p \cdot m$. We shall apply the formula in Theorem 3.1.2 in computing the quotient between root numbers

$$w(E/K) = w(E, Ind_{\mathbb{Q}}^{K} 1) \text{ and } w(E, \rho_{\chi_n}).$$

Let us first compute the terms appearing in the formula in Theorem 3.1.2 for $\rho = \rho_K$ and ρ_{χ_n} respectively.

Proposition 3.2.1. *We have*

1. $dim\rho_K^- = \frac{1}{2} dim\rho_K = \frac{1}{2}(p-1)$
2. $\begin{cases} dim\rho_K^{I_p} = 1, \\ dim\rho_K^{I_q} = dim\rho_K = p-1, \quad when\ q \neq p \end{cases}$

3. $\begin{cases} det(\Phi_p|\rho_K^{I_p}) = 1, \\ det(\Phi_q|\rho_K^{I_q}) = (\frac{q}{p}), \quad when\ q \neq p \end{cases}$

where I_p and I_q denotes the inertia subgroups at primes p and q respectively of the abelian extension $K/\mathbb{Q}$.

Proof. Fix an embedding $K \hookrightarrow \mathbb{C}$ and pick ξ_p, a fixed primitive p^{th} root of unity. Let $g_i \in Gal(K/\mathbb{Q})$ such that $g_i(\xi_p) = \xi_p^i$ with i a primitive root modulo p. Then g_i generates $Gal(K/\mathbb{Q})$ and we denote $g_{i^l} \stackrel{\text{def}}{=} (g_i)^l$ for any l modulo $p-1$.
$\rho_K = Ind_{\mathbb{Q}}^K 1_K$ acts on the vector space spanned by $\{g_i, \ldots\ldots, g_{i^{p-1}}\}$. Since $g_{i^l} \cdot g_{i^j} = g_{i^{l+j}}$, the matrix of $\rho_K(g_{i^l})$ under this basis is

$$\begin{pmatrix} 0 & I_{p-1-l} \\ I_l & 0 \end{pmatrix}$$

where I_k denotes the $k \times k$ identity matrix.
In particular, since the image of complex conjugation in $Gal(K/\mathbb{Q})$ takes $\xi_p \mapsto \xi_p^{-1} = \xi_p^{p-1} = (\xi_p)^{i^{\frac{p-1}{2}}}$ hence it is $g_{i^{\frac{p-1}{2}}}$, and the corresponding matrix is

$$\begin{pmatrix} 0 & I_{\frac{p-1}{2}} \\ I_{\frac{p-1}{2}} & 0 \end{pmatrix}$$

which has zero trace. Therefore

$$dim\rho_K^+ = dim\rho_K^- = \frac{1}{2} dim\rho_K = \frac{1}{2}(p-1)$$

which justifies part(1).
Since ρ_K factors through K, it can be viewed as a representation of $Gal(K/\mathbb{Q})$. Since p is totally ramified over $K/\mathbb{Q}$, the inertia subgroup $I_p = Gal(K/\mathbb{Q})$. Suppose

$$\sum_{k=1}^{p-1} c_k \cdot g_{i^k} \in \rho_K^{I_p}$$

i.e

$$\rho_K(g_{i^l}) \cdot (\sum_{k=1}^{p-1} c_k \cdot g_{i^k}) = \sum_{k=1}^{p-1} c_k \cdot g_{i^k}$$

for every $1 \leq l \leq p-1$, i.e

$$(c_{p-l}, \ldots, c_{p-1}, c_1, c_2, \ldots, c_{p-1-l}) = (c_1, \ldots, c_{p-1})$$

When l runs over $1, 2, 3, \ldots, p-1$, we see this criterion is equivalent to

$$c_1 = c_2 = \ldots = c_{p-1}$$

i.e $dim\rho_K^{I_p} = 1$. Since prime $q \neq p$ is unramified over $K/\mathbb{Q}$, the inertia subgroup $I_q = \{id\} \subset Gal(K/\mathbb{Q})$. Hence,

$$dim\rho_K^{I_q} = dim\rho_K = p-1$$

that shows part(2).
For prime $q \neq p$, denote q^{-1} as the inverse of the residue of q modulo p. Since $\Phi_q(\xi_p) = \xi_p^{q^{-1}} \equiv \xi_p^{i^{-d}}$ where $q \equiv i^d \bmod p$ for some d modulo $p-1$. The matrix of $\rho_K(\Phi_q)$ is

$$\begin{pmatrix} 0 & I_d \\ I_{p-1-d} & 0 \end{pmatrix}$$

by picking the least positive residue of d modulo $p-1$.
This matrix has

$$\begin{aligned} \text{determinant} &= (-1)^{\text{parity of permutation of } p-d, p-d+1, \ldots, p-1, 1, 2, \ldots, p-d-1} \\ &= (-1)^{(p-1-d)\times d} \\ &= (-1)^d \\ &= (\frac{q}{p}). \end{aligned}$$

The image of Φ_p in $Gal(K/\mathbb{Q})$ is trivial, since p is totally ramified over $K/\mathbb{Q}$ hence

$$det(\Phi_p | \rho_K^{I_p}) = 1$$

. □

Recall that the notion $m = \prod q_i^{r_i}$, $p \nmid r_i$.

Proposition 3.2.2. *We have*

1. $$dim\rho^{-}_{\chi_n} = \frac{1}{2}dim\rho_{\chi_n} = \frac{1}{2}p^{n-1}(p-1)$$

2. - *For prime p,*
     - *if $p \mid m$, then*
       $$dim\rho^{I_p}_{\chi_n} = 0.$$
     - *if $p \nmid m$, then*
       $$dim\rho^{I_p}_{\chi_n} = \begin{cases} 1, & \text{for } r \geq n, \\ 0, & \text{for } n > r. \end{cases}$$
       where $r \geq 0$ be the integer such that $p^{r+1} \parallel m^{p-1} - 1$.
   - *For prime $q_i \mid m$ but $q_i \neq p$,*
     $$dim\rho^{I_{q_i}}_{\chi_n} = 0.$$
   - *For prime $q \nmid mp$,*
     $$dim\rho^{I_q}_{\chi_n} = dim\rho_{\chi_n} = p^{n-1}(p-1).$$

3. $$det(\Phi_q|\rho^{I_q}_{\chi_n}) = \begin{cases} 1, & \text{for prime } q \mid mp, \\ (\frac{q}{p}), & \text{for prime } q \nmid mp. \end{cases}$$

where I_p and I_q denotes the inertia subgroups at primes p and q respectively of the extension $F_n/\mathbb{Q}$.

Proof. Fix an embedding $F_n \hookrightarrow \mathbb{C}$, and pick ξ_{p^n}, a fixed primitive p^n-th root of unity. Let $\sigma_i \in H_n$, such that $\sigma_i(\xi_{p^n}) = \xi^i_{p^n}$ with i a primitive root modulo p^n, then σ_i generates H_n, a cyclic group of order $p^{n-1}(p-1)$, and we denote $\sigma_{i^l} \overset{\text{def}}{=} (\sigma_i)^l$ for any l modulo $p^{n-1}(p-1)$.
There is a canonical isomorphism between $Gal(F_n/K_n)$ and $\mathbb{Z}/p^n\mathbb{Z}$, $n_k \in Gal(F_n/K_n)$ is correspondent to k modulo p^n, via the relation $n_k(\sqrt[p^n]{m}) = \xi^k_{p^n} \cdot \sqrt[p^n]{m}$.

The multiplication in G_n is carried out in the following fashion:-

$$(n_k, \sigma_{i^l}) \times (n_{k'}, \sigma_{i^{l'}}) = (n_k \times \varphi_n(\sigma_{i^l})(n_{k'}), \sigma_{i^l} \times \sigma_{i^{l'}})$$

Suppose χ_n is a character of $Gal(F_n/K_n) \cong \mathbb{Z}/p^n\mathbb{Z}$ of exact order p^n, i.e χ_n is fully determined by $e_{\chi_n} \stackrel{\text{def}}{=} \chi_n(n_1)$, a primitive element in μ_{p^n}.
Denote $g_{i^l} \stackrel{\text{def}}{=} (1, \sigma_{i^l}) \in G_n, \rho_{\chi_n}$ acts on the vector space spanned by $\{g_i, g_{i^2}, \ldots, g_{i^{p^{n-1}(p-1)}}\}$.
Since

$$\begin{aligned}(n_k, \sigma_{i^l}) \times (1, \sigma_{i^j}) &= (n_k \times \varphi_n(\sigma_{i^l})(1), \sigma_{i^{l+j}}) \\ &= (n_k, \sigma_{i^{l+j}})\end{aligned}$$

$$\begin{aligned}(1, \sigma_{i^{l+j}}) \times (\varphi_n(\sigma_{i^{l+j}})^{-1}(n_k), 1) &= (1 \times \varphi_n(\sigma_{i^{l+j}})(\sigma_{i^{l+j}})^{-1}(n_k)), \sigma_{i^{l+j}}) \\ &= (n_k, \sigma_{i^{l+j}})\end{aligned}$$

hence $\rho_{\chi_n}((n_k, \sigma_{i^l}))$ acts on the vector space $\mathbb{C}$-linearly via sending

$$g_{i^j} \mapsto \chi_n(\varphi_n(\sigma_{i^{l+j}})^{-1}(n_k)) \times g_{i^{l+j}}$$

Computation of the dimension of subspaces of ρ_{χ_n}

- $dim\rho^-_{\chi_n}$:-

  Since complex conjugation takes $\xi_{p^n} \mapsto \xi^{-1}_{p^n} = \xi^{i^{\frac{p^{n-1}(p-1)}{2}}}_{p^n}$ and fixes $\sqrt[p^n]{m} \in \mathbb{R}$, hence the image of complex conjugation in G_n is correspondent to $(1, \sigma_{-1}) = (1, \sigma_{i^{\frac{p^{n-1}(p-1)}{2}}})$ and the correspondent matrix is

  $$\begin{pmatrix} 0 & I_{\frac{p^{n-1}(p-1)}{2}} \\ I_{\frac{p^{n-1}(p-1)}{2}} & 0 \end{pmatrix}$$

  which has zero trace. Hence,

  $$dim\rho^+_{\chi_n} = dim\rho^-_{\chi_n} = \frac{1}{2} dim\rho_{\chi_n} = \frac{1}{2} p^{n-1}(p-1)$$

- $dim\rho^{Inertia}_{\chi_n}$:-

– For prime $q \nmid mp$,
q is unramified over $F_n/\mathbb{Q}$, hence the inertia subgroup $I_q = \{id\}$ and

$$dim\rho_{\chi_n}^{I_q} = dim\rho_{\chi_n} = p^{n-1}(p-1)$$

– For prime $q_i \mid m$ but $q_i \neq p$,
q_i is unramified over $K_n/\mathbb{Q}$, but totally ramified over F_n/K_n hence $I_{q_i} \cong N_n \subset G_n$.
Let

$$\sum_{j=1}^{p^{n-1}(p-1)} c_j \cdot g_{ij} \in \rho_{\chi_n}^{I_{q_i}}$$

i.e

$$\rho_{\chi_n}((n_k,1))(\sum_{j=1}^{p^{n-1}(p-1)} c_j \cdot g_{ij}) = (\sum_{j=1}^{p^{n-1}(p-1)} c_j \cdot g_{ij})$$

for all k modulo p^n, i.e

$$c_j \times \chi_n(\widetilde{\sigma_{ij}}^{-1} \cdot n_k \cdot \widetilde{\sigma_{ij}}) = c_j$$

for each j and all k modulo p^n, where $\widetilde{\sigma_{ij}}$ is any lifting in G_n of σ_{ij}. For each j, since χ_n is of exact order p^n, $\chi_n(\widetilde{\sigma_{ij}}^{-1} \cdot n_k \cdot \widetilde{\sigma_{ij}}) = 1$ if and only if $\widetilde{\sigma_{ij}}^{-1} \cdot n_k \cdot \widetilde{\sigma_{ij}} = id$ which holds if and only if $n_k = id$. Taking $k \neq 0$ modulo p^n implies that $c_j = 0$ for each j, therefore

$$dim\rho_{\chi_n}^{I_{q_i}} = 0.$$

– For prime p,

* if $p \mid m$,
then p is totally ramified over $F_n/\mathbb{Q}$, and the inertia subgroup

$$I_p \cong G_n.$$

Hence $\rho_{\chi_n}^{I_p} \subseteq \rho_{\chi_n}^{I_{q_i}} = 0$, so

$$dim\rho_{\chi_n}^{I_p} = 0.$$

* if $p \nmid m$, let $r \geq 0$ be the largest integer such that $p^{r+1} \mid m^{p-1}-1$, then it is shown in [28, Theorem 5.2 and Theorem 5.5] that
  - for $n > r \geq 0$, there are p^r distinct primes of F_n above p. Each of these has residue degree 1 and ramification degree $p^{n-r} \times p^{n-1}(p-1)$ and the inertia subgroup I_p contains the subgroup $N_n^{p^r}$.

  - for $r \geq n \geq 1$, there are p^n distinct primes of F_n above p. Each of these has residue degree 1 and ramification degree $p^{n-1}(p-1)$. Let ϱ be one of these primes, the corresponding inertia subgroup I_p is just the decomposition subgroup, which consists of pairs (n_{k_l}, σ_{i^l}), indexed by l modulo $p^{n-1}(p-1)$, where n_{k_l} is the unique element in N_n such that $n_{k_l} \cdot (\widetilde{\sigma_{i^l}}(\varrho)) = \varrho$, where $\widetilde{\sigma_{i^l}} = (1, \sigma_{i^l}) \in G_n$.

  Again let

$$\sum_{j=1}^{p^{n-1}(p-1)} c_j \cdot g_{i^j} \in \rho_{\chi_n}^{I_p}$$

  i.e

$$\rho_{\chi_n}((n_k, \sigma_{i^l}))(\sum_{j=1}^{p^{n-1}(p-1)} c_j \cdot g_{i^j}) = (\sum_{j=1}^{p^{n-1}(p-1)} c_j \cdot g_{i^j})$$

  for all $(n_k, \sigma_{i^l}) \in I_p$.

  In the case when $n > r \geq 0$, since there exists an non-trivial element $n_k \in N_n^{p^r} \subset I_p$. For the same reason as before, we have

$$dim\rho_{\chi_n}^{I_p} = 0.$$

  In the case when $r \geq n \geq 1$, $(n_k, \sigma_{i^l}) \in I_p$ if and only if $n_k = n_{k_l}$. Hence, for any l modulo $p^{n-1}(p-1)$ we have

$$\sum_{j=1}^{p^{n-1}(p-1)} c_j \cdot \chi_n(\varphi_n(\sigma_{i^{j+l}})^{-1} n_{k_l}) \cdot g_{i^{j+l}} = \sum_{j=1}^{p^{n-1}(p-1)} c_j \cdot g_{i^j}.$$

  I claim the equality

$$\chi_n(\varphi_n(\sigma_{i^{j+l}})^{-1} n_{k_l}) = \frac{\chi_n(\varphi_n(\sigma_{i^{j+l}})^{-1} n_{k_{j+l}})}{\chi_n(\varphi_n(\sigma_{i^j})^{-1} n_{k_j})},$$

from which we deduce that $\sum_{j=1}^{p^{n-1}(p-1)} c_j \cdot g_{i^j} \in \rho_{\chi_n}^{I_p}$ if and only if

$$\frac{c_j}{\chi_n(\varphi_n(\sigma_{i^j})^{-1} n_{k_j})} = \frac{c_l}{\chi_n(\varphi_n(\sigma_{i^l})^{-1} n_{k_l})}$$

for all j, l modulo $p^{n-1}(p-1)$, and thus

$$dim \rho_{\chi_n}^{I_p} = 1.$$

The claim follows from the equality

$$\begin{aligned} & \varphi_n(\sigma_{i^{j+l}})^{-1} n_{k_l} \cdot \varphi_n(\sigma_{i^j})^{-1} n_{k_j} = \varphi_n(\sigma_{i^{j+l}})^{-1} n_{k_{j+l}} \\ \Leftrightarrow \quad & n_{k_l} \widetilde{\sigma_{i^l}} \cdot n_{k_j} \widetilde{\sigma_{i^j}} \cdot \widetilde{\sigma_{i^{j+l}}}^{-1} = n_{k_l} \widetilde{\sigma_{i^l}} \cdot n_{k_j} \widetilde{\sigma_{i^l}}^{-1} = n_{k_{j+l}} \end{aligned}$$

which clearly holds since $n_{k_l} \widetilde{\sigma_{i^l}} \cdot n_{k_j} \widetilde{\sigma_{i^j}} \cdot \widetilde{\sigma_{i^{j+l}}}^{-1}$ is an element in N_n which maps $\widetilde{\sigma_{i^{j+l}}}(\varrho)$ to ϱ.

When $q = p$, since the residue degree over F_n is trivial, Φ_p is trivial and

$$det(\Phi_p | \rho_{\chi_n}^{I_p}) = 1.$$

When $q = q_i \mid m$ but $q_i \neq p$, we have shown that $\rho_{\chi_n}^{I_{q_i}} = 0$ and hence

$$det(\Phi_{q_i} | \rho_{\chi_n}^{I_{q_i}}) = 1.$$

How does Φ_q act on F_n, $q \nmid mp$.

The aim here is to compute $det(\Phi_q | \rho_{\chi_n})$ which takes value ± 1. Hence this is equal to computing $det(\phi_q | \rho_{\chi_n})$ where ϕ_q is an arithmetic Frobenius element. As

$$\phi_q : \xi_{p^n} \mapsto \xi_{p^n}^q = \xi_{p^n}^{i^d}$$

for some d modulo $p^{n-1}(p-1)$ such that $q \equiv i^d \bmod p^n$, hence

$$\phi_q = (n_k, \sigma_{i^d}) \in N_n \rtimes_{\varphi_n} H_n = G_n$$

for some k modulo p^n. Since

$$(n_k, \sigma_{i^d}) \cdot (1, \sigma_{i^j}) = (n_k, \sigma_{i^{d+j}}) = (1, \sigma_{i^{d+j}}) \cdot (\varphi_n(\sigma_{i^{d+j}})^{-1} n_k, 1)$$

the matrix of $\rho_{\chi_n}(\phi_q)$ under basis $\{g_i, g_{i^2}, \ldots, g_{i^{p^{n-1}(p-1)}}\}$ is

$$\begin{pmatrix}
0 & \cdots & \cdots & 0 & \chi_n(\varphi_n(\sigma_{i^{d+1}}^{-1})n_k) & 0 & \cdots & \cdots & 0 \\
0 & \cdots & \cdots & \cdots & 0 & \chi_n(\varphi_n(\sigma_{i^{d+2}}^{-1})n_k) & 0 & \cdots & 0 \\
 & & & & & & \ddots & & \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \ddots & \cdots & \cdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & \chi_n(\varphi_n(\sigma_{i^{p^{n-1}(p-1)-1}}^{-1})n_k) & 0 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & \chi_n(\varphi_n(\sigma_{i^{p^{n-1}(p-1)}}^{-1})n_k) \\
\chi_n(\varphi_n(\sigma_{i^1}^{-1})n_k) & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & \chi_n(\varphi_n(\sigma_{i^2}^{-1})n_k) & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
 & & \ddots & & & & & & \\
\cdots & \cdots & \ddots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & \cdots & 0 & \chi_n(\varphi_n(\sigma_{i^d}^{-1})n_k) & 0 & \cdots & \cdots & \cdots & 0
\end{pmatrix}$$

This matrix has

$$\begin{aligned}
\text{determinant} &= (-1)^{\text{parity of permutation of } d+1,d+2,\ldots,p^{n-1}(p-1),1,2,\ldots,d} \cdot \prod_{j=1}^{p^{n-1}(p-1)} \chi_n(\varphi_n(\sigma_{i^{d+j}}^{-1})n_k) \\
&= (-1)^{(p^{n-1}(p-1)-d)\times d} \cdot 1 \text{ (Applying the lemma below)} \\
&= (-1)^d \\
&= (\frac{q}{p})
\end{aligned}$$

□

Lemma 3.2.1. *Choose $g_{i^l} \overset{def}{=} (1, \sigma_{i^l})$ as a lifting of σ_{i^l}, we have $g_{i^l}^{-1} \cdot n_k \cdot g_{i^l} = n_{i^{-l}\cdot k \bmod p^n}$. and further*

$$\prod_{j=1}^{p^{n-1}(p-1)} \chi_n(\varphi_n(\sigma_{i^{d+j}}^{-1})n_k) = 1$$

.

Proof.

$$g_{i^l}^{-1} \cdot n_k \cdot g_{i^l} : \sqrt[p^n]{m} \overset{g_{i^l}}{\longmapsto} \sqrt[p^n]{m} \overset{n_k}{\longmapsto} \xi_{p^n}^k \cdot \sqrt[p^n]{m} \overset{g_{i^l}^{-1}}{\longmapsto} \xi_{p^n}^{i^{-l}k} \cdot \sqrt[p^n]{m}$$

hence $g_{i^l}^{-1} \cdot n_k \cdot g_{i^l} = n_{i^{-l} \cdot k \bmod p^n}$. Therefore

$$\begin{aligned}
\prod_{j=1}^{p^{n-1}(p-1)} \chi_n(\varphi_n(\sigma_{i^{d+j}}^{-1}) n_k) &= \chi_n \left(\prod_{j=1}^{p^{n-1}(p-1)} g_{i^l}^{-1} \cdot n_k \cdot g_{i^l} \right) \\
&= \chi_n \left(\prod_{j=1}^{p^{n-1}(p-1)} n_{i^{-l} \cdot k \bmod p^n} \right) \\
&= \chi_n \left(n_{\sum_{r \bmod p^n}^{(r,p)=1} r \cdot k} \right) \\
&= \chi_n(n_0) \\
&= 1
\end{aligned}$$

□

Theorem 3.2.1. *Suppose the triple (E, p, m) satisfies the assumptions made in Section 1.1. We have*

$$w(E, \rho_{\chi_n}) = w(E, \rho_K) \cdot \prod_{q_i \neq p \in S_{multi}} \left(\frac{q_i}{p} \right) \cdot s_p^{(1 - dim \rho_{\chi_n}^{I_p})} \tag{3.10}$$

for $n \geq 1$. Moreover, if we assume further that $p \parallel m^{p-1} - 1$ if $(p, m) = 1$, then

$$w(E, \rho_{\chi_n}) = w(E, \rho_K) \cdot \prod_{q_i \neq p \in S_{multi}} \left(\frac{q_i}{p} \right) \cdot s_p \tag{3.11}$$

for $n \geq 1$.

Proof. Applying the formula of Theorem 3.1.2, by Proposition 3.2.1 and Propo-

sition 3.2.2, we have

$$\begin{aligned}
\frac{w(E,\rho_{\chi_n})}{w(E,\rho_K)} &= \frac{w(E)^{dim\rho_{\chi n}}}{w(E)^{dim\rho_K}} \cdot \frac{(-1)^{dim\rho^-_{\chi n}}}{(-1)^{dim\rho^-_K}} \cdot \prod_{q\in S_{multi}} \frac{s_q^{dim\rho_{\chi n}-dim\rho^{I_q}_{\chi n}}}{s_q^{dim\rho_K-dim\rho_K^{I_q}}} \cdot \frac{det(\Phi_q|\rho^{I_q}_{\chi_n})}{det(\Phi_q|\rho_K^{I_q})} \cdot \prod_{q\in S_{add}} \left(\frac{det(\Phi_q|\rho_{\chi_n})}{det(\Phi_q|\rho_K)}\right)^{N_q(E)} \\
&= \prod_{q\neq p\in S_{multi}} \frac{det(\Phi_q|\rho^{I_q}_{\chi_n})}{det(\Phi_q|\rho_K)} \cdot \frac{s_p^{dim\rho^{I_p}_{\chi n}}}{s_p} \cdot \frac{1}{det(\Phi_p|\rho_K^{I_p})} \cdot \prod_{q\in S_{add}} \left(\frac{det(\Phi_q|\rho_{\chi_n})}{det(\Phi_q|\rho_K)}\right)^{N_q(E)} \\
&= \prod_{q_i\neq p\in S_{multi}} \frac{1}{det(\Phi_{q_i}|\rho_K)} \cdot \prod_{q\nmid mp\in S_{multi}} \frac{det(\Phi_q|\rho_{\chi_n})}{det(\Phi_q|\rho_K)} \cdot \frac{s_p^{(dim\rho^{I_p}_{\chi n}-1)}}{det(\Phi_p|\rho_K^{I_p})} \cdot \prod_{q\in S_{add}} \left(\frac{det(\Phi_q|\rho_{\chi_n})}{det(\Phi_q|\rho_K)}\right)^{N_q(E)} \\
&= \prod_{q_i\neq p\in S_{multi}} \left(\frac{q_i}{p}\right) \cdot \prod_{q\nmid mp\in S_{multi}} \frac{\left(\frac{q}{p}\right)}{\left(\frac{q}{p}\right)} \cdot s_p^{(dim\rho^{I_p}_{\chi n}-1)} \cdot \prod_{q\in S_{add}} \left(\frac{\left(\frac{q}{p}\right)}{\left(\frac{q}{p}\right)}\right)^{N_q(E)} \\
&= \prod_{q_i\neq p\in S_{multi}} \left(\frac{q_i}{p}\right) \cdot s_p^{(1-dim\rho^{I_p}_{\chi n})}.
\end{aligned}$$

□

3.3 Parity Conjecture

In this section, we continue from the previous section in assuming that the triple (E, p, m) satisfies the assumption in Section 1.1.

Lemma 3.3.1. *Let p be an odd prime and $K \overset{def}{=} \mathbb{Q}(\mu_p)$, for any rational prime $q \neq p$, we have*

$$(-1)^{\#S_q(K)} = \left(\frac{q}{p}\right)$$

where $S_q(K)$ is the set of primes of K above q.

Proof. Since $K/\mathbb{Q}$ is a cyclic extension of even order, namely $p-1$, there is a unique quadratic intermediate extension $R = \mathbb{Q}(\sqrt{p^*})$, where $p^* = \pm p$ s.t.

$p^* \equiv 1 \bmod 4$.

$$
\begin{aligned}
& q \neq p \text{ splits into even many primes over } K/\mathbb{Q} \\
\Leftrightarrow\ & \text{The decomposition subgroup of } q \text{ is of even index in } Gal(K/\mathbb{Q}) \\
\Leftrightarrow\ & \text{The decomposition subgroup of } q \text{ is a subgroup of } Gal(K/R) \\
\Leftrightarrow\ & q \text{ splits in } R \\
\Leftrightarrow\ & \left(\frac{p^*}{q}\right) = 1
\end{aligned}
$$

hence the lemma follows since $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$ by Quadratic Reciprocity Law.

□

Proposition 3.3.1. *Suppose the triple (E, p, m) satisfies the assumptions made in Section 1.1. Write $K_\infty \overset{def}{=} \mathbb{Q}(\mu_{p^\infty})$, then we have*

$$(-1)^{\#\{S_{ram}(K_\infty)\cap S_s(K_\infty) - S_p(K_\infty)\}} = \prod_{q_i \neq p \in S_{multi}} \left(\frac{q_i}{p}\right). \tag{3.12}$$

where the sets $S_{ram}(K_\infty)$, $S_s(K_\infty)$ and $S_p(K_\infty)$ are as defined in the paragraph preceding Proposition 2.3.1, in the case $L^{cyc} = K_\infty$.

Proof. Since K_∞/K is a pro-p extension with $p \geq 5$ an odd prime, the reduction type is invariant over this extension and there are only odd many primes of K_∞ above each prime of K. Hence

$$(-1)^{\#\{S_{ram}(K_\infty)\cap S_s(K_\infty) - S_p(K_\infty)\}} = (-1)^{\#\{S_{ram}(K)\cap S_s(K) - S_p(K)\}}$$

By assumption (E, p, m), none of the prime divisors q_i of m is of additive reduction type for E, hence any $\mathfrak{q}_i \in S_{ram}(K) \cap S_s(K) - S_p(K)$ is lying above some rational prime $q_i \mid m$, $q_i \neq p$, at where $E/\mathbb{Q}$ has split or non-split multiplicative reduction. Therefore we have plainly the partition

$$S_{ram}(K) \cap S_s(K) - S_p(K) = \coprod_{q_i \neq p \in S_{multi}} S_{q_i}(K) \cap S_s(K)$$

For each $q_i (\neq p) \mid m$, $q_i \in S_{multi}$,

- If E has split multiplicative reduction at q_i,
  then E has split multiplicative reduction at all primes $\mathfrak{q}_i$'s of K above q_i

and hence $S_{q_i}(K) \subset S_s(K)$ and by the lemma above,

$$(-1)^{\#S_{q_i}(K)\cap S_s(K)} = (-1)^{\#S_{q_i}(K)} = \left(\frac{q_i}{p}\right)$$

- If E has non-split multiplicative reduction at q_i, then

  - if q_i is inert over $R = \mathbb{Q}(\sqrt{p^*})$, we have

    $$\left(\frac{p^*}{q_i}\right) = \left(\frac{q_i}{p}\right) = -1$$

    On the other hand, E attains split multiplicative reduction at the prime of R above q_i and hence $S_{q_i}(K) \subset S_s(K)$. Thus,

    $$(-1)^{\#S_{q_i}(K)\cap S_s(K)} = (-1)^{\#S_{q_i}(K)} = \left(\frac{q_i}{p}\right) = -1$$

  - if q_i splits over $R = \mathbb{Q}(\sqrt{p^*})$,
    we have
    $$\left(\frac{p^*}{q_i}\right) = \left(\frac{q_i}{p}\right) = 1$$
    and also, $\#S_{q_i}(K)$ is even and so is $S_{q_i}(K) \cap S_s(K)$ and hence

    $$(-1)^{\#S_{q_i}(K)\cap S_s(K)} = 1$$

We see the proposition follows by multiplying through all such q_i's.

□

Theorem 3.3.1. *Under the assumptions of the triple (E, p, m) made in Section 1.1, assume further that $p \parallel m^{p-1} - 1$ if E has split multiplicative reduction at p and $(p, m) = 1$. Assuming the validity of Conjecture 2.2.1, we have*

$$(-1)^{rank_{\Lambda(H_K)} Y_p(E/F_\infty)} = w(E, \rho_{\chi_n})$$

for all ρ_{χ_n} as defined in Section 3.2.

We shall apply two theorems below to $k = K = \mathbb{Q}(\mu_p)$ to finally filling up the gaps to the proof of Theorem 3.3.1.

Theorem 3.3.2. *(Greenberg-Guo)[9, Proposition 3.10][10, Section 5]*
Assume that E is an elliptic curve defined over a number field k and that $Sel_p(E/k^{cyc})$ is $\Lambda(\Gamma_k)$-cotorsion, where p is any odd prime, then

$$\lambda_{\Lambda(\Gamma_k)}\big(X_p(E/k^{cyc})\big) \equiv corank_{\mathbb{Z}_p} Sel_p(E/k) \bmod 2 \tag{3.13}$$

Proof. Let us use the notations introduced in Theorem 2.1.1. For brevity, we denote $\lambda \overset{\text{def}}{=} \lambda_{\Lambda(\Gamma_k)}\big(X_p(E/k^{cyc})\big)$; for each $n \geq 0$, we denote $S_n \overset{\text{def}}{=} Sel_p(E/k_n)$, its maximal divisible subgroup by $D_n \overset{\text{def}}{=} Sel_p(E/k_n)_{div}$ and $Q_n \overset{\text{def}}{=} S_n/D_n$, which is a finite abelian p-group. Since Cassels-Tate pairing on Q_n is non-degenerate and skew-symmetric, we can write $Q_n \cong M_n \oplus M_n$ for M_n a maximal isotropic subgroup of Q_n.
Since the restriction map

$$H^1(k^n, E_{p^\infty}) \xrightarrow{r_{k_n}} H^1(k^{cyc}, E_{p^\infty})$$

has kernel $ker(r_{k_n}) = H^1(\Gamma_n, E(k^{cyc})_{p^\infty}) \cong E(k^{cyc})_{p^\infty}/(\gamma^{p^n} - 1)E(k^{cyc})_{p^\infty}$ which is clearly of finite order, bounded by the order of $E(k^{cyc})_{p^\infty}$ which is finite by Ribet's Theorem. Therefore we have an upper bound $corank_{\mathbb{Z}_p} S_n \leq \lambda$ for all $n \geq 1$. Let $\lambda' \overset{\text{def}}{=} \max_{n\geq 0}\{corank_{\mathbb{Z}_p} S_n\}$, then there exists some integer $n_0 \geq 0$ such that for all $n \geq n_0$, we have $corank_{\mathbb{Z}_p} S_n = \lambda'$. Let $Q_\infty = S_\infty/D_\infty = \varinjlim Q_n$, where $S_\infty \overset{\text{def}}{=} Sel_p(E/k^{cyc}) = \varinjlim S_n$ and $D_\infty \overset{\text{def}}{=} \varinjlim D_n$. We have $D_\infty \cong \big(\mathbb{Q}_p/\mathbb{Z}_p\big)^{\lambda'}$ and hence

$$corank_{\mathbb{Z}_p} Q_\infty = \lambda - \lambda'.$$

We shall go on and prove that $corank_{\mathbb{Z}_p} Q_\infty$ is even and λ' has the same parity as $corank_{\mathbb{Z}_p} S_0$.
For any finite abelian p-group Q, write uniquely $Q \cong \mathbb{Z}/p^{a^{(1)}}\mathbb{Z} \oplus \mathbb{Z}/p^{a^{(2)}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{a^{(l)}}\mathbb{Z}$ with $a^{(1)} \geq a^{(2)} \geq \cdots \geq a^{(l)} \geq 0$. We call this sequence $(a^{(1)}, a^{(2)}, \cdots, a^{(l)})$ the index of Q and the largest r such that $a^{(r)} \neq 0$ the number of generators of Q. Since Q_∞ has finite $\mathbb{Z}_p$-corank, all the finite subgroup $i_n(Q_n)$ has bounded number of generators, say l. Using the canonical map $Q_n \xrightarrow{i_n} Q_\infty$, we have $i_n(Q_n) \subset i_{n+1}(Q_{n+1})$ and hence for each $1 \leq i \leq l$, $b_n^{(i)}$ is non-decreasing when n increases and hence either converges to infinity or to a finite bound, where the sequence $(b_n^{(1)}, b_n^{(2)}, \cdots, b_n^{(l)})$ denotes the index of $i_n(Q_n)$. The $\mathbb{Z}_p$-

corank of Q_∞ is just the number of

$$\#\{1 \leq i \leq l \mid b_n^{(i)} \to \infty\}.$$

For $n \geq n_0$, since $D_n \longrightarrow D_\infty$ is surjective, we can lift each element in the kernel of $Q_n \longrightarrow Q_\infty$ to an element in the kernel of $S_n \longrightarrow S_\infty$, hence we have

$$\#\left(ker(Q_n \xrightarrow{i_n} Q_\infty)\right) \leq \#\left(ker(S_n \longrightarrow S_\infty)\right) \leq \#\left(ker(r_{k_n})\right)$$

which is finite, bounded independent on $n \geq n_0$ by $|E(k^{cyc})_{p^\infty}|$, and therefore $ker(i_n)$, and hence Q_n have bounded numbers of generators. Without loss of generality, by increasing the value l above, let us assume l is a bound for the number of generators of Q_n for all $n \geq n_0$. Suppose p^N is an exponent of $ker(i_n)$ for all $n \geq n_0$ and N is an integer, and denote by $(a_n^{(1)}, a_n^{(2)}, \cdots, a_n^{(l)})$ and $(c_n^{(1)}, c_n^{(2)}, \cdots, c_n^{(l)})$ the index of Q_n and $Q_n/(Q_n)_{p^N}$ respectively, then obviously, $c_n^{(i)} = max\{a_n^{(i)} - N, 0\}$ for all $1 \leq i \leq l$. We have surjections $Q_n \longrightarrow i_n(Q_n)$ and $i_n(Q_n) \longrightarrow Q_n/(Q_n)_{p^N}$ since $ker(i_n) \subseteq (Q_n)_{p^N}$ for $n \geq n_0$, hence we have

$$a_n^{(i)} \geq b_n^{(i)} \geq c_n^{(i)} \geq a_n^{(i)} - N$$

for all $1 \leq i \leq l$ and $n \geq n_0$. This implies the equality

$$\#\{1 \leq i \leq l \mid a_n^{(i)} \to \infty\} = \#\{1 \leq i \leq l \mid b_n^{(i)} \to \infty\},$$

since we have $0 \leq a_n^{(i)} - b_n^{(i)} \leq N$ for all the i's and n's above. Thus, we showed that $corank_{\mathbb{Z}_p} Q_\infty$ is even since $a_n^{(1)} = a_n^{(2)} \geq a_n^{(3)} = a_n^{(4)} \geq \cdots \geq a_n^{(2j-1)} = a_n^{(2j)} = \cdots \geq a_n^{(l)}$ by the decomposition $Q_n \cong M_n \oplus M_n$ above.
On the other hand, the restriction map $S_0 \longrightarrow S_n^{Gal(k_n/k_0)}$ has finite kernel and cokernel and hence so is the kernel and cokernel of $D_0 \longrightarrow D_n^{Gal(k_n/k_0)}$. Since the degree of any non-trivial irreducible representation over $\mathbb{Q}_p$ of $Gal(k_n/k_0) \cong \mathbb{Z}/p^n\mathbb{Z}$ is divisible by $p-1$, we have

$$corank_{\mathbb{Z}_p} S_0 = corank_{\mathbb{Z}_p} D_0 \overset{mod(p-1)}{\equiv} corank_{\mathbb{Z}_p} D_n = corank_{\mathbb{Z}_p} S_n$$

since p is odd, this implies that the $\mathbb{Z}_p$-corank of $Sel_p(E/k)$ has the same parity as that of $Sel_p(E/k_n)$ which the latter equals λ' when $n \geq n_0$.

□

Theorem 3.3.3 (T,V. Dokchitser)**.** *[7, Theorem 1.2]*
Let E be an elliptic curve defined over $\mathbb{Q}$. For every abelian extension $k/\mathbb{Q}$ and every prime p,

$$w(E/k) = (-1)^{corank_{\mathbb{Z}_p} Sel_p(E/k)} \tag{3.14}$$

Proof. See the proof of [7, Theorem 2.8].

□

Proof of Theorem 3.3.1

Proof. From Proposition 2.5.2, eq(2.16) for $L = K$, we have

$$(-1)^{rank_{\Lambda(H_K)} Y_p(E/F_\infty)} = (-1)^{\lambda_{\Lambda(\Gamma_K)}(X_p(E/K_\infty))} \cdot (-1)^{\sum_{u\in S(K_\infty)} corank_{\mathbb{Z}_p} ker(h_u)}$$

The former term of the right hand side, by the two theorems eq(3.13) and eq(3.14) above, for $k = K$, is

$$(-1)^{\lambda_{\Lambda(\Gamma_K)}(X_p(E/K_\infty))} = w(E/K) \tag{3.15}$$

The latter term of the right hand side, by Theorem 2.4.1 eq(2.7), Proposition 2.3.1 and Proposition 3.3.1 eq(3.12), is

$$\begin{aligned}(-1)^{\sum_{u\in S(K_\infty)} corank_{\mathbb{Z}_p} ker(h_u)} &= s_p \cdot (-1)^{\#\{S_{ram}(K_\infty)\cap S_s(K_\infty) - S_p(K_\infty)\}} \\ &= s_p \cdot \prod_{q_i \neq p \in S_{multi}} \left(\frac{q_i}{p}\right).\end{aligned} \tag{3.16}$$

Lastly, the product of eq(3.15) and eq(3.16) is given in Theorem 3.2.1 eq(3.11) and hence proved

$$(-1)^{rank_{\Lambda(H_K)} Y_p(E/F_\infty)} = w(E, \rho_{\chi_n}).$$

□

3.4 More on the representations ρ_{χ_n}

In [26, Proposition 25], Serre provides a recipe to constructively list out all of the isomorphic classes of representations of any finite group of the form

$$G = N \rtimes H$$

with N an abelian normal subgroup of G and H a subgroup of G. The arguments are subject to representations over $\mathbb{C}$ but in fact, they hold in general over any algebraically closed field K, of characteristic 0, for instance $\bar{\mathbb{Q}}_p$. I shall rephrase the recipe here.

Firstly, any irreducible representation of N is one dimensional since N is abelian. Hence, we can identify them as elements in $Hom(N, \bar{\mathbb{Q}}_p^\times)$. Since N is normal in G, there's a G-action on it, namely

$$(g\chi)(n) = \chi(g^{-1}ng) \tag{3.17}$$

for $g \in G, n \in N, \chi \in Hom(N, \bar{\mathbb{Q}}_p^\times)$.

Choose a system of representatives for the H-orbits in $Hom(N, \bar{\mathbb{Q}}_p^\times)$, denoted by $\{\chi_\alpha\}$. Let $H_\alpha \leq H$ denote the stabilizer subgroup of χ_α, then we can extend χ_α to a representation $\widetilde{\chi_\alpha}$ of $G_\alpha \overset{\text{def}}{=} N \rtimes H_\alpha$ by

$$\widetilde{\chi_\alpha}(nh_\alpha) = \chi_\alpha(n)$$

for $n \in N$, $h_\alpha \in H_\alpha$. Indeed, plainly we have

$$\begin{aligned}
\widetilde{\chi_\alpha}(nh_\alpha n'h'_\alpha) &= \widetilde{\chi_\alpha}(nh_\alpha n' {h_\alpha}^{-1} h_\alpha h'_\alpha) \\
&= \chi_\alpha(nh_\alpha n' {h_\alpha}^{-1}) \\
&= \chi_\alpha(n)\chi_\alpha(h_\alpha n' {h_\alpha}^{-1}) \\
&= \widetilde{\chi_\alpha}(nh_\alpha)({h_\alpha}^{-1}\chi_\alpha)(n') \\
&= \widetilde{\chi_\alpha}(nh_\alpha)\widetilde{\chi_\alpha}(n'h'_\alpha)
\end{aligned}$$

On the other hand, composing the canonical projection $G_\alpha \to H_\alpha$ with any irreducible representation η_α of H_α, we obtain another irreducible representation $\widetilde{\eta_\alpha}$ of G_α. Eventually, we obtain a representation $\rho_{(\chi_\alpha, \eta_\alpha)}$ of G by induction:

$$\rho_{(\chi_\alpha, \eta_\alpha)} \overset{\text{def}}{=} Ind_{G_\alpha}^G(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})$$

Lemma 3.4.1 (J-P. Serre). *[26, Proposition 25]*
$\rho_{(\chi_\alpha,\eta_\alpha)}$ runs over all isomorphic classes of irreducible $\bar{\mathbb{Q}}_p$-representations of G when χ_α runs over the representatives of the H-orbits of $Hom(N,\bar{\mathbb{Q}}_p^\times)$ and η_α runs over all the isomorphic classes of irreducible representations of the stabilizer subgroup H_α.

Proof. Since both $\widetilde{\chi_\alpha}$ and $\widetilde{\eta_\alpha}$ are irreducible, their tensor product $\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}$ is irreducible. Using Frobenius reciprocity, we have

$$< Ind_{G_\alpha}^G(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}), Ind_{G_\alpha}^G(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}) >_G = < \widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}, Res_{G_\alpha} Ind_{G_\alpha}^G(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}) >_{G_\alpha}$$

where $< V, W >_G$ denotes the inner product of the characters of the representations V and W of G. Let $T_\alpha = \{t_i \in G\}$ be a left transversal for G_α, G has a left action on T_α, induced by left multiplication. This G-action inscribes the induced module

$$Ind_{G_\alpha}^G(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}) \cong \oplus_{t_i\in T_\alpha} t_i(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}). \tag{3.18}$$

The direct summands $t_i(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha})$ on the right are not G-stable, but permuted under the left action of G. Restricted to the action by G_α, we may rewrite the above decomposition courser with regard to their G_α-orbits, we have

$$Res_{G_\alpha} Ind_{G_\alpha}^G(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}) \cong \bigoplus_{G_\alpha t_i} (\oplus_{t\in G_\alpha t_i} t(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha})).$$

where $G_\alpha t_i \subset T_\alpha$ runs over all G_α-orbits in T_α. Each of the summand $\oplus_{t\in G_\alpha t_i} t(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha})$ is now G_α-stable and hence this is a decomposition of representations of G_α. For each $t_i \in T_\alpha$, it is easily seen that its stabilizer subgroup in G_α is $G_\alpha \cap t_i G_\alpha t_i^{-1}$. Hence it is obvious that $\oplus_{t\in G_\alpha t_i} t(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha})$ is an induced representation from the subgroup $G_\alpha \cap t_i G_\alpha t_i^{-1}$. More precisely,

$$\begin{aligned}\bigoplus_{t\in G_\alpha t_i} t(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}) &= \bigoplus_{s\in S_{\alpha,t_i}} s(t_i(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha})) \\ &= Ind_{G_\alpha\cap t_i G_\alpha t_i^{-1}}^{G_\alpha}(t_i(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}))\end{aligned}$$

where S_{α,t_i} is a left transversal of $G_\alpha \cap t_i G_\alpha t_i^{-1}$ in G_α. Applying Frobenius reciprocity again, we obtain from the above that

$$< Ind_{G_\alpha}^G(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}), Ind_{G_\alpha}^G(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}) >_G = \sum_{G_\alpha t_i} < Res_{G_\alpha\cap t_i G_\alpha t_i^{-1}}(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}), t_i(\widetilde{\chi_\alpha}\otimes\widetilde{\eta_\alpha}) >_{G_\alpha\cap t_i G_\alpha t_i^{-1}}$$

The $G_\alpha \cap t_i G_\alpha {t_i}^{-1}$-action on $t_i(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})$ is by the following:
For $g_\alpha \in G_\alpha$ such that ${t_i}^{-1} g_\alpha t_i \in G_\alpha$, $g_\alpha = t_i {t_i}^{-1} g_\alpha t_i {t_i}^{-1}$ maps $t_i(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})$ to $t_i({t_i}^{-1} g_\alpha t_i \widetilde{\chi_\alpha} \otimes {t_i}^{-1} g_\alpha t_i \widetilde{\eta_\alpha})$. Hence if we let $(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})_{t_i}$ denote the vector space $(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})$, with g_α above sending $(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})$ to $({t_i}^{-1} g_\alpha t_i \widetilde{\chi_\alpha} \otimes {t_i}^{-1} g_\alpha t_i \widetilde{\eta_\alpha})$, then $(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})_{t_i}$ is equipped as a $G_\alpha \cap t_i G_\alpha {t_i}^{-1}$-module which is $G_\alpha \cap t_i G_\alpha {t_i}^{-1}$-isomorphic to $t_i(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})$, given by left multiplication by t_i .
Let t_0 be the unique element in T_α that lies in G_α. Clearly, $t_0 G_\alpha {t_0}^{-1} = G_\alpha$ and so the summand with regard to the orbit $G_\alpha t_0$ is

$$< Res_{G_\alpha \cap t_0 G_\alpha {t_0}^{-1}}(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha}), t_0(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha}) >_{G_\alpha \cap t_0 G_\alpha {t_0}^{-1}} =< \widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha}, (\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})_{t_0} >_{G_\alpha}$$
$$=< \widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha}, \widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha} >_{G_\alpha} = 1.$$

The last equality holds because $\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha}$ is an irreducible representation of G_α, and the second equality holds because $(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})_{t_0}$ is G_α-isomorphic to $(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})$ since they share the same character.
For the summand with regard to other orbits, say $G_\alpha t_i$ with $t_i \neq t_0$, when restricted further to $N \leq G_\alpha \cap t_i G_\alpha {t_i}^{-1}$,

$$Res_N(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha}) \cong {\chi_\alpha}^{\oplus deg \eta_\alpha}$$

and since N is normal in G, ${t_i}^{-1} N t_i = N$

$$Res_N(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})_{t_i} \cong {t_i \chi_\alpha}^{\oplus deg \eta_\alpha}.$$

Since G_α is the stabilizer subgroup of χ_α in G, $t_i \chi_\alpha \neq \chi_\alpha$ for all $t_i \neq t_0$. Therefore, their restrictions to N are disjoint implying they are disjoint, and

$$< Res_{G_\alpha \cap t_i G_\alpha {t_i}^{-1}}(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha}), t_i(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha}) >_{G_\alpha \cap t_i G_\alpha {t_i}^{-1}} = 0$$

for $t_i \leq t_0$. As a result, $< \rho_{(\chi_\alpha, \eta_\alpha)}, \rho_{(\chi_\alpha, \eta_\alpha)} >_G = 1$, hence $\rho_{(\chi_\alpha, \eta_\alpha)}$ is irreducible.
Look at the restriction of $Ind_{G_\alpha}^G(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha}) \cong \oplus_{t_i \in T_\alpha} t_i(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})$ to N, each of the summands $t_i(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})$ is isomorphic to $(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})_{t_i}$ as N-modules, since $N \lhd G$. Hence, $Res_N \rho_{(\chi_\alpha, \eta_\alpha)} \cong \oplus_{t_i \in T_\alpha} (\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})_{t_i} \cong (\oplus_{t_i \in T_\alpha} t_i \chi_\alpha)^{\oplus deg \eta_\alpha}$ which only involves the G-orbit of χ_α in $Hom(N, \bar{\mathbb{Q}}_p^\times)$ and so it decides the representative χ_α. Once this is decided, the subspace $(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})_{t_0}$ is identify as the N-submodule of $\rho_{(\chi_\alpha, \eta_\alpha)}$ which N acts via the character χ_α. As obtained earlier, $(\widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha})_{t_0} \cong \widetilde{\chi_\alpha} \otimes \widetilde{\eta_\alpha}$ as $G_\alpha = N H_\alpha$-modules. Restricted to the H_α, this is simply η_α and hence distinct

pair of $(\chi_\alpha, \eta_\alpha)$ give non-isomorphic $\rho_{(\chi_\alpha,\eta_\alpha)}$.
Lastly, to prove that these $\{\rho_{(\chi_\alpha,\eta_\alpha)}\}$ give a complete set of irreducible $\bar{\mathbb{Q}}_p$-representations of G up to isomorphism, it is sufficient to check if the sum of the squares of the degrees of these representations equals to $|G|$. Easily, we have

$$\begin{aligned}
\sum_\alpha \sum_{\eta_\alpha} (deg(\rho_{(\chi_\alpha,\eta_\alpha)}))^2 &= \sum_\alpha \sum_{\eta_\alpha} (|G/G_\alpha| deg\eta_\alpha)^2 \\
&= \sum_\alpha |G/G_\alpha|^2 \sum_{\eta_\alpha} (deg\eta_\alpha)^2 \\
&= \sum_\alpha |H/H_\alpha|^2 |H_\alpha| \\
&= |H| \sum_\alpha |H/H_\alpha| \\
&= |H||Hom(N, \bar{\mathbb{Q}}_p^\times)| \\
&= |H||N| \\
&= |G|
\end{aligned}$$

□

Now I would like to apply this argument to give a collective description of the representations ρ_{χ_n} of the Galois group $G_n = Gal(F_n/\mathbb{Q})$, defined in Section 3.2.

Allowing the abuse of notation, we denote again by ρ_{χ_n} the composition of itself to the canonical projection $G = Gal(F_\infty/\mathbb{Q}) \longrightarrow G_n = Gal(F_n/\mathbb{Q})$.

Proposition 3.4.1. *The irreducible self-dual Artin representations of G of degree greater than 1 are all orthogonal. Namely, up to G-isomorphism, these representations are precisely given by ρ_{χ_n} where χ_n is any character of exact order p^n of the Galois group $N_n = Gal(F_n/K_n)$, with n runs over all positive integers.*

Lemma 3.4.2. *Up to G_n-isomorphism, ρ_{χ_n} is the unique $\bar{\mathbb{Q}}_p$-representation of G_n which does not factor through $F_{n-1}(\mu_{p^n})$.*

Proof of lemma. Identifying the galois groups $Gal(F_n/L_n)$ and $Gal(K_n/\mathbb{Q})$ by their actions on μ_{p^n} and still refer the former by H_n. From the argument above, more precisely eq(3.17), we know that $G_n = N_nH_n$ acts on $Hom(N_n, \bar{\mathbb{Q}}_p^\times)$ from the left, where N_n acts trivially and so most of the time, we just focus on the H_n-action.

For $0 \leq k \leq n$,

$$Orb_k \overset{\text{def}}{=} \{\text{characters of exact order } p^{n-k}\} \subseteq Hom(N_n, \bar{\mathbb{Q}}_p^\times)$$

forms a H_n-orbit. Since H_n is a finite cyclic group of order $p^{n-1}(p-1)$, all characters in Orb_k share the same stabilizer subgroup $H_n^{p^{n-k-1}(p-1)}$, when $k < n$; whereas $Orb_n = \{trivial\, character\}$ has stabilizer subgroup H_n

For $k = 0$, from the recipe in the lemma above, the stabilizer subgroup is trivial $1 \leq H_n$, and this leaves no other choice for the corresponding η_0 but $\eta_0 = id$, the trivial representation of degree 1. Picking any $\chi_n \in Orb_0$, we have

$$\rho_{\chi_n} = \rho_{(\chi_n, \eta_0)}.$$

This obviously does not factor through $F_{n-1}(\mu_{p^n})$. In fact, not even the N_n-submodule χ_n of ρ_{χ_n} factors through $F_{n-1}(\mu_{p^n})$, because χ_n is of exact order p^n hence the it cannot be trivial over subgroup $N_n^{p^{n-1}}$.

For $0 < k < n$, we shall see that for any irreducible $\bar{\mathbb{Q}}_p$-representation η_k of the stabilizer subgroup $H_n^{p^{n-k-1}(p-1)} \leq H_n$ and any $\chi \in Orb_k$, the corresponding induced representation $\rho_{(\chi,\eta_k)}$ is factored through $F_{n-1}(\mu_{p^n})$. To see this, we can choose $T_k = \{t_i \in H_n\}$ be a left transversal for $H_n^{p^{n-k-1}(p-1)}$. This could serve too as a left transversal for subgroup $N_nH_n^{p^{n-k-1}(p-1)} \leq N_nH_n$. In view of the decomposition (3.18), each of the direct summand $t_i(\widetilde{\chi} \otimes \widetilde{\eta_k})$ of $\rho_{(\chi,\eta_k)}$ is N_n-invariant and hence a subspace of representation of N_n. As seen before, the representation $t_i(\widetilde{\chi} \otimes \widetilde{\eta_k})$ is isomorphic to $(\widetilde{\chi} \otimes \widetilde{\eta_k})_{t_i}$. Since N_n acts trivially on $\widetilde{\eta_k}$, this direct summand, when viewed as a representation of N_n, is isomorphic to $(t_i\chi)^{\oplus deg\, \eta_k}$ by the notation in (3.17). With $t_i\chi \in Orb_k$, $(t_i\chi)(N_n^{p^{n-1}}) = (t_i\chi)^{p^{n-1}}(N_n) = 1$ since $t_i\chi$ has exact order p^{n-k} dividing p^{n-1}

Lastly for $k = n$, $\chi = id \in Orb_n$. The corresponding induced representation $\rho_{(\chi,\eta_n)}$ is just $\widetilde{\eta_n}$ which is trivial when restricted to the whole N_n, for any irreducible representation η_n of H_n. □

Lemma 3.4.3. *Let $char_\phi$ denote the character of a representation ϕ of subgroup*

$H \leq G$, then the character of $Ind_H^G \phi$ is given by

$$char_{Ind_H^G \phi}(g) = \sum_{t \in T}^{t^{-1}gt \in H} char_\phi(t^{-1}gt)$$

for any $g \in G$ and any given set T of coset representatives of H in G.

Lemma 3.4.4. *[26, Proposition 39]*
Let $char_\rho$ denote the character of an irreducible representation ρ of a finite group G, then the value

$$\frac{1}{|G|} \sum_{g \in G} char_\rho(g^2) = \begin{cases} 0, & \text{if } \rho \text{ is not self-dual,} \\ 1, & \text{if } \rho \text{ is self-dual and orthogonal,} \\ -1, & \text{if } \rho \text{ is self-dual and symplectic.} \end{cases} \tag{3.19}$$

Proof. Proof omitted. □

Proof of Proposition 3.4.1. Since F_∞ is the direct limit of F_n, any Artin representation of G must factor through G_n for certain $n \geq 1$. Therefore, it is sufficient to search among the irreducible representations of G_n for a fixed $n \geq 1$.
As seen in the proof of Lemma 3.4.2, for k=n, $\rho_{(id,\eta_n)} = \widetilde{\eta}_n$ is of dimension 1.
For $0 \leq k < n$, I want to compute the summation

$$\frac{1}{|G_n|} \sum_{g = n_l h_{i'} \in N_n H_n} char_{\rho_{(\theta_k, \eta_k)}}(g^2) \tag{3.20}$$

As before, $n_l \in N_n$ denotes the element which sends $\sqrt[p^n]{m}$ to $\xi_{p^n}^l \sqrt[p^n]{m}$ and leaves ξ_{p^n} unchanged; $h_{i'} \in H_n$ denotes the element which sends ξ_{p^n} to $\xi_{p^n}^{i'}$ and leaves $\sqrt[p^n]{m}$ unchanged, where $i \in \mathbb{Z}$ is a chosen primitive root modulo p^α for all $\alpha \geq 1$.
By the formula in Lemma 3.4.3, we can rewrite the sum in (3.20) as

$$\frac{1}{p^{2n-1}(p-1)} \sum_{g = n_l h_{i'}} \sum_{t \in T_k}^{t^{-1}g^2 t \in N_n H_n^{p^{n-k-1}(p-1)}} \widetilde{\theta}_k(t^{-1}g^2 t) \widetilde{\eta}_k(t^{-1}g^2 t)$$

where $\theta_k \in Orb_k$, η_k is an irreducible representation of $H_n^{p^{n-k-1}(p-1)}$, T_k is a left transversal of $H_n^{p^{n-k-1}(p-1)}$ in H_n, which can hence be treated as a left transversal of $N_nH_n^{p^{n-k-1}(p-1)}$ in N_nH_n. Since $N_nH_n^{p^{n-k-1}(p-1)}$ is normal in N_nH_n,

$$\begin{aligned}\{t \in T_k \mid t^{-1}(n_l h_{i^{l'}})^2 t \in N_n H_n^{p^{n-k-1}(p-1)}\} &= \{t \in T_k \mid (n_l h_{i^{l'}})^2 \in N_n H_n^{p^{n-k-1}(p-1)}\} \\ &= \begin{cases} T_k & when\,(h_{i^{l'}})^2 \in H_n^{p^{n-k-1}(p-1)} \\ \emptyset & when\,(h_{i^{l'}})^2 \notin H_n^{p^{n-k-1}(p-1)} \end{cases}\end{aligned} \tag{3.21}$$

Simple computation gives $h_{i^{l'}} n_l h_{i^{l'}}^{-1} = n_{l \cdot i^{l'}}$. Hence, the summation above can be further rewritten as

$$\begin{aligned}&\frac{1}{p^{2n-1}(p-1)} \sum_{l' \in \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z}}^{p^{n-k-1}(p-1)|2l'} \sum_{t \in T_k} \sum_{l \in \mathbb{Z}/p^n\mathbb{Z}} t\theta_k(n_{l+l\cdot i^{l'}})\eta_k(h_{i^{2l'}}) \\ =&\frac{1}{p^{2n-1}(p-1)} \sum_{l' \in \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z}}^{p^{n-k-1}(p-1)|2l'} \eta_k(h_{i^{2l'}}) \sum_{\theta \in Orb_k} \sum_{l \in \mathbb{Z}/p^n\mathbb{Z}} \theta(n_{l(1+i^{l'})}) \\ =&\frac{1}{p^{2n-1}(p-1)} \sum_{l'} \eta_k(h_{i^{2l'}}) |Orb_k| |\mathbb{Z}/p^n\mathbb{Z}| \\ =&\frac{1}{p^k} \sum_{l'} \eta_k(h_{i^{2l'}})\end{aligned} \tag{3.22}$$

where the summation $\sum_{l'}$ runs over l' in the set

$$L_k \stackrel{\text{def}}{=} \{l'\, mod\, p^{n-1}(p-1) : p^{n-k} \mid 1 + i^{l'}\, and\, p^{n-k-1}(p-1) \mid 2l'\}.$$

Since

$$\begin{aligned} p^{n-k} \mid 1 + i^{l'} &\Leftrightarrow i^{l'} \equiv -1\, mod\, p^{n-k} \\ &\Leftrightarrow l' \equiv p^{n-k-1}(p-1)/2\, mod\, p^{n-k-1}(p-1) \\ &\Leftrightarrow l' \equiv p^{n-k-1}(p-1)/2 + b \cdot p^{n-k-1}(p-1)\, mod\, p^{n-1}(p-1) \\ &\Rightarrow 2l' \equiv (2b+1)p^{n-k-1}(p-1)\, mod\, p^{n-1}(p-1) \\ &\Rightarrow p^{n-k-1}(p-1) \mid 2l', \end{aligned} \tag{3.23}$$

where b runs over integers $0 \leq b \leq p^k - 1$, the set L_k can be rephrased by

$$L_k = \{l' \equiv p^{n-k-1}(p-1)/2 + b \cdot p^{n-k-1}(p-1) \, mod \, p^{n-1}(p-1) : 0 \leq b \leq p^k - 1\}.$$

Noticing that when l' runs over residues in L_k, $h_{i^{2l'}}$ runs over all the elements of the cyclic subgroup $H_n^{p^{n-k-1}(p-1)}$ of order p^k, the summation in the last line of (3.22) is hence equal to 1 when η_k is the trivial representation of degree 1; and equal to 0 otherwise.
In conclusion, the self-dual irreducible representations of G_n are $\rho_{\chi_{n-k},id}$, where χ_{n-k} is any character of N_n of exact order p^{n-k}, for all $0 \leq k < n$. These are all orthogonal in view of the Lemma 3.4.4.

□

I shall conclude this section with yet another proposition which will be needed in a proof in next chapter.

Proposition 3.4.2. *The fixed subspace* $\left(\rho_{\chi_k}\right)^{Gal(F_n/L_n)}$ *is one dimensional for* $n \geq k \geq 1$.

Proof. Since $Gal(F_n/L_n)$ is a cyclic group generated by σ_i as given in the proof of Proposition 3.2.2, it is clear that $\left(\rho_{\chi_k}\right)^{Gal(F_n/L_n)}$ is just the fixed subspace of ρ_{χ_k} by the generator σ_i. Recall again the notation σ_{i^l} from proof of the same theorem, $Gal(F_n/L_n) = \{\sigma_{i^l} \mid l \in \mathbb{Z}/(p^{n-1}(p-1))\mathbb{Z}\}$.
Let T_k denote a left transversal of $Gal(F_k/\mathbb{Q})$ for $Gal(F_k/K_k)$, we can actually pick a nice choice here with

$$T_k = Gal(F_k/L_k).$$

We can then write

$$\rho_{\chi_k} \cong \bigoplus_{\tau_j \in T_k} \tau_j(\chi_k).$$

When $k = n$, we have $T_k = \{\tau_j\} = \{\sigma_{i^l}\}$, so we can shuffle the order of $\{\tau_j\}$ of the decomposition above by $\{\sigma_{i^l}\}$ and denote by an $(p^{k-1}(p-1))$-tuple $\{a_l\}$ a general vector in the vector space underlying ρ_{χ_k}, with each a_l a general vector (and in this case a field element) of the underlying space $\sigma_{i^l}(\chi_k)$ (which is one-dimensional, hence in this case it is just $\bar{\mathbb{Q}}_p$). Notice that for each l modulo

$p^{k-1}(p-1)$,

$$\sigma_i \cdot \sigma_{i^l} = \sigma_{i^{l+1}},$$

this shows that the action of σ_i via the representation ρ_{χ_k} is taking

$$(a_1, a_2, a_3, \cdots, a_{p^{k-1}(p-1)-1}, a_{p^{k-1}(p-1)}) \mapsto (a_{p^{k-1}(p-1)}, a_1, a_2, \cdots a_{p^{k-1}(p-1)-2}, a_{p^{k-1}(p-1)-1}).$$

Therefore the fixed vector space consists of the diagonal tuples

$$(a, a, a, \cdots, a, a), \quad \forall a \in \bar{\mathbb{Q}}_p$$

hence $\left(\rho_{\chi_k}\right)^{Gal(F_k/L_k)} \equiv \bar{\mathbb{Q}}_p$.
When $n > k$, since the representation ρ_{χ_k} factors through $Gal(F_k/\mathbb{Q})$, the action of $\sigma_i \in Gal(F_n/L_n) < Gal(F_n/\mathbb{Q})$ via this representation is the corresponding action of its image in the canonical surjection

$$Gal(F_n/\mathbb{Q}) \longrightarrow Gal(F_k/\mathbb{Q}).$$

This shows that the image of σ_i can be determined by its Galois action on F_k, or more precisely, on $\sqrt[p^k]{m}$ and on any primitive p^k-th root of unity ξ_{p^k}, and in particular a particular choice $\xi_{p^n}^{p^{n-k}}$. Since σ_i fixes $\sqrt[p^n]{m}$, it must fix $\sqrt[p^k]{m} = (\sqrt[p^n]{m})^{p^{n-k}}$; and it takes ξ_{p^k} to $\xi_{p^k}^i$ with i modulo p^k. Since i is a primitive root modulo p^n, it is also a primitive root modulo p^k and hence the image of σ_i in $Gal(F_k/\mathbb{Q})$ is a generator of the cyclic subgroup $Gal(F_k/L_k)$ which reduces to the case when $n = k$. □

Chapter 4

Homological Ranks and Rank Growth

4.1 Homological Ranks

In this section, I am to establish some knowledge of the growth of the Mordell-Weil ranks of E over the fields within the False Tate curve extension tower. The methods are similar to those used in [3], but we deal with the case of multiplicative reduction at p.

We assume throughout this chapter again the validity of Conjecture 2.2.1, which claims that $X_p(E/F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$ for any triple (E, p, m) satisfying the assumptions made in Section 1.1. This implies that $Y_p(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module, and hence is finitely generated $\Lambda(H_*)$-module for any H_* a subgroup of H of finite index. Moreover, for each number field $L \subset F_\infty$, we have seen that the validity of Conjecture 2.2.1 implies the validity of Mazur's Conjecture over L.

Definition:. *Put*

$$\tau \stackrel{def}{=} rank_{\Lambda(H_K)} Y_p(E/F_\infty)$$

$$s_{E/L} \stackrel{def}{=} corank_{\mathbb{Z}_p} Sel_p(E/L) = dim_{\bar{\mathbb{Q}}_p} \left(X_p(E/L) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p \right)$$

for any number field $L \subset F_\infty$.

Recall the notations $L_n \overset{\text{def}}{=} \mathbb{Q}(\sqrt[p^n]{m})$ and $L'_n \overset{\text{def}}{=} \mathbb{Q}(\mu_p, \sqrt[p^n]{m})$.

Definition:. *For $n \geq 0$, let $H_{L_n} \overset{def}{=} Gal(F_\infty/L_n^{cyc})$, $H_{L'_n} \overset{def}{=} Gal(F_\infty/L_n'^{cyc})$ its maximal pro-p subgroup, and denote the λ-invariant by*

$$\lambda_n \overset{def}{=} \lambda_{\Lambda(\Gamma_{L_n})}\left(X_p(E/L_n^{cyc})\right) = rank_{\mathbb{Z}_p} Y_p(E/L_n^{cyc}).$$

Let us once and for all, introduce the same notation Δ for all of the cyclic Galois groups of order $p-1$ appearing in the tower, they can be identified by their action on the group μ_p. For instance:

$$\Delta \overset{\text{def}}{=} Gal(F_\infty/L_\infty^{cyc}) \cong Gal(K_\infty/\mathbb{Q}^{cyc}) \cong Gal(K/\mathbb{Q}).$$

Meanwhile, denote by $\hat{\Delta} \overset{\text{def}}{=} Hom(\Delta, \mathbb{Z}_p^\times)$ the dual of Δ, and by $\mathbf{1}$ the trivial element of $\hat{\Delta}$.

Definition:. *For a ring R, we can define $K_0(R)$, the Grothendieck group of R being the abelian group with generators $[P]$, one for each isomorphism class in the category of finitely generated projective R-modules with relations*

$$[P_2] = [P_1] + [P_3]$$

if there is a short exact sequence of finitely generated projective R-modules

$$0 \longrightarrow P_1 \longrightarrow P_2 \longrightarrow P_3 \longrightarrow 0.$$

Definition:. *Let M be a finitely generated $\Lambda(H)$-module and*

$$\cdots \longrightarrow P_{j+1} \longrightarrow P_j \longrightarrow P_{j-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0 \tag{4.1}$$

be a finite projective resolution of M, that is $P_j = 0$ for $j \gg 0$. We denote by

$$[M] \overset{def}{=} \sum_{i \geq 0} (-1)^i [P_i] \tag{4.2}$$

the formal alternating series, which is a finite sum.

Proposition 4.1.1. *This well-defines an element* $[M] \in K_0(\Lambda(H))$.

Proof. Clearly, since $\Lambda(H)$ has finite global homological dimension, such an finite projective resolution eq(4.1) exists for the finitely generated module M. We need to show that the right side of eq(4.2), as an element of $K_0(\Lambda(H))$, is independent on the choice of finite projective resolution of M. Take any finite projective resolution of M:

$$\cdots \longrightarrow P'_{j+1} \longrightarrow P'_j \longrightarrow P'_{j-1} \longrightarrow \cdots \longrightarrow P'_0 \longrightarrow M \longrightarrow 0. \tag{4.3}$$

We may assume $P_j = P'_j = 0$ for $j \gg 0$. By long Schanuel's lemma, [16, Corollary (5.5)] since P_i, P'_i are all projective, we have

$$P_0 \oplus P'_1 \oplus P_2 \oplus P'_3 \oplus P_4 \oplus \cdots \cong P'_0 \oplus P_1 \oplus P'_2 \oplus P_3 \oplus P'_4 \oplus \cdots$$

which yields the equality

$$\sum_{i\geq 0}(-1)^i[P_i] = \sum_{i\geq 0}(-1)^i[P'_i]$$

in $K_0(\Lambda(H))$. □

Lemma 4.1.1. *There is a canonical isomorphism*

$$l_\Delta : K_0\big(\Lambda(H)\big) \longrightarrow \bigoplus_{\chi\in\hat{\Delta}} \mathbb{Z} \tag{4.4}$$

where $[\Lambda(H) \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi)]$ *is correspondent to* $(0, \cdots, 0, 1, 0, \cdots, 0)$ *where* 1 *appears in the* χ*-component.*

Proof. This isomorphism is in fact the composition of the following isomorphisms:
Firstly, we have $H \cong H_K \rtimes \Delta$. Let J denote the kernel of the canonical surjection $\Lambda(H) \longrightarrow \mathbb{Z}_p[\Delta]$. This surjection induces a group homomorphism

$$K_0\big(\Lambda(H)\big) \longrightarrow K_0(\mathbb{Z}_p[\Delta])$$

which sends the isomorphic class of any finitely generated projective $\Lambda(H)$-module M to the isomorphic class of the module M/JM. The injectivity of this homomorphism is proved in [4, Lemma 3.5], using Nakayama's lemma by the fact that $H_K \cong \mathbb{Z}_p$ is a pro-p open normal subgroup of H and hence J is an ideal of $\Lambda(H)$ with $J^n \to 0$. The surjectivity of this group homomorphism is proved in [2, Chapter III Proposition 2.12] that we can write any finitely generated projective $\mathbb{Z}_p[\Delta]$-module as $Im(e_\Delta)$ for some idempotent e_Δ in $M_n(\mathbb{Z}_p[\Delta])$, the endomorphism ring of $\mathbb{Z}_p[\Delta]^n$ for some integer $n \geq 1$. In [2, Chapter III Proposition 2.10], since $\Lambda(H)$ is J-adically complete, e_Δ has a idempotent lifting e_H in $M_n(\Lambda(H))$, the endomorphism ring of $\Lambda(H)^n$. So, we have $Im(e_H)/J(Im(e_H)) \cong Im(e_\Delta)$.
Secondly since the ring homomorphism

$$\mathbb{Z}_p[\Delta] \longrightarrow \prod_{\chi \in \hat{\Delta}} \mathbb{Z}_p$$

induced by sending

$$\delta \mapsto (\chi(\delta))_{\chi \in \hat{\Delta}}$$

is an isomorphism too, (indeed, this $\mathbb{Z}_p$-modules homomorphism is given by a Vandermonde matrix of determinant $\pm \prod_{1 \leq < i < j \leq p-1}(\alpha_j - \alpha_i) \in \mathbb{Z}_p^\times$ for $\{\alpha_i\}$ the set of $(p-1)^{-th}$ roots of unity in $Z_p^\times$.) $K_0(\mathbb{Z}_p[\Delta])$ is hence further isomorphic to $\bigoplus_{\chi \in \hat{\Delta}} K_0(\mathbb{Z}_p) \cong \bigoplus_{\chi \in \hat{\Delta}} \mathbb{Z}$. From this construction, we see that this homomorphism l_Δ sends $[M]$, for any finitely generated projective $\Lambda(H)$ module, to $(\sum_{i \geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_K, M)^{(\chi)})_{\chi \in \hat{\Delta}}$. The second argument is trivial by the construction of the homomorphism. □

Definition:. *Let h_{L_n} be the group homomorphism*

$$h_{L_n} : K_0\big(\Lambda(H)\big) \longrightarrow \mathbb{Z}$$

defined by

$$[M] \mapsto \sum_{i \geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_{L_n}, M)$$

for M any finitely generated $\Lambda(H)$-module, and being extended to the Grothendieck group linearly.

This term $\sum_{i \geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_{L_n}, M)$ appears in [13, Section 2] where it is

denoted as $\chi_*(H_{L_n}, M)$ or $hmrank_{\Lambda(H_{L_n})}(M)$ which is called the homological rank of M if this value is finite.

Let us check that this homomorphism h_{L_n} is well defined. Since H_{L_n} (and H) has no non-trivial element of order p, $\Lambda(H_{L_n})$ (and $\Lambda(H)$) has finite p-homological dimension. So the sum $\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_{L_n}, M)$ is a finite sum for any finitely generated $\Lambda(H)$-module M. When M is a finitely generated projective $\Lambda(H)$-module, suppose we have the relation $[M] = [M'] + [M'']$, which by the definition of $K_0(\Lambda(H))$, is a short exact sequence of finitely generated projective $\Lambda(H)$-modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0.$$

From this, we get a long exact sequence

$$\begin{aligned}
&\cdots \longrightarrow H_m(H_{L_n}, M') \longrightarrow H_m(H_{L_n}, M) \longrightarrow H_m(H_{L_n}, M'') \longrightarrow \\
&\cdots \longrightarrow H_1(H_{L_n}, M') \longrightarrow H_1(H_{L_n}, M) \longrightarrow H_1(H_{L_n}, M'') \\
&\quad \longrightarrow H_0(H_{L_n}, M') \longrightarrow H_0(H_{L_n}, M) \longrightarrow H_0(H_{L_n}, M'') \longrightarrow 0
\end{aligned}$$

and $H_m(H_{L_n}, M') = H_m(H_{L_n}, M) = H_m(H_{L_n}, M'') = 0$ for $m \gg 0$. The alternating sum of the $\mathbb{Z}_p$-ranks along this long exact sequence is zero, and this yields

$$\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_{L_n}, M) = \sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_{L_n}, M') + \sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_{L_n}, M'')$$

hence this h_{L_n} is well-defined in $K_0(\Lambda(H))$. By Proposition 4.1.1, when M is a finitely generated $\Lambda(H)$-module, having a finite projective resolution as in eq(4.1), we can split up this resolution into short exact sequences and hence obtain long exact sequences of the corresponding H_{L_n} homology groups. Gathering these together, we have

$$\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_{L_n}, M) = \sum_{j\geq 0}(-1)^j \sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_{L_n}, P_j).$$

On the other hand, since $[M] = \sum_{j\geq 0}(-1)^j [P_j]$ we have also

$$h_{L_n}([M]) = \sum_{j\geq 0}(-1)^j \sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_{L_n}, P_j).$$

Hence h_{L_n} is well-defined by in the definition above.

Now, although $Y_p(E/F_\infty)$ is not a projective $\Lambda(H)$-module, we can still compute the value $h_{L_n}([Y_p(E/F_\infty)])$ since $Y_p(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module by assuming Conjecture 2.2.1. In the next two sections, we shall carry out this computation in two different approaches, leading to its relation to τ and λ_n respectively.

4.2 Computation of Homological Ranks of $Y_p(E/F_\infty)$ I

Proposition 4.2.1. *For $n \geq 0$, we have*

$$h_{L_n}([\Lambda(H) \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi)]) = \begin{cases} \dfrac{p^n - 1}{p - 1}, & \chi \neq \mathbf{1}, \quad (4.5) \\ \dfrac{p^n - 1}{p - 1} + 1, & \chi = \mathbf{1}. \quad (4.6) \end{cases}$$

Proof. Since $\Lambda(H) \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi)$ is a projective $\Lambda(H_{L_n})$-module,

$$H_i(H_{L_n}, \Lambda(H) \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi)) = 0$$

for $i \geq 1$. Hence, by the definition, it remains to compute the $\mathbb{Z}_p$-rank of

$$H_0(H_{L_n}, \Lambda(H) \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi)) = \mathbb{Z}_p \otimes_{\Lambda(H_{L_n})} \Lambda(H) \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi) \quad (4.7)$$

where $\mathbb{Z}_p \otimes_{\Lambda(H_{L_n})} \Lambda(H)$ clearly is a free $\mathbb{Z}_p$-module on generators the right cosets of H_{L_n} in H, hence is endowed naturally with an action of Δ from the right. To compute the Z_p-rank of the module in eq(4.7), we first partition $\mathbb{Z}_p \otimes_{\Lambda(H_{L_n})} \Lambda(H)$ by its Δ-orbits.

$$\mathbb{Z}_p \otimes_{\Lambda(H_{L_n})} \Lambda(H) \cong \bigoplus_{\Delta-orbits\, Z} R_Z \quad (4.8)$$

where R_Z is a free $\mathbb{Z}_p$-module of rank the length of the orbit Z. In fact, apart from the singleton orbit $\{H_{L_n}\}$, the rest of the Δ-orbits are faithful. Hence we

have

$$R_Z \cong \begin{cases} \mathbb{Z}_p(\mathbf{1}), & \text{when } Z = \text{singleton } \{H_{L_n}\}, \quad (4.9) \\ \mathbb{Z}_p[\Delta], & \text{when } Z \neq \text{singleton } \{H_{L_n}\}, \quad (4.10) \end{cases}$$

and there are $\frac{p^n-1}{p-1}$ copies of $\mathbb{Z}_p[\Delta]$ and one copy of $\mathbb{Z}_p(\mathbf{1})$. Hence, the result follows from the trivial facts that

$$\mathbb{Z}_p(\mathbf{1}) \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi) \cong \begin{cases} \mathbb{Z}_p(\mathbf{1}), & \text{when } \chi = \mathbf{1}, \quad (4.11) \\ 0, & \text{when } \chi \neq \mathbf{1}. \quad (4.12) \end{cases}$$

and

$$\mathbb{Z}_p[\Delta] \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi) \cong \mathbb{Z}_p(\chi) \quad (4.13)$$

as $Z_p[\Delta]$-modules.

□

Proposition 4.2.2. *For $n \geq 0$, we have*

$$h_{L_n}([Y_p(E/F_\infty)]) = \sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}\left(H_i\left(H_K, Y_p(E/F_\infty)\right)^{(\mathbf{1})}\right) + \tau \cdot \frac{p^n-1}{p-1}. \quad (4.14)$$

Proof. Let Y denote $Y_p(E/F_\infty)$. From the construction of the group isomorphism l_Δ in the proof of Lemma 4.1.1, by linearity we have

$$l_\Delta([Y]) = \left(\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_K, Y)^{(\chi)}\right)_{\chi\in\hat{\Delta}}$$

or equivalently,

$$[Y] = \sum_{\chi\in\hat{\Delta}}\left(\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p} H_i(H_K, Y)^{(\chi)}\right)[\Lambda(H) \otimes_{\mathbb{Z}_p[\Delta]} Z_p(\chi)] \in K_0\left(\Lambda(H)\right)$$

Applying the formula in Proposition 4.2.1, we get

$$\begin{aligned} h_{L_n}([Y]) =&(\frac{p^n-1}{p-1})\cdot\sum_{\chi\neq\mathbf{1}}\left(\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}H_i(H_K,Y)^{(\chi)}\right)\\ &+(\frac{p^n-1}{p-1}+1)\cdot\left(\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}H_i(H_K,Y)^{(\mathbf{1})}\right)\\ =&(\frac{p^n-1}{p-1})\cdot\sum_{\chi\in\hat{\Delta}}\left(\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}H_i(H_K,Y)^{(\chi)}\right)\\ &+1\cdot\left(\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}H_i(H_K,Y)^{(\mathbf{1})}\right) \end{aligned}$$

and the summation

$$\begin{aligned} \sum_{\chi\in\hat{\Delta}}\left(\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}\big(H_i(H_K,Y)\big)^{(\chi)}\right) &= \sum_{i\geq 0}(-1)^i\sum_{\chi\in\hat{\Delta}} rank_{\mathbb{Z}_p}\big(H_i(H_K,Y)\big)^{(\chi)}\\ &= \sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}\bigoplus_{\chi\in\hat{\Delta}}\big(H_i(H_K,Y)\big)^{(\chi)}\\ &= \sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}\big(H_i(H_K,Y)\big) \end{aligned}$$

and the right hand side is just the $\Lambda(H_K)$-rank of Y by Howson's formula eq(1.8). Hence eq(4.14) follows. □

4.3 Computation of Homological Ranks of $Y_p(E/F_\infty)$ II

On the other hand, we can relate $h_{L_n}([Y_p(E/F_\infty)])$ with the invariant λ_n. Let S_p denote the singleton $\{p\}$, S_{ram} denote the set of primes $\{q_i : q_i \mid m\}$. Let $S_*(F)$ denote the set of primes of F lying above S_*, for any algebraic extension F over $\mathbb{Q}$ and $S_* = S_p$ or S_{ram}. For each integer $n \geq 0$, we denote by w_{u_n} a fixed place of F_∞ lying above u_n, which denote a place of L_n^{cyc}. We shall denote the corresponding decomposition subgroup by H_{L_n,u_n}.

Let us introduce the following notation.

Definition:. *For any odd prime p, positive integer $m > 1$ and integer $n \geq 0$,*

define an integer

$$\beta_{p,m,n} \overset{def}{=} \begin{cases} 0, & \text{if } p \mid m, \\ min\{n, r\}, & \text{if } p \nmid m \text{ and } p^{r+1} \parallel m^{p-1} - 1. \end{cases}$$

We saw before that the prime p decomposes into $p^{\beta_{p,m,n}}$ totally ramified primes over $\mathbb{Q}(\mu_{p^n}, \sqrt[p^n]{m})$. We say the pair (p, m) satisfies assumption "$\beta = 0$" if either $p \mid m$ or $p \parallel m^{p-1} - 1$. Clearly, p totally ramifies to a unique prime of F_∞ when assuming "$\beta = 0$".

Theorem 4.3.1. *Suppose the triple (E, p, m) satisfies the assumption made in Section 1.1 and assuming the validity of Conjecture 2.2.1. When E has split multiplicative reduction at p, we further assume "$\beta = 0$". Then for $n \geq 0$, we have*

$$h_{L_n}([Y_p(E/F_\infty)]) = \lambda_n + \sum_{u_n} rank_{\mathbb{Z}_p}\left(T_p(E)^{J_{u_n}}\right) + \delta_p \tag{4.15}$$

where the u_n runs over all places of $S_{ram}(L_n^{cyc}) - S_p(L_n^{cyc})$ in the sum, J_{u_n} denotes the absolute Galois group of L_{n,u_n}^{cyc}, and

$$\delta_p \overset{def}{=} \begin{cases} 1, & \text{if } E \text{ has split multiplicative reduction at } p; \\ 0, & \text{if } E \text{ has non-split multiplicative reduction at } p. \end{cases} \tag{4.16}$$

Applying the fundamental diagram (2.3) with L replaced by number field L_n

for $n \geq 0$, we have

$$\begin{array}{ccccccc}
 & & & & H^2\left(H_{L_n}, E_{p^\infty}(F_\infty)\right) & & \\
 & & & & \uparrow & & \\
0 & \longrightarrow & Sel_p(E/F_\infty)^{H_{L_n}} & \longrightarrow & H^1\left(G_S(F_\infty), E_{p^\infty}\right)^{H_{L_n}} & \xrightarrow{\lambda_{F_\infty}^{H_{L_n}}} & \oplus_{u_n \in S(L_n^{cyc})} J_{u_n}(F_\infty)^{H_{L_n}} \\
 & & \uparrow{\scriptstyle r_{L_n^{cyc}}} & & \uparrow{\scriptstyle res_{L_n^{cyc}}} & & \uparrow{\scriptstyle \oplus_{u_n \in S(L_n^{cyc})} h_{u_n}} \\
0 & \longrightarrow & Sel_p(E/L_n^{cyc}) & \longrightarrow & H^1\left(G_S(L_n^{cyc}), E_{p^\infty}\right) & \xrightarrow{\lambda_{L_n^{cyc}}} & \oplus_{u_n \in S(L_n^{cyc})} J_{u_n}(L_n^{cyc}) \\
 & & & & \uparrow & & \\
 & & & & H^1\left(H_{L_n}, E_{p^\infty}(F_\infty)\right) & &
\end{array} \tag{4.17}$$

where $S = S^f(\mathbb{Q}) = S_p \cup S_{bad} \cup S_{ram}$ denotes finite set of rational primes consist of p and all the other primes where the elliptic curve E has bad reduction and all the prime divisors of m; and $S(F)$ denotes the set of primes of F lying above S, for any algebraic extension F over $\mathbb{Q}$. Applying Theorem 2.3.1 again to $F/k = L_n^{cyc}/L_n$, since Ribet's theorem implies the finiteness of $E(L_n^{cyc})_{p^\infty}$ and the validity of $\mathfrak{M}_H(G)$ conjecture ensures that $X_p(E/L_n^{cyc})$ is $\Lambda(\Gamma_{L_n})$-torsion, we deduce that $H^2\left(G_S(L_n^{cyc}), E_{p^\infty}\right) = 0$ and $\lambda_{L_n^{cyc}}$ is surjective.

Lemma 4.3.1. *For each $n \geq 0$, $H^1\left(H_{L_n}, E_{p^\infty}(F_\infty)\right)$ has vanishing $\mathbb{Z}_p$-corank.*

Proof. Let Δ denote the Galois group $Gal(L_n'^{cyc}/L_n^{cyc})$, we have the following inflation-restriction exact sequence

$$0 \longrightarrow H^1\left(\Delta, E_{p^\infty}(L_n'^{cyc})\right) \longrightarrow H^1\left(H_{L_n}, E_{p^\infty}(F_\infty)\right) \longrightarrow H^1\left(H_{L_n'}, E_{p^\infty}(F_\infty)\right)^\Delta \tag{4.18}$$

By Ribet's theorem again, $E_{p^\infty}(L_n'^{cyc})$ is finite, and thus $H^1\left(\Delta, E_{p^\infty}(L_n'^{cyc})\right)$ is finite. On the other hand, by Poincare duality, $H^1\left(H_{L_n'}, E_{p^\infty}(F_\infty)\right) \cong E_{p^\infty}(F_\infty)_{H_{L_n'}}$, which has vanishing $\mathbb{Z}_p$-corank since $E_{p^\infty}(F_\infty)^{H_{L_n'}} = E_{p^\infty}(L_n'^{cyc})$ is again finite. Consequently, $corank_{\mathbb{Z}_p} H^1\left(H_{L_n}, E_{p^\infty}(F_\infty)\right) = 0$. □

We will later see in Lemma 4.3.3 that $ker(h_{u_n})$ is a co-finitely generated $\mathbb{Z}_p$-

module, for each $u_n \in S(L_n^{cyc})$.

Proposition 4.3.1. *For each $n \geq 0$, $Sel_p(E/F_\infty)^{H_{L_n}}$ is a finitely generated $\Lambda(\Gamma_{L_n})$-cotorsion module and the λ-invariant of its Pontryagin dual is*

$$\lambda_{\Lambda(\Gamma_{L_n})}(\widehat{Sel_p(E/F_\infty)^{H_{L_n}}}) = \lambda_{\Lambda(\Gamma_{L_n})}\widehat{Sel_p(E/L_n^{cyc})} + \sum_{u_n \in S(L_n^{cyc})} corank_{\mathbb{Z}_p} ker(h_{u_n}) \tag{4.19}$$

Proof. Since

$$H_{L_n} = H_{L_n'} \rtimes \Delta$$

with Δ a cyclic group of order $p-1$, which is coprime to p, H_{L_n} and $H_{L_n'}$ have the same p-cohomological dimension, which is equal to 1 since $H_{L_n'} \cong \mathbb{Z}_p$. Hence, $H^2\big(H_{L_n}, E_{p^\infty}(F_\infty)\big)$ vanishes. The rest of the proof is identical to the proof of Corollary 2.3.2. □

Similarly to Lemma 2.5.1, we have

Lemma 4.3.2.

$$H_1\big(H_{L_n}, X_p(E/F_\infty)\big) = 0 \tag{4.20}$$

Proof. Since the validity of Conjecture 2.2.1 and Ribet's theorem enable one to checks the surjectivity of $\lambda_{L_n^{cyc}}$ by Theorem 2.3.1. Together with $cd_p(H_{L_n}) = 1$, this is essentially the same proof of Lemma 2.5.1. □

Proposition 4.3.2. *For any $n \geq 0$, we have*

$$H_i\big(H_{L_n}, Y_p(E/F_\infty)\big) = 0, \qquad for \;\; i \geq 1; \tag{4.21}$$

$$rank_{\mathbb{Z}_p} H_0\big(H_{L_n}, Y_p(E/F_\infty)\big) = \lambda_{\Lambda(\Gamma_{L_n})} H_0\big(H_{L_n}, X_p(E/F_\infty)\big). \tag{4.22}$$

Proof. By assumption, $Y_p(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module and hence a finitely generated $\Lambda(H_{L_n})$-module. By Proposition 1.2.2, $H_i\big(H_{L_n}, Y_p(E/F_\infty)\big)$ is a finitely generated $\mathbb{Z}_p$-module for each $i \geq 0$. Since H_{L_n} has p-cohomological dimension 1, plainly $H_i\big(H_{L_n}, Y_p(E/F_\infty)\big) = 0$ for $i \geq 2$. To observe the case

when $i = 1$, take the H_{L_n}-homology of the canonical short exact sequence of $\Lambda(H_{L_n})$-modules

$$0 \to X_p(E/F_\infty)(p) \to X_p(E/F_\infty) \to Y_p(E/F_\infty) \to 0. \tag{4.23}$$

It yields an exact sequence of $\Lambda(\Gamma_{L_n})$-modules

$$\begin{aligned} 0 = H_1\big(H_{L_n}, X_p(E/F_\infty)\big) \to H_1\big(H_{L_n}, Y_p(E/F_\infty)\big) \to H_0\big(H_{L_n}, X_p(E/F_\infty)(p)\big) \\ \to H_0\big(H_{L_n}, X_p(E/F_\infty)\big) \to H_0\big(H_{L_n}, Y_p(E/F_\infty)\big) \to 0. \end{aligned} \tag{4.24}$$

In fact, each term in this exact sequence is $\Lambda(\Gamma_{L_n})$-torsion. Indeed, the validity of Conjecture 2.2.1 implies that $Sel_p(E/L_n^{cyc})$ is a finitely generated $\Lambda(\Gamma_{L_n})$-cotorsion module. Together with the remark preceding of Proposition 4.3.1, $H_0\big(H_{L_n}, X_p(E/F_\infty)\big)$ is $\Lambda(\Gamma_{L_n})$-torsion, hence so is $H_0\big(H_{L_n}, Y_p(E/F_\infty)\big)$. On the other hand, $X_p(E/F_\infty)(p)$ is annihilated by some power of p and hence the homology group $H_i\big(H_{L_n}, X_p(E/F_\infty)(p)\big)$ will be annihilated by this power of p, for each $i \geq 0$. In particular, they are $\Lambda(\Gamma_{L_n})$-torsion, with trivial $\lambda_{\Lambda(\Gamma_{L_n})}$-invariants and so is the submodule $H_1\big(H_{L_n}, Y_p(E/F_\infty)\big)$. Moreover, since multiplying by p, (and hence by any power of p) is injective in $Y_p(E/F_\infty)$, the induced multiplying by p in $H_1\big(H_{L_n}, Y_p(E/F_\infty)\big)$ is again injective, (so is the multiplying by a power of p map). Hence, $H_1\big(H_{L_n}, Y_p(E/F_\infty)\big) = 0$ since it injects into a module which is annihilated by some power of p.
Since the $\lambda_{\Lambda(\Gamma_{L_n})}$-invariant is additive in exact sequences and it coincides the $\mathbb{Z}_p$-rank upon finitely generated $\mathbb{Z}_p$-modules, eq(4.22) follows from taking $\lambda_{\Lambda(\Gamma_{L_n})}$-invariant along the long exact sequence above. □

Lemma 4.3.3. *For $n \geq 0$ and any non-Archimedean place u_n of $S(L_n^{cyc})$, we have*

1. *For $u_n \notin S_{ram}(L_n^{cyc}) \cup S_p(L_n^{cyc})$,*

$$ker(h_{u_n}) = 0$$

2. *For $u_n \in S_p(L_n^{cyc})$,*

$$ker(h_{u_n}) \cong \begin{cases} 0 & u_n \in S_{ns}(L_n^{cyc}) \\ \mathbb{Q}_p/\mathbb{Z}_p & u_n \in S_s(L_n^{cyc}) \end{cases} \tag{4.25}$$

3. *For $u_n \in S_{ram}(L_n^{cyc}) - S_p(L_n^{cyc})$,*
say $u_n = u_{q_i,n}$ being a place lying above some rational prime $q_i \neq p$ dividing m, we have

$$\widehat{ker(h_{u_{q_i,n}})} \cong T_p(E)^{J_{u_{q_i,n}}} \tag{4.26}$$

and this latter module remain the same regardless of the choice of the place $u_{q_i,n}$ above q_i and $n \geq 0$. In particular, its $\mathbb{Z}_p$-rank is dependent only on q_i but not n nor the choice of $u_{q_i,n}$. Here, $J_{u_{q_i,n}}$ denotes the absolute Galois group of $L^{cyc}_{n,u_{q_i,n}}$.

Proof. Trivially,

$$ker(h_{u_n}) = H^1(H_{L_n,u_n}, E(F_{\infty,w_{u_n}}))_{p^\infty}.$$

As a result of Lutz's theorem, this is isomorphic to $H^1(H_{L_n,u_n}, E_{p^\infty}(F_{\infty,w_{u_n}}))$ in case 1 and 3. Since the extension F_∞/L_n^{cyc} is unramified outside $S_{ram}(L_n^{cyc}) \cup S_p(L_n^{cyc})$, the corresponding inertia subgroup for $u_n \notin S_{ram}(L_n^{cyc}) \cup S_p(L_n^{cyc})$ is trivial and hence the corresponding decomposition subgroup H_{L_n,u_n} is a subgroup of Δ. Therefore

$$ker(h_{u_n}) \cong H^1(H_{L_n,u_n}, E_{p^\infty}(F_{\infty,w_{u_n}})) = 0.$$

So proved 1.
For 3, we first notice that

$$H^1(H_{L_n,u_{q_i,n}}, E_{p^\infty}(F_{\infty,w_{u_{q_i,n}}})) \cong H^1(J_{u_{q_i,n}}, E_{p^\infty}).$$

Indeed, the subgroup of $J_{u_{q_i,n}}$ which fixes $F_{\infty,w_{u_{q_i,n}}}$ has no quotient of order divisible by p since $F_{\infty,w_{u_{q_i,n}}}$ contains the maximal tamely ramified p-extension of $\mathbb{Q}_{q_i}$ as $u_{q_i,n}$ is infinitely ramified over $F_{\infty,w_{u_{q_i,n}}}$. On the other hand, $H^1(J_{u_{q_i,n}}, E_{p^\infty})$ is Pontryagin dual to

$$H^0(J_{u_{q_i,n}}, Hom(E_{p^\infty}, \mu_{p^\infty})) \cong H^0(J_{u_{q_i,n}}, T_p(E))$$

since $Hom(E_{p^\infty}, \mu_{p^\infty}) \cong T_p(E)$ by Weil pairing. This proves eq(4.26) and hence shows that $ker(h_{u_{q_i,n}})$ has finite $\mathbb{Z}_p$-corank. Moreover, by the assumption of the triple (E, p, m), E has semistable reduction over each $u \in S_{ram} - S_p$ and hence has semistable reduction over $u_n \in S_{ram}(L_n^{cyc}) - S_p(L_n^{cyc})$. When E has good reduction at q_i, E has good reduction at $u_{q_i,n}$ for all $n \neq 0$. Since $q_i \neq p$, the

action of $J_{u_{q_i,n}}$ on $T_p(E)$ is unramified for every $n \geq 0$ and thus this action factors through its quotient by the inertia, which are all isomorphic among the integers $n \geq 0$ since $\{L_n^{cyc}\}_{n\geq 0}$ is a totally ramified tower of extensions for $u_{q_i,0}$. Hence

$$T_p(E)^{J_{u_{q_i,n}}} = T_p(E)^{J_{u_{q_i,0}}}$$

for all $n \geq 0$. When E has multiplicative reduction at q_i, E has multiplicative reduction at $u_{q_i,n}$ for all $n \neq 0$, as a result of Tate curve, we see that $T_p(E)^{I_{u_{q_i,n}}}$ is independent on $n \geq 0$ and

$$rank_{\mathbb{Z}_p} T_p(E)^{I_{u_{q_i,n}}} = 1,$$

where $I_{u_{q_i,n}}$ denotes the inertia subgroup of $J_{u_{q_i,n}}$ for each $n \geq 0$. Now, since $J_{u_{q_i,n}}$ acts unramifiedly on the common $\mathbb{Z}_p$-ranked one module $T_p(E)^{I_{u_{q_i,n}}} = T_p(E)^{I_{u_{q_i,0}}}$ for each $n \geq 0$, by the same argument before, $\{L_n^{cyc}\}_{n\geq 0}$ being a totally ramified tower of extensions for $u_{q_i,0}$ implies that $T_p(E)^{J_{u_{q_i,n}}}$ has $\mathbb{Z}_p$-rank at most 1 which is independent on n, and Case 3 is proved.
For Case 2, we need to apply the argument of theorem of deeply ramified again. Let $u_n = u_{p,n}$ denote a place in $S_p(L_n^{cyc})$. Obviously, both $L_{n,u_{p,n}}^{cyc}$ and $F_{\infty,\tilde{p}}$ are deeply ramified over $\mathbb{Q}_p$. Using the notations and arguments in Section 2.4, $Im(\kappa_{\mathcal{F}}) = Im(\lambda_{\mathcal{F}})$ for both $\mathcal{F} = L_{n,u_{p,n}}^{cyc}$ and $F_{\infty,\tilde{p}}$, and hence the restriction map $h_{u_{p,n}}$ can be rewritten as

$$Im(\pi_{L_{n,u_{p,n}}^{cyc}}) \xrightarrow{h_{u_{p,n}}} Im(\pi_{F_{\infty,\tilde{p}}})^{H_K}.$$

Since the absolute Galois group $G_{L_{n,u_{p,n}}^{cyc}}$ has p-cohomological dimension 1, $\pi_{L_{n,u_{p,n}}^{cyc}}$ is surjective and hence

$$ker(h_{u_{p,n}}) \cong H^1(H_{L_n,u_{p,n}}, \mathcal{D}^{G_{F_{\infty,\tilde{p}}}})$$

with $\mathcal{D}$ as defined in Section 2.4.

- When $u_{p,n} \in S_s(L_n^{cyc})$,
  since p is totally ramified over L_n^{cyc}, E has split multiplicative reduction at p. Hence,
  $$\mathcal{D} \cong \mathbb{Q}_p/\mathbb{Z}_p$$

as $G_{\mathbb{Q}_p}$-modules with trivial action. We have then

$$H^1(H_{L_n,u_{p,n}}, \mathcal{D}^{G_{F_{\infty,\tilde{p}}}}) \cong Hom(H_{L_n,u_{p,n}}, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Q}_p/\mathbb{Z}_p$$

as groups, and hence proved the statement in this case.

- when $u_{p,n} \in S_{ns}(L_n^{cyc})$,
  E has non-split multiplicative reduction at p. Hence,

$$\mathcal{D} \cong \mathbb{Q}_p/\mathbb{Z}_p \otimes \phi$$

as $G_{\mathbb{Q}_p}$-modules with ϕ the unramified non-trivial quadratic character of $G_{\mathbb{Q}_p}$. Since $F_{\infty,\tilde{p}}/\mathbb{Q}_p$ is totally ramified, we have

$$\mathcal{D}^{G_{F_{\infty,\tilde{p}}}} = 0$$

and hence

$$ker(h_{u_{p,n}}) = 0.$$

Hence proved Case 2. □

Proof of Theorem 4.3.1

Proof. Combining Proposition 4.3.1 and Proposition 4.3.2, immediately we get

$$h_{L_n}([Y_p(E/F_\infty)]) = \lambda_{\Lambda(\Gamma_{L_n})} \widehat{Sel_p(E/L_n^{cyc})} + \sum_{u_n \in S(L_n^{cyc})} corank_{\mathbb{Z}_p} ker(h_{u_n}) \tag{4.27}$$

By Lemma 4.3.3, we can rewrite the term $\sum_{u_n \in S(L_n^{cyc})} corank_{\mathbb{Z}_p} ker(h_{u_n})$ as

$$\delta_p \times \#S_p(L_n^{cyc}) + \sum_{u_n \in S_{ram}(L_n^{cyc}) - S_p(L_n^{cyc})} rank_{\mathbb{Z}_p}\left(T_p(E)^{J_{u_n}}\right) \tag{4.28}$$

since each of the prime in $S_p(F_\infty)$ is totally ramified over p, each of the prime in $S_p(L_n^{cyc})$ is totally ramified over p too, hence E has the same type of multiplicative reduction at all primes in $S_p(L_n^{cyc})$ as at p. Thus when $\delta_p = 0$, eq(4.15) follows. When $\delta_p = 1$, by assumption "$\beta = 0$", we have $\#S_p(L_n^{cyc}) = 1$ and hence eq(4.15) follows.

□

From Proposition 4.2.2, noticing that there is a term

$$\sum_{i\geq 0}(-1)^i rank_{\mathbb{Z}_p}\big(H_i\big(H_K, Y_p(E/F_\infty)\big)\big)^{(1)}$$

which is independent of n in the formula eq(4.14). We can easily get rid of this term by taking the difference of the same equation eq(4.14) for for different n's. A similar phenomena actually happens to Theorem 4.3.1.

Lemma 4.3.4. *For each rational prime $q_i \neq p$ dividing m, and any non-negative integral pair (n, n'), we have*

$$\sum_{u_n|q_i} rank_{\mathbb{Z}_p}\big(T_p(E)^{J_{u_n}}\big) = \sum_{u_{n'}|q_i} rank_{\mathbb{Z}_p}\big(T_p(E)^{J_{u_{n'}}}\big).$$

Proof. From the proof of Case 3 of Lemma 4.3.3, we have seen that $rank_{\mathbb{Z}_p}\big(T_p(E)^{J_{u_n}}\big)$ only depends on q_i, not on n nor the choice of u_n. Hence, it suffices to show that the number of primes over L_n^{cyc} above q_i is again independent on n. Indeed, this follows from the fact that q_i is totally ramified within the tower $\{L_n\}_{n\geq 0}$ of fields and hence there is a unique prime above q_i over each number field L_n, and each of these splits into a same (finite) number of primes in its $\mathbb{Z}_p$-cyclotomic extension L_n^{cyc}.

□

4.4 Rank Growth in the False Tate Curve Extension

The property of having these highly complicated but n-independent terms in both the expressions of $h_{L_n}([Y_p(E/F_\infty)])$ essentially allows us to 'extinguish' them and give a neat connection to link up the arithmetic invariants which at prior seem unrelated.

From this point onward, we always assume the pair (p, m) satisfies hypothesis "$\beta = 0$" when E has split multiplicative reduction at p.

Proposition 4.4.1. *For $n \geq 0$, we have*

$$\lambda_{n+1} - \lambda_n = \tau p^n \tag{4.29}$$

Proof. From the discussion above, both sides of eq(4.29) equal to

$$h_{L_{n+1}}([Y_p(E/F_\infty)]) - h_{L_n}([Y_p(E/F_\infty)])$$

by eq(4.15) and eq(4.14) respectively.

□

Corollary 4.4.1. *We have*

$$s_{E/L_0} \equiv s_{E/L_2} \equiv \cdots \equiv s_{E/L_{2k}} \equiv \cdots \mod 2, \tag{4.30}$$

and

$$s_{E/L_1} \equiv s_{E/L_3} \equiv \cdots \equiv s_{E/L_{2k+1}} \equiv \cdots \mod 2. \tag{4.31}$$

Moreover, the values in eq(4.30) and eq(4.31) have the same parity if and only if τ is even.

Proof. In view of Theorem 3.3.2 for $k = L_n$, we have

$$\lambda_n \equiv s_{E/L_n} \mod 2.$$

Hence, by taking *mod* 2 of eq(4.29), since p is odd, we obtain

$$s_{E/L_{n+1}} \equiv s_{E/L_n} + \tau \mod 2,$$

and consequently

$$s_{E/L_{n+2}} \equiv s_{E/L_n} \mod 2.$$

Finally the statements follow from these.

□

Corollary 4.4.2. *When τ is odd, we have*

$$s_{E/L_0} < s_{E/L_1} < s_{E/L_2} < \cdots < s_{E/L_{n-1}} < s_{E/L_n} < \cdots \tag{4.32}$$

and in particular, s_{E/L_n} has a lower bound

$$s_{E/L_n} \geq s_{E/\mathbb{Q}} + n \tag{4.33}$$

for $n \geq 1$.

Proof. By Proposition 1.4.1 eq(1.28), the p-Selmer rank never decreases over any field extensions. From the last statement of the corollary above, we see that when τ is odd, the p-Selmer rank can never be unraised over the tower $\{L_n\}_{n\geq 0}$ since

$$s_{E/L_{n+1}} \not\equiv s_{E/L_n} \mod 2$$

for all $n \geq 0$. Therefore,

$$s_{E/L_{n+1}} \geq s_{E/L_n} + 1 \tag{4.34}$$

for all $n \geq 0$ and eq(4.32) follows. In particular, the lower bound given in eq(4.33) is just the inductive lower bound of eq(4.34).

□

For any finite Galois extension L over $\mathbb{Q}$, since by assumption, E is defined over $\mathbb{Q}$, $X_p(E/L)\otimes_{\mathbb{Z}_p}\bar{\mathbb{Q}}_p$ is a $\bar{\mathbb{Q}}_p$-representation of $Gal(L/\mathbb{Q})$, and more generally, a $\bar{\mathbb{Q}}_p$-representation of $Gal(L/L')$ for any intermediate number field $L' \subset L$. This $\bar{\mathbb{Q}}_p$-representation is of finite dimension $s_{E/L}$. Hence by Maschke's theorem, this representation is semisimple and thus we have

$$\left(X_p(E/L) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right)^{Gal(L/L')} = X_p(E/L') \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$$

and decomposition of representation

$$X_p(E/L) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p \cong X_p(E/L') \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p \oplus A_{L/L'}$$

where $A_{L/L'}$ is the complement of $X_p(E/L')\otimes_{\mathbb{Z}_p}\bar{\mathbb{Q}}_p$ in $X_p(E/L)\otimes_{\mathbb{Z}_p}\bar{\mathbb{Q}}_p$ which can also be characterized by being the largest $Gal(L/\mathbb{Q})$-invariant sub-representation of $X_p(E/L) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$, that contains no non-zero sub-representation on which $Gal(L/L')$ acts trivially.

Using these properties of semisimple Galois representations, one can deduce the growth of the $\mathbb{Z}_p$-Selmer coranks over certain tower of finite Galois extensions, according to the respective growth over a tower of non-Galois tower.

More specifically, given the strict growth of p-Selmer rank of E over L_n, we shall obtain certain strict growth over the tower of the respective Galois closures F_n which inductively provides a lower bound of the growth of p-Selmer rank of E over F_n. Here F_n is just the composite field K_nL_n, and more generally, the composite field K_iL_j is Galois over $\mathbb{Q}$ when $i \geq j$.

Proposition 4.4.2. *When τ is odd, we have*

$$s_{E/F_n} \geq s_{E/K_nL_{n-1}} + p^{n-1}(p-1) \geq s_{E/F_{n-1}} + p^{n-1}(p-1) \tag{4.35}$$

for all $n \geq 1$. In particular, s_{E/F_n} has a lower bound

$$s_{E/F_n} \geq s_{E/K} + p^n - 1 \tag{4.36}$$

for $n \geq 1$.

Proof. For $n \geq 1$, from the preceding discussion, we have a decomposition of $Gal(F_n/\mathbb{Q})$-representation

$$X_p(E/F_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p = \left(X_p(E/K_nL_{n-1}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right) \oplus A_{F_n/K_nL_{n-1}}.$$

We shall first show that when τ is odd,

$$A_{F_n/K_nL_{n-1}} \neq 0.$$

Assume the contrary, we have

$$X_p(E/F_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p = \left(X_p(E/K_nL_{n-1}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right) \cong \left(X_p(E/F_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right)^{Gal(F_n/K_nL_{n-1})}.$$

Note that $Gal(F_n/L_n) \cong Gal(K_nL_{n-1}/L_{n-1})$, taking the $Gal(F_n/L_n)$-invariant from the above, we get

$$\begin{aligned} X_p(E/L_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p &= \left(X_p(E/F_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right)^{Gal(F_n/L_n)} \\ &\cong \left(\left(X_p(E/F_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right)^{Gal(F_n/K_nL_{n-1})}\right)^{Gal(K_nL_{n-1}/L_{n-1})}. \\ &= \left(X_p(E/F_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right)^{Gal(F_n/L_{n-1})}. \\ &= X_p(E/L_{n-1}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p, \end{aligned}$$

hence $s_{E/L_n} = s_{E/L_{n-1}}$, which contradicts Corollary 4.4.2 eq(4.32) as τ is odd.

Secondly, we shall try to determine this non-zero $Gal(F_n/\mathbb{Q})$-representation $A_{F_n/K_nL_{n-1}}$. By definition, $A_{F_n/K_nL_{n-1}}$ contains no non-zero $Gal(F_n/\mathbb{Q})$-sub-representation on which $Gal(F_n/K_nL_{n-1})$ acts trivially. By semisimplicity, $A_{F_n/K_nL_{n-1}}$ is a direct sum of irreducible $Gal(F_n/\mathbb{Q})$-representations on which the subgroup $Gal(F_n/K_nL_{n-1})$ does not act trivially. We have established in Lemma 3.4.2 that there is a unique irreducible $\bar{\mathbb{Q}}_p$-representation of $Gal(F_n/\mathbb{Q})$ which does not factor through $Gal(K_nL_{n-1}/\mathbb{Q})$, denoted by ρ_{χ_n}. Therefore, we have

$$A_{F_n/K_nL_{n-1}} \cong (\rho_{\chi_n})^{\oplus k_n}$$

for some integer $k_n \geq 1$, as $A_{F_n/K_nL_{n-1}} \neq 0$. Thus, we have

$$\begin{aligned} s_{E/F_n} &= s_{E/K_nL_{n-1}} + k_n \cdot p^{n-1}(p-1) \\ &\geq s_{E/K_nL_{n-1}} + p^{n-1}(p-1) \end{aligned}$$

as ρ_{χ_n} is of $p^{n-1}(p-1)$ dimensional. This proves the left inequality of eq(4.35). The right inequality of eq(4.35) is just a trivial fact since $X_p(E/F_{n-1}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$ is a $Gal(K_nL_{n-1}/\mathbb{Q})$-subrepresentation of $X_p(E/K_nL_{n-1}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$.

Lastly, eq(4.36) is just the inductive consequence of eq(4.35), as

$$\begin{aligned} s_{E/F_n} &\geq p^{n-1}(p-1) + s_{E/F_{n-1}} \\ &\geq p^{n-1}(p-1) + p^{n-2}(p-1) + s_{E/F_{n-2}} \\ &\geq \cdots\cdots\cdots\cdots \\ &\geq p^{n-1}(p-1) + p^{n-2}(p-1) + \cdots + p^1(p-1) + s_{E/F_1} \\ &\geq p^{n-1}(p-1) + p^{n-2}(p-1) + \cdots + p^1(p-1) + (p-1) + s_{E/K_1} \\ &= p^n - 1 + s_{E/K} \end{aligned} \tag{4.37}$$

□

Definition:. *Let ρ be an irreducible $\bar{\mathbb{Q}}_p$-Artin representation which factors through $Gal(k/\mathbb{Q})$ for k a finite Galois extension of $\mathbb{Q}$. Let $s_{E,\rho}$ denote the number of copies of ρ occurring in the representation $X_p(E/k) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$.*

Theorem 4.4.1. *Suppose the triple (E, p, m) satisfies the assumption made in Section 1.1 and assuming the validity of Conjecture 2.2.1. When E has split multiplicative reduction at p, we further assume "$\beta = 0$", then for all absolutely irreducible self-dual Artin representations ρ of $G = Gal(F_\infty/\mathbb{Q})$ with dimension greater than 1, we have*

$$w(E, \rho) = (-1)^{s_{E,\rho}}. \tag{4.38}$$

Proof. By Lemma 3.4.1 and Proposition 3.4.1, we have $\rho \cong \rho_{\chi_n}$ for some χ_n given in Section 3.2. From the proof of Proposition 4.4.2, since up to isomorphism, ρ_{χ_n} is the only irreducible representation of $Gal(F_n/\mathbb{Q})$ which does not factor through $Gal(K_n L_{n-1}/\mathbb{Q})$, we have

$$X_p(E/F_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p = \left(X_p(E/K_n L_{n-1}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right) \oplus (\rho_{\chi_n})^{s_{E,\rho_{\chi_n}}}.$$

Taking the $Gal(F_n/L_n)$-invariants, and compute their $\bar{\mathbb{Q}}_p$-dimensions, using Proposition 3.4.2, and Greenberg-Guo Theorem 3.3.2, we obtain

$$s_{E,\rho_{\chi_n}} = s_{E/L_n} - s_{E/L_{n-1}} \overset{mod\ 2}{\equiv} \lambda_n - \lambda_{n-1}.$$

Since p is odd, by Proposition 4.4.1, we have

$$\tau \overset{mod\ 2}{\equiv} \lambda_n - \lambda_{n-1}.$$

Therefore from the proof of Theorem 3.3.1 eq(3.15) and eq(3.16), together with Theorem 3.2.1 eq(3.10), we conclude that

$$(-1)^{s_{E,\rho_{\chi_n}}} = (-1)^{\tau} = w(E, \rho_{\chi_n}) \cdot s_p^{dim\rho_{\chi_n}^{I_p}}.$$

The statement follows immediately in the case when $s_p = 1$, that is when E has non-split multiplicative reduction at p. In the case when E has split multiplicative reduction at p, the statement follows by the description of $dim\rho_{\chi_n}^{I_p}$ in Case 2 of Proposition 3.2.2, since under the assumption "$\beta = 0$", $dim\rho_{\chi_n}^{I_p} = 0$ for all $n \geq 1$.

□

4.5 $\Lambda(H_K)$-rank 1 case

In this section, we carry on assuming "$\beta = 0$" when E has split multiplicative reduction at p.

In this very special case when $rank_{\Lambda(H_K)}(Y_p(E/F_\infty)) = 1$, we shall prove that the lower bounds in eq(4.33) and eq(4.36) are precisely the respective p-Selmer ranks.

Theorem 4.5.1. *When $\tau = 1$, we have*

$$s_{E/L_n} = corank_{\mathbb{Z}_p} Sel_p(E/\mathbb{Q}) + n \tag{4.39}$$

and

$$s_{E/F_n} = corank_{\mathbb{Z}_p} Sel_p(E/K) + p^n - 1 \tag{4.40}$$

for $n \geq 1$.

Proof. As the restriction homomorphism

$$Sel_p(E/K) \longrightarrow Sel_p(E/K_\infty)$$

has finite kernel, we have

$$s_{E/K} = corank_{\mathbb{Z}_p} Sel_p(E/K) \leq \lambda_{\Lambda(\Gamma_K)} \left(\widehat{Sel_p(E/K_\infty)} \right).$$

For the same reason,

$$s_{E/F_n} = corank_{\mathbb{Z}_p} Sel_p(E/F_n) \leq \lambda_{\Lambda(\Gamma_{F_n})} \left(\widehat{Sel_p(E/F_n^{cyc})} \right).$$

By the theorem of Greenberg-Guo,

$$s_{E/K} \equiv \lambda_{\Lambda(\Gamma_K)} \left(\widehat{Sel_p(E/K_\infty)} \right) \ mod\ 2.$$

By Proposition 2.5.2 (for $L = K$ and $L = F_n$),

$$\tau = rank_{\Lambda(H_K)}(Y_p(E/F_\infty)) = \lambda_{\Lambda(\Gamma_K)} \left(\widehat{Sel_p(E/K_\infty)} \right) + \sum_{u \in S(K_\infty)} corank_{\mathbb{Z}_p} ker(h_u),$$

$$rank_{\Lambda(H_{F_n})}(Y_p(E/F_\infty)) = \lambda_{\Lambda(\Gamma_{F_n})}\left(\widehat{Sel_p(E/F_n^{cyc})}\right) + \sum_{v_n \in S(F_n^{cyc})} corank_{\mathbb{Z}_p} ker(h_{v_n}).$$

The criterion $\tau = 1$ forces $\lambda_{\Lambda(\Gamma_K)}\left(\widehat{Sel_p(E/K_\infty)}\right) = 0$ or 1. Hence, we have equality

$$s_{E/K} = \lambda_{\Lambda(\Gamma_K)}\left(\widehat{Sel_p(E/K_\infty)}\right) = 0 \text{ or } 1.$$

This again forces

$$\sum_{u \in S(K_\infty)} corank_{\mathbb{Z}_p} ker(h_u) = 1 - s_{E/K} = 1 \text{ or } 0.$$

I now claim that

$$\sum_{u \in S(K_\infty)} corank_{\mathbb{Z}_p} ker(h_u) \equiv \sum_{v_n \in S(F_n^{cyc})} corank_{\mathbb{Z}_p} ker(h_{v_n}) \ mod\ 2.$$

Indeed, since F_n^{cyc}/K_∞ is a Galois extension of degree p^n where p is an odd prime, each $u \in S(K_\infty)$ will only split into an odd number of primes in $S(F_n^{cyc})$. Moreover, the corresponding ramification degree and residue degree are both a power of p. With $p \geq 5$, the reduction type should remain unchanged in this extension. By Proposition 2.3.1 and Theorem 2.4.1, both sums coincide in their parity, and moreover

$$\sum_{u \in S(K_\infty)} corank_{\mathbb{Z}_p} ker(h_u) \leq \sum_{v_n \in S(F_n^{cyc})} corank_{\mathbb{Z}_p} ker(h_{v_n}).$$

On the other hand, since $[\Lambda(H_K) : \Lambda(H_{F_n})] = p^n$,

$$\begin{aligned} rank_{\Lambda(H_{F_n})}\left(Y_p(E/F_\infty)\right) &= p^n \cdot rank_{\Lambda(H_K)}\left(Y_p(E/F_\infty)\right) \\ &= p^n. \end{aligned} \tag{4.41}$$

Hence,

$$\begin{aligned} s_{E/F_n} \leq \lambda_{\Lambda(\Gamma_{F_n})}\left(\widehat{Sel_p(E/F_n^{cyc})}\right) &= p^n - \sum_{v_n \in S(F_n^{cyc})} corank_{\mathbb{Z}_p} ker(h_{v_n}) \\ &\leq p^n - \sum_{u \in S(K_\infty)} corank_{\mathbb{Z}_p} ker(h_u) \\ &= p^n - 1 + s_{E/K}. \end{aligned} \tag{4.42}$$

By eq(4.36), the right hand side is also the lower bound and hence we get the equality

$$s_{E/F_n} = \lambda_{\Lambda(\Gamma_{F_n})}\left(\widehat{Sel_p(E/F_n^{cyc})}\right) = p^n - 1 + s_{E/K}.$$

From the proof of Proposition 4.4.2, we see that when the lower bound eq(4.36) is reached, every intermediate inequality in eq(4.37) is in fact equality. This implies that the value $k_n = 1$, that is $A_{F_n/K_nL_{n-1}} = \rho_{\chi_n}$ for all $n \geq 1$, and the inequalities in eq(4.35) are equalities, except for the right inequality in $n = 1$ case. Hence, we have

$$X_p(E/F_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p = \left(X_p(E/F_{n-1}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right) \oplus \rho_{\chi_n} \tag{4.43}$$

for $n \geq 2$ and

$$X_p(E/F_1) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p = \left(X_p(E/K) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right) \oplus \rho_{\chi_1}. \tag{4.44}$$

Thus,

$$X_p(E/F_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p = \left(X_p(E/K) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right) \oplus \rho_{\chi_1} \oplus \rho_{\chi_2} \oplus \cdots \oplus \rho_{\chi_n}$$

as a decomposition of $Gal(F_n/\mathbb{Q})$-representation. Taking the subspace fixed by subgroup $Gal(F_n/L_n)$, we get

$$X_p(E/L_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p = \left(X_p(E/K) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right)^{Gal(F_n/L_n)} \oplus \rho_{\chi_1}^{Gal(F_n/L_n)} \oplus \rho_{\chi_2}^{Gal(F_n/L_n)} \oplus \cdots \oplus \rho_{\chi_n}^{Gal(F_n/L_n)}.$$

Since the canonical surjection $Gal(F_n/\mathbb{Q}) \longrightarrow Gal(K/\mathbb{Q})$ is still surjective when restricted to subgroup $Gal(F_n/L_n)$, we get

$$\left(X_p(E/K) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right)^{Gal(F_n/L_n)} = \left(X_p(E/K) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p\right)^{Gal(K/\mathbb{Q})} = X_p(E/\mathbb{Q}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p.$$

Counting dimensions, by Proposition 3.4.2, we obtain eq(4.39).

□

Corollary 4.5.1. *When $\tau = 1$, we have*

$$s_{E/K_{n'}L_n} = s_{E/F_n} = p^n - 1 + s_{E/K} \tag{4.45}$$

for all $n' \geq n \geq 1$, and

$$s_{E/K_{n'}} = s_{E/K} \tag{4.46}$$

for $n' \geq 1$. In particular, in this case, we have the following refinements of Greenberg-Guo:

$$\lambda_{\Lambda(\Gamma_K)}\left(\widehat{Sel_p(E/K_\infty)}\right) = s_{E/K} = 0 \ \text{ or } \ 1 \tag{4.47}$$

and

$$\lambda_{\Lambda(\Gamma_{F_n})}\left(\widehat{Sel_p(E/F_n^{cyc})}\right) = s_{E/F_n} \tag{4.48}$$

for $n \geq 1$.

Proof. In the proof of the theorem above, we showed that the inequalities in eq(4.35) are equalities, namely we have

$$X_p(E/K_{j+1}L_j)\otimes_{\mathbb{Z}_p}\bar{\mathbb{Q}}_p = X_p(E/F_j)\otimes_{\mathbb{Z}_p}\bar{\mathbb{Q}}_p = \left(X_p(E/K_{j+1}L_j)\otimes_{\mathbb{Z}_p}\bar{\mathbb{Q}}_p\right)^{Gal(K_{j+1}L_j/K_jL_j)} \tag{4.49}$$

for all $j \geq 1$.
Since

$$Gal(K_{j+1}L_j/K_{j+1}L_n) \cong Gal(K_jL_j/K_jL_n)$$

for all $j \geq n$, taking the $Gal(K_{j+1}L_j/K_{j+1}L_n)$-invariant of eq(4.49), we get

$$X_p(E/K_{j+1}L_n)\otimes_{\mathbb{Z}_p}\bar{\mathbb{Q}}_p = X_p(E/K_jL_n)\otimes_{\mathbb{Z}_p}\bar{\mathbb{Q}}_p. \tag{4.50}$$

When j runs over $n, n+1, \cdots, n'-1$ we get

$$X_p(E/K_{n'}L_n)\otimes_{\mathbb{Z}_p}\bar{\mathbb{Q}}_p = X_p(E/K_nL_n)\otimes_{\mathbb{Z}_p}\bar{\mathbb{Q}}_p, \tag{4.51}$$

hence proved eq(4.45).
Since $Gal(K_{n'}L_1/K_{n'}) \cong Gal(KL_1/K)$, eq(4.46) is just the $Gal(K_{n'}L_1/K_{n'})$-invariant of eq(4.51) in $n = 1$ case.
The refinements of Greenberg-Guo are true because both K and F_n contain μ_p and hence

$$F_n^{cyc} = \bigcup_{n'\geq n} K_{n'}L_n$$

and

$$K_\infty = K^{cyc} = \bigcup_{n'\geq 1} K_{n'}.$$

□

It is never easy to find the generators of the Mordell-Weil group of an elliptic curve over a number field. However, in each of the following two examples of our kind (E, p, m), I managed to obtain a rational point of infinite order over the number field $\mathbb{Q}(\sqrt[p]{m})$, by using the Pari-GP package ell.gp, by Denis Simon [27]. The level of computation becomes much more complicated and massive in the process to go on to number field $\mathbb{Q}(\sqrt[p^2]{m})$, over which we expect to reach extra rank.

Example 1 The elliptic curve 70A1 in Cremona's Table has Weierstrass equation

$$E : y^2 + xy + y = x^3 - x^2 + 2x - 3 \tag{4.52}$$

It has split multiplicative reduction at 2 and non-split multiplicative reduction at 5 and 7. This elliptic curve E has Mordell-Weil rank 0 over $\mathbb{Q}$. Taking triple $(E, p, m) = (70A1, 5, 2)$ in our setting, then $K := \mathbb{Q}(\mu_5)$ and $L_1 := \mathbb{Q}(\theta)$ with $\theta = \sqrt[5]{2}$.

$$P := (4\theta^4 - 2\theta^3 + \theta^2 + 2\theta - 5, -3\theta^4 - 6\theta^3 + 17\theta^2 - 20\theta + 17) \tag{4.53}$$

is a rational point on E over L_1, with height $\simeq 1.5505$ hence is a point of infinite order in $E(L_1)$. This indeed matches the prediction by our theorems, which tell the Mordell-Weil rank of E over L_1 is 1.
In fact $L(E/K, 1) \neq 0$ hence assuming Birch and Swinnerton-Dyer Conjecture, E has Mordell-Weil rank over K, $r_{E(K)} = 0$. Applying J.Jones' formula [14, Theorem 1], we know that (since 5 is the only prime ramified (totally) over $K^{cyc}/\mathbb{Q}$, hence $e \stackrel{\text{def}}{=}$ the number of split multiplicative reduction primes of K which ramifies in K^{cyc}/K is equal to 0.) $R_{E/K}$, the order of vanishing at $T = 0$ of the characteristic polynomial of $Sel_5(E/K^{cyc})$ is $\geq r_{E(K)}$. Moreover, up to multiplication by a 5-adic unit, the coefficient of the $T^{r_{E(K)}}$ term in the characteristic polynomial of $Sel_5(E/K^{cyc})$ is equal to

$$\prod_{v \nmid \infty} m_v \cdot \frac{|Ш(E/K)(p)|}{|E(K)(p)|^2} \tag{4.54}$$

The product of the Tamagawa numbers $\prod_{v \nmid \infty} m_v = 8$, the torsion part of $E(K)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and by assuming Birch and Swinnerton-Dyer Conjecture of the leading coefficient of the complex L-series of E over K at $s = 1$

in terms of the product involving the order of $Ш(E/K)$, we obtain conjecturally that $Ш(E/K)$ is a trivial group. Hence, the product in (4.54) should be itself a 5-adic unit. Consequently, the coefficient of the $T^{r_{E(K)}}$ term in the characteristic polynomial of $Sel_5(E/K^{cyc})$ should be a 5-adic unit and this forces

$$\mu(X_5(E/K^{cyc})) = 0 \text{ and } \lambda(X_5(E/K^{cyc})) = r_{E(K)} = 0.$$

Since the prime $m = 2$ is inert over K^{cyc} and E has split multiplicative reduction at 2, by the third case of Proposition 2.3.1, together with eq(2.7) and Proposition 2.5.2 for $L = K$, we have

$$rank_{\Lambda(H_K)} Y_5(E/F_\infty) = 1. \tag{4.55}$$

So the prediction of the 5-Selmer rank of E over L_1 by first assertion of Theorem 4.5.1 coincides the Mordell-Weil rank of E over L_1, i.e $s_{E/L_1} = r_{E(L_1)} = 1$. Hence proved in this case that the 5-part of the $Ш(E/L_1)$ is finite.

Example 2 The elliptic curve 30A1 in Cremona's Table has Weierstrass equation

$$E : y^2 + xy + y = x^3 + x + 23 \tag{4.56}$$

It has split multiplicative reduction at 3 and non-split multiplicative reduction at 2 and 5. This elliptic curve E has Mordell-Weil rank 0 over $\mathbb{Q}$. Taking triple $(E, p, m) = (30A1, 5, 3)$ in our setting, then $K := \mathbb{Q}(\mu_5)$ and $L_1 := \mathbb{Q}(\theta)$ with $\theta = \sqrt[5]{3}$.

$$P := (2\theta^4 - 2\theta^3 + 2\theta^2 - 3, 4\theta^4 - 6\theta^2 + 12\theta - 14) \tag{4.57}$$

is a rational point on E over L_1, with height $\simeq 0.5749$ hence is a point of infinite order in $E(L_1)$. This indeed matches the prediction by our theorems, which tell the Mordell-Weil rank of E over L_1 is 1.

In fact $L(E/K, 1) \neq 0$ hence assuming Birch and Swinnerton-Dyer Conjecture, E has Mordell-Weil rank over K, $r_{E(K)} = 0$. Applying J.Jones' formula [14, Theorem 1], we know that (since 5 is the only prime ramified (totally) over $K^{cyc}/\mathbb{Q}$, hence $e \stackrel{\text{def}}{=}$ the number of split multiplicative reduction primes of K which ramifies in K^{cyc}/K is equal to 0.) $R_{E/K}$, the order of vanishing at $T = 0$ of the characteristic polynomial of $Sel_5(E/K^{cyc})$ is $\geq r_{E(K)}$. Moreover, up to mul-

tiplication by a 5-adic unit, the coefficient of the $T^{r_{E(K)}}$ term in the characteristic polynomial of $Sel_5(E/K^{cyc})$ is equal to

$$\prod_{v\nmid\infty} m_v \cdot \frac{|Ш(E/K)(p)|}{|E(K)(p)|^2} \tag{4.58}$$

The product of the Tamagawa numbers $\prod_{v\nmid\infty} m_v = 24$, the torsion part of $E(K)$ is isomorphic to $\mathbb{Z}/12\mathbb{Z}$ and by assuming Birch and Swinnerton-Dyer Conjecture of the leading coefficient of the complex L-series of E over K at $s = 1$ in terms of the product involving the order of $Ш(E/K)$, we obtain conjecturally that $Ш(E/K)$ is a trivial group. Hence, the product in (4.58) should be itself a 5-adic unit. Consequently, the coefficient of the $T^{r_{E(K)}}$ term in the characteristic polynomial of $Sel_5(E/K^{cyc})$ should be a 5-adic unit and this forces

$$\mu(X_5(E/K^{cyc})) = 0 \text{ and } \lambda(X_5(E/K^{cyc})) = r_{E(K)} = 0.$$

Since the prime $m = 3$ is inert over K^{cyc} and E has split multiplicative reduction at 3, by the third case of Proposition 2.3.1, together with (2.7) and Proposition 2.5.2 for $L = K$, we have

$$rank_{\Lambda(H_K)} Y_5(E/F_\infty) = 1. \tag{4.59}$$

So the prediction of the 5-Selmer rank of E over L_1 by first assertion of Theorem 4.5.1 coincides the Mordell-Weil rank of E over L_1, i.e $s_{E/L_1} = r_{E(L_1)} = 1$. Hence proved in this case that the 5-part of the $Ш(E/L_1)$ is finite.

Remark:. *I apply [14, Theorem 1] in the case L/K replaced by K^{cyc}/K. Hence, e takes value 1 when E has a split multiplicative reduction at p and takes value 0 when E has a non-split multiplicative reduction at p. Let r denote the Mordell-Weil rank of E over K. Jones defines for each discrete $\Lambda(\Gamma_K)$-module with its Pontryagin dual a compact finitely generated $\Lambda(\Gamma_K)$-torsion module, an Iwasawa L-function $L(G;s) \overset{def}{=} F_G(\omega^{1-s} - 1)$, for some $\omega \in \mathbb{Z}_p^\times$, where $F_G(T)$ denotes the characteristic element of the Pontryagin dual of G. Let $G_2 \overset{def}{=} H^1(spec(\mathcal{O}_{K^{cyc}}), E^0_{p^\infty})$ and $G_1 \overset{def}{=} H^1(spec(\mathcal{O}_{K^{cyc}}), E_{p^\infty})$ be the fpqf cohomology groups, where we let E denote its Neron model over $\mathcal{O}_{K^{cyc}}$, and by E^0 its connected component. This G_1 is the flat Selmer group defined by Jones, which*

he also proves to be quasi-isomorphic to Greenberg Selmer group and therefore $F_{G_1}(T) = T^e \times F_{G_3}(T)$, *where* $G_3 \stackrel{def}{=} Sel_p(E/K^{cyc})$ *is the classical Selmer group. Jones shows that* $F_{G_2}(T) = F_{G_1}(T)$ *and hence* $L(G_2; s) = L(G_1; s)$. *This theorem [14, Theorem 1] asserts that the Iwasawa L-function* $L(G_2; s)$ *has zero of order at least* $r + e$ *at* $s = 1$, *and the corresponding* $(r + e)$*-th coefficient is up to multiplication by a p-adic unit, given by a product involving some local invariants, Schneider's p-adic height regulator and the p-primary part of* $Ш(E/K)$ *and* $E(K)$. *From the construction of the Iwasawa L-function, it is clear by simple calculus that* $L(G_3; s)$ *has zero of order at least r at* $s = 1$, *and the corresponding r-th coefficient is up to multiplication by a p-adic unit, given by the same product given above. The computations in the two examples above are due to this final statement.*

Remark:. *There are a lot more similar examples* (E, p, m) *which conjecturally have* $rank_{\Lambda(H_K)} Y_p(E/F_\infty) = 1$. *However, the two examples above are the only ones among these of which 'ell.gp' returns a rational point of infinite order over* $\mathbb{Q}(\sqrt[p]{m})$.

In a forthcoming paper, I will further discuss the case left out by the restriction "$\beta = 0$*", which is when E has split multiplicative reduction at p but* $p^{r+1} \parallel m^{p-1} - 1$ *with a positive integer r. I will describe the growth of the Selmer ranks within the False Tate curve tower in this case which would be slightly different from the relevant results in Chapter 4. However, I will prove the validity of Theorem 4.4.1 with the assumption "*$\beta = 0$*" dropped.*

Bibliography

[1] P. N. Balister and S. Howson. Note on Nakayama's lemma for compact Λ*-modules.* Asian J. Math.*, 1(2):224–229, 1997.*

[2] H. Bass. Algebraic K-theory. *W. A. Benjamin, Inc., New York-Amsterdam, 1968.*

[3] J. Coates, T. Fukaya, K. Kato, and R. Sujatha. Root numbers, Selmer groups, and non-commutative Iwasawa theory. J. Algebraic Geom.*, 19(1):19–97, 2010.*

[4] J. Coates, T. Fukaya, K. Kato, R. Sujatha, and O. Venjakob. The GL_2 *main conjecture for elliptic curves without complex multiplication.* Publ. Math. Inst. Hautes Études Sci.*, (101):163–208, 2005.*

[5] J. Coates and R. Greenberg. Kummer theory for abelian varieties over local fields. Invent. Math.*, 124(1-3):129–174, 1996.*

[6] P. Deligne. Les constantes des équations fonctionnelles des fonctions L. In Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.*

[7] T. Dokchitser and V. Dokchitser. Self-duality of Selmer groups. Math. Proc. Cambridge Philos. Soc.*, 146(2):257–267, 2009.*

[8] V. Dokchitser. Root numbers of non-abelian twists of elliptic curves. Proc. London Math. Soc.*, 3(91):300–324, 2005.*

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

[10] L. Guo. On a generalization of Tate dualities with application to Iwasawa theory. Compositio Math.*, 85(2):125–161, 1993.*

[11] Y. Hachimori and K. Matsuno. An analogue of kida's formula for selmer groups of elliptic curves. J. Algebraic Geom.*, 8:581–601, 1999.*

[12] Y. Hachimori and O. Venjakob. Completely faithful selmer groups over kummer extensions. Doc. Math. Extra Volume: Kazuya Kato's Fiftieth Birthday*, pages 443–478, 2003.*

[13] S. Howson. Euler characteristics as invariants of Iwasawa modules. Proc. London Math. Soc. (3)*, 85(3):634–658, 2002.*

*[14] J. Jones. Iwasawa L-functions and the mysterious -invariant. In p-*adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, volume 165 of* Contemp. Math.*, pages 63–70. Amer. Math. Soc., Providence, RI, 1994.*

[15] G. T. Konovalov. The universal G-norms of formal groups over a local field. Ukrain. Mat. Ž.*, 28(3):399–401, 431, 1976.*

[16] T. Y. Lam. Lectures on modules and rings*, volume 189 of* Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.*

[17] R.P. Langlands. On the functional equation of artin l-functions. Yale University Lecture note., 1970.

[18] M. Lazard. Groupes analytiques p-adiques. Publ. Math. Inst. Hautes Études Sci.*, 26:389–603, 1965.*

[19] J. Manin. Cyclotomic fields and modular curves. Russian Mathematical Surveys*, 26:7–78, 1971.*

[20] B. Mazur. Rational points of abelian varieties with values in towers of number fields. Inventiones math*, 18:183–266, 1972.*

[21] L. Ribes and P. Zalesskii. Profinite groups*, volume 40 of* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, 2000.*

[22] *K. Ribet. Torsion points of abelian varieties in cyclotomic extensions.* Lenseignement Mathematique*, 27:315–319, 1981.*

[23] *D. E. Rohrlich. Elliptic curves and the Weil-Deligne group. In* Elliptic curves and related topics*, volume 4 of* CRM Proc. Lecture Notes*, pages 125–157. Amer. Math. Soc., Providence, RI, 1994.*

[24] *P. Schneider. p-adic height pairings. II.* Invent. Math.*, 79(2):329–374, 1985.*

[25] *J-P. Serre. Sur la dimension cohomologique des groupes profinis.* Topology*, 3:413–420, 1965.*

[26] *J-P. Serre.* Linear representations of finite groups*, volume 42 of* Graduate Texts in Mathematics*. Springer, New York-Heidelberg, 1977.*

[27] *D. Simon. Computing the rank of elliptic curves over number fields.* LMS J. Comput. Math.*, 5:7–17 (electronic), 2002.*

[28] *F. Viviani. Ramification groups and Artin conductors of radical extensions of* $\mathbb{Q}$*.* J. Théor. Nombres Bordeaux*, 16(3):779–816, 2004.*

[29] *L. C. Washington.* Introduction to cyclotomic fields*, volume 83 of* Graduate Texts in Mathematics*. Springer, New York, 2nd edition, 1997.*