Iwasawa Theory of Fine Selmer Groups

by

Debanjana Kundu

A thesis submitted in conformity with the requirements
for the degree of Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto

Abstract

Iwasawa Theory of Fine Selmer Groups

Debanjana Kundu
Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto
2020

Iwasawa theory began as a Galois module theory of ideal class groups, initiated by Kenkichi Iwasawa as part of the theory of cyclotomic fields. In the early 1970s, Barry Mazur considered generalizations of Iwasawa theory to Selmer groups of elliptic curves (Abelian varieties in general). At the turn of this century, Coates and Sujatha initiated the study of a subgroup of the Selmer group of an elliptic curve called the *fine* Selmer group.

The focus of this thesis is to understand arithmetic properties of this subgroup. In particular, we understand the structure of fine Selmer groups and their growth patterns. We investigate a strong analogy between the growth of the p-rank of the fine Selmer group and the growth of the p-rank of the class groups. This is done in the classical Iwasawa theoretic setting of (multiple) $\mathbb{Z}_p$-extensions; but what is more striking is that this analogy can be extended to non-p-adic analytic extensions as well, where standard Iwasawa theoretic tools fail.

We provide new evidence towards the two conjectures on the structure of the fine Selmer groups proposed by Coates and Sujatha. Conjecture A is viewed as a generalization of the classical Iwasawa $\mu = 0$ conjecture to the context of the motive associated to an elliptic curve; whereas Conjecture B is in the spirit of generalising Greenberg's pseudonullity conjecture to elliptic curves.

Acknowledgements

1. Bubs and Ma
2. Kumar
3. Sujatha
4. Steve and Jim
5. Jonathan, Joe Repka, Dror, and Sarah
6. Arul, Jacob, and Ila
7. Arthur Packet
8. GANITA folks: past and present
9. Asif, Erick, Zack Wolske, Abhishek, Heejong, Roy Magen, Kenneth Chiu, Ali Cheraghi
10. Jemima + Everyone else in the Math Office
11. Greenberg, Coates, Nguyen Quang Do, Antonio Lei, Preston Wake, Ahmed Matar, Kestutis, Soren Kleine, Andrea Bandini, Meng Fai, Ashay Burungale, Christian Wuthrich, Sudhanshu Shekhar, Aribam, Somnath Jha, Anwesh
12. Matilde Lalin, Ali Altug, Bianca Viray
13. Wanlin Li, Soumya Sankar, Alyssa Lumley
14. Kapil and Passi
15. Pishi, Mashimoni, Mesho, and the boys
16. Nidhi, Vibhav, Rahul

Contents

Chapter 1

Introduction

Iwasawa Theory is an area of number theory that emerged out of the foundational work of Kenkichi Iwasawa in the 1950s [47]. It has its origins in the following (at first counter-intuitive) insight of Iwasawa: instead of trying to understand the structure of a *particular* Galois module, it is often easier to describe *every* Galois module in an infinite tower of number fields at once. It was inspired by Weil's theory of the characteristic polynomial of Frobenius acting on the Jacobian of a curve over a finite field. The primary question in classical Iwasawa theory is to study the growth of arithmetic objects in infinite towers. It began as a Galois module theory of ideal class groups and was then generalized to Selmer groups of Abelian varieties by Mazur [66]. More recently, Greenberg proposed an Iwasawa theory for motives [38].

A key observation is that growth of Galois modules in certain towers exhibits remarkable regularity. This can be described in terms of values of L-functions, such as the Riemann ζ function. Hence, Iwasawa theory truly unveils intricate links between algebraic, geometric, and analytic objects.

The foundations of the subject were laid way back in the mid 19th century with Kummer's work on Fermat's Last Theorem and reciprocity laws. Kummer discovered that special values of the Riemann ζ function have remarkable arithmetic properties. In particular, the class number of $\mathbb{Q}(\zeta_p)$ is divisible by p if and only if $p \mid \zeta(n)$ for some negative odd integer $n \geq 4-p$. Such primes p are called *irregular*. He showed that for all regular primes p, $x^p + y^p = z^p$ has no non-trivial integral solutions. In a way, Kummer showed that the ideal class group is both a "bitter" and a "sweet" group at the same time. While it is an obstruction to the study of arithmetic of number fields, it is closely related to zeta values. Another mysterious relationship between ζ functions and the ideal class group is the analytic class number formula which was also proved in the mid 19th century by Dedekind and Dirichlet.

After Kubota and Leopoldt introduced p-adic L-functions, Iwasawa interpreted them in terms of $\mathbb{Z}_p$-extensions [48]. The link between the analytic and the algebraic worlds is provided by the *Main Conjecture* which states that the p-adic L-functions are essentially the characteristic power series of certain Galois actions arising in the theory of $\mathbb{Z}_p$-extensions. Using the theory of modular forms, Mazur and Wiles proved the first case of this deep connection [68]. In [86], Rubin provided a proof based on the technically complex machinery of Euler systems developed by Kolyvagin.

In the setting of elliptic curves, the arithmetic objects that replace class groups are the Selmer groups. For an elliptic curve defined over a number field F, its Mordell-Weil group $E(F)$ of F-rational points of the elliptic curve is a finitely generated group. The Selmer group intertwines the Mordell-Weil group and the mysterious, conjecturally finite Shafarevich-Tate group. This intertwining is reflected in analytic formulae. Given $E/\mathbb{Q}$, one constructs an L-series from the data of the number of $\mathbb{F}_p$-points of the mod p reductions of E. By the modularity of rational elliptic curves, this L-series has analytic continuation. The *Birch and Swinnerton-Dyer Conjecture* (BSD) equates the order of vanishing of the L-function $L(E,\ s)$ at $s = 1$ to the rank of $E(\mathbb{Q})$. Much of the progress towards this conjecture uses Iwasawa theory. The first major theoretical evidence towards BSD was due to Coates and Wiles [24]; they proved that if the order of vanishing of the L-function associated to elliptic curves with complex multiplication over an imaginary quadratic field of class number 1 is zero, then the rational Mordell-Weil group is finite.

For elliptic curves with good ordinary reduction at p, Mazur and Swinnerton-Dyer constructed p-adic L-functions $L_p(E,\ s)$ interpolating values of $L(E,\ s)$ up to Euler factors. Mazur formulated an analogous Main Conjecture in this setting. For elliptic curves with complex multiplication, this is equivalent to the Main Conjecture for imaginary quadratic fields proven by Rubin. One direction of the elliptic curve Main Conjecture was proven by Kato employing the method of Euler systems [54]; the other direction was proven by Skinner and Urban under mild hypothesis using Galois representations attached to automorphic forms [99]. The Main Conjecture for elliptic curves implies a p-adic analogue of BSD that relates the rank of the rational Mordell-Weil group to the order of vanishing of $L_p(E,\ s)$ at $s = 1$.

In the early 2000's, Iwasawa theory over towers of number fields with Galois groups isomorphic to subgroups of $\mathrm{GL}_n(\mathbb{Z}_p)$ was developed. A major breakthrough was the non-commutative Main Conjecture for elliptic curves by Coates, Fukaya, Kato, Sujatha, and Venjakob [16]. The invariants playing the roles of characteristic ideals and p-adic L-functions lie in a first K-group of a localization of the non-commutative Iwasawa algebra. In the intervening two decades, significant progress has been made in this direction by the work of Burns, Kakde, and Ritter and Weiss [10], [53], [84].

Fine Selmer Groups

The focus of this thesis is to understand arithmetic properties of a subgroup of the Selmer group, called the *fine Selmer group*. This is defined by imposing stricter restriction conditions on the elements of the classical Selmer group at all places above p. This subgroup plays a key role in the formulation of the Main Conjecture in Iwasawa theory. A detailed study of the fine Selmer group was first undertaken by Coates and Sujatha [22]. The authors proposed that in a $\mathbb{Z}_p$-extension, the right analogue of the ideal class group is not the classical Selmer group, but instead it is the fine Selmer group.

The underlying theme of this thesis is to understand the structure of fine Selmer groups and their growth patterns. We investigate a strong analogy between the growth of the p-rank of the fine Selmer group and the growth of the p-rank of the class groups. This is done in the classical Iwasawa theoretic setting of (multiple) $\mathbb{Z}_p$-extensions; but what is more striking is that this analogy can be extended to non-p-adic analytic extensions as well, where standard Iwasawa theoretic tools fail.

We provide new evidence towards the two conjectures on the structure of the fine Selmer groups proposed by Coates and Sujatha [22]. Conjecture A is viewed as a generalization of the classical Iwasawa $\mu = 0$ conjecture to the context of the motive associated to an elliptic curve; whereas Conjecture B is in the spirit of generalising Greenberg's pseudonullity conjecture to elliptic curves [35]. These conjectures have been generalised to fine Selmer groups of ordinary Galois representations associated to modular forms [52]. In this thesis, we restrict our attention to fine Selmer groups of Abelian varieties, often elliptic curves with good reduction at a prime p, over p-adic Lie extensions of the base field. However, many of the results easily generalise to the case of ordinary Galois representations.

Organization of this Thesis:

Chapter 2 is expository in nature. We introduce the key definitions and results which will be required throughout the thesis. In Chapter 3, we investigate the strong finiteness properties of the fine Selmer group. Exploiting techniques used by Lim and Murty in [59] and [60], we study the growth of the fine Selmer group (and fine Shafarevich-Tate groups) in different situations. In Chapter 4, we prove a Riemann-Hurwitz type formula for λ-invariants of fine Selmer groups. In Chapter 5, we provide new evidence for Conjecture A and establish isogeny invariance in previously unknown cases. In Chapter 6, we investigate Conjecture B. Even though Conjecture B was proposed as a generalization of the Generalized Greenberg's Conjecture, the precise formulation of this relationship is rather intricate. This connection is made explicit using the Powerful Diagram. We also provide unconditional evidence towards this conjecture in a large number of cases. The results in the final chapter are joint work with R. Sujatha.

Chapter 2

Background

This chapter is expository in nature. We introduce the objects of study and give a detailed background of the theory of modules over an Iwasawa algebra which is crucial for the study of Iwasawa theory. We also discuss some aspects of non-commutative Iwasawa theory. In the final section, we briefly mention some technical tools that are required in the study of Iwasawa theory.

2.1 Classical Iwasawa Theory

Fix a prime p and a number field F. A **$\mathbb{Z}_p$-extension F_∞** of F is one where the corresponding Galois group $\Gamma = \mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}_p$, the additive group of p-adic integers. Such an extension is visualized as a tower of number fields

$$F = F_0 \subset F_1 \ldots \subset F_n \ldots \subset F_\infty = \bigcup_n F_n$$

with each $\mathrm{Gal}(F_n/F) \simeq \mathbb{Z}/p^n\mathbb{Z}$. To see this, note that the non-trivial closed subgroups of Γ are of the form Γ^{p^n} for $n \geq 0$ and are denoted by Γ_n. These $\{\Gamma_n\}_n$ form a descending sequence with $\Gamma/\Gamma_n \simeq \mathbb{Z}/p^n\mathbb{Z}$. With $F_n = F_\infty^{\Gamma_n}$, we obtain the above tower.

Every number field has *at least* one $\mathbb{Z}_p$-extension, i.e. the cyclotomic $\mathbb{Z}_p$-extension, which is a subfield of $F(\mu_{p^\infty})$. Indeed, consider the canonical homomorphism

$$\begin{aligned} \chi : \mathrm{Gal}\big(F(\mu_{p^\infty})/F\big) &\to \mathbb{Z}_p^\times \\ \sigma &\mapsto \chi(\sigma) = u. \end{aligned}$$

Let ζ_{p^n} be a primitive p^n-th root of unity, then $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{u_n}$ with $u_n \in \mathbb{Z}$ and $\gcd(u_n, p) = 1$. This sequence of $\{u_n\}_n$ is a Cauchy sequence in $\mathbb{Z}_p$ and converges to a well-defined element $u \in \mathbb{Z}_p^\times$. For all $\zeta \in \mu_{p^\infty}$, it follows that $\sigma(\zeta) = \zeta^{\chi(\sigma)}$. χ is a continuous and injective homomorphism with image of finite index in $\mathbb{Z}_p^\times$. The p-adic logarithm gives the isomorphism

$$\begin{aligned} \mathbb{Z}_p^\times &\simeq \big(\mathbb{Z}/p\mathbb{Z}\big)^\times \times \mathbb{Z}_p && \text{for } p \neq 2 \\ \mathbb{Z}_2^\times &\simeq \{\pm 1\} \times \mathbb{Z}_2 && \text{for } p = 2. \end{aligned}$$

Therefore $\mathrm{Im}(\chi) \simeq \Delta \times \Gamma$ with Δ a finite group and $\Gamma \simeq \mathbb{Z}_p$. This proves there exists a *unique* subfield F_{cyc} of $F(\mu_{p^\infty})$ such that $\mathrm{Gal}(F_{\mathrm{cyc}}/F) \simeq \Gamma \simeq \mathbb{Z}_p$. This is the **cyclotomic** $\mathbb{Z}_p$-extension of F.

Let $\widetilde{F}/F$ denote the compositum of *all* $\mathbb{Z}_p$-extensions of F. By idelic class field theory, it follows

$$\mathrm{Gal}(\widetilde{F}/F) \simeq \mathbb{Z}_p^d \tag{2.1}$$

where $r_2 + 1 \leq d \leq [F : \mathbb{Q}]$. Thus, for a number field which is not totally real, there are *infinitely* many $\mathbb{Z}_p$-extensions. The **Leopoldt Conjecture** asserts $d = r_2 + 1$. This would imply that for a totally real field there is precisely *one* $\mathbb{Z}_p$-extension, namely the one constructed above.

In 1959, Iwasawa proved the following result on the growth of the orders of p-parts of the class groups of the fields F_n [47].

Theorem 2.1.1. *Consider a $\mathbb{Z}_p$-extension F_∞/F. Let A_n denote the p-part of the class group of F_n. There exist non-negative integers λ, μ and an integer ν such that for $n \gg 0$,*

$$|A_n| = p^{\mu p^n + \lambda n + \nu}.$$

In the same paper, Iwasawa made the following conjecture.

Classical $\mu = 0$ Conjecture. *For $F_\infty = F_{\mathrm{cyc}}$, $\mu = 0$.*

This is known for Abelian number fields by the work of Ferrero-Washington [30]. In 1984, Sinnott proved the same using p-adic L-functions [98].

Idea of Proof of Iwasawa's Theorem. The proof hinges on studying the Galois group $X := \mathrm{Gal}(L_\infty/F_\infty)$ where $L_\infty = \bigcup_n L_n$ and L_n is the maximal Abelian unramified p-extension of F_n, i.e. its p-Hilbert class field. The inverse limit of Artin isomorphisms identifies X with $\varprojlim_n A_n$. By class field theory, $[L_n : F_n] = p^{e_n}$ is finite. The Galois extension $\mathrm{Gal}(L_\infty/F)$ fits into the short exact sequence

$$0 \to X \to \mathrm{Gal}(L_\infty/F) \to \Gamma \to 0.$$

First, X is a compact $\mathbb{Z}_p$-module because it is a projective limit of finite Abelian p-groups. There is also a natural action of Γ on $\varprojlim_n A_n$ and via the Artin isomorphism it can be identified with the conjugation action of Γ on X. This gives X a rich structure of a module over the Iwasawa algebra; this structure allows the study of the growth of $[L_n : F_n]$, giving the precise formula. ☕

2.1.1 Modules over the Iwasawa Algebra

The **Iwasawa algebra** $\Lambda(G)$ of a profinite group G is a variation of the group ring of G with p-adic coefficients taking into account the topology of G. More precisely,

$$\Lambda(G) := \varprojlim \mathbb{Z}_p[G/H]$$

where H runs over the open normal subgroups of G and the inverse limit is taken with respect to natural projection maps. For now, the focus is on commutative Iwasawa algebras. We choose $G = \Gamma \simeq \mathbb{Z}_p$. Their non-commutative analogues were introduced by Lazard and will be discussed in brief in Section 2.4.

Fix a topological generator γ of Γ; it is an element that generates a dense subgroup of Γ. The isomorphism $\mathbb{Z}_p \simeq \Gamma$ is given by $x \mapsto \gamma^x$. Serre proved that the Iwasawa algebra is isomorphic to a power series in one variable. More precisely,

$$\begin{aligned}\Lambda(\Gamma) &\xrightarrow{\sim} \mathbb{Z}_p[\![T]\!]\\ \gamma - 1 &\mapsto T\end{aligned}$$

This Iwasawa algebra is a Noetherian ring. If $f(T) = \sum_{i\geq 0} \alpha_i T^i$ is an element of the Iwasawa algebra, it is invertible if and only if $\alpha_0 \in \mathbb{Z}_p^{\times}$. This makes the Iwasawa algebra a local ring with maximal ideal $\mathfrak{m} = (p,\, T)$. This gives us a powerful tool from commutative algebra, namely the *Nakayama's Lemma* (see Section A.1.1). Since $\Lambda(\Gamma)/\mathfrak{m}^k$ is finite for all positive k, the Iwasawa algebra is viewed as a topological ring by giving it the $\mathfrak{m}$-adic topology. Moreover, it is compact because $\Lambda(\Gamma) \simeq \varprojlim \Lambda(\Gamma)/\mathfrak{m}^k$.

$\Lambda(\Gamma)$ is not a Principal Ideal Domain (PID). However, the structure theory of *finitely generated* modules over $\Lambda(\Gamma)$ is similar to that of finitely generated modules over a PID, provided these $\Lambda(\Gamma)$-modules are defined up to finite submodules and quotient modules.

A homomorphism $\theta : M \to N$ of finitely generated $\Lambda(\Gamma)$ modules is called a **pseudo-isomorphism** if both its kernel and cokernel are finite. This notion gives an equivalence relation on *any* set of finitely generated, *torsion* $\Lambda(\Gamma)$-modules.

Theorem 2.1.2 (Structure Theorem). *For any finitely generated, torsion $\Lambda(\Gamma)$-module M, there is a pseudo-isomorphism*

$$M \to \bigoplus_{i=1}^{s} {}^{\Lambda(\Gamma)}\Big/_{(p^{m_i})} \oplus \bigoplus_{j=1}^{t} {}^{\Lambda(\Gamma)}\Big/_{\left(f_j^{l_j}\right)}$$

where $s,\ t$ are finite, $m_i,\ l_j > 0$ and each f_j is a distinguished polynomial (i.e. a monic irreducible polynomial in $\mathbb{Z}_p[T]$ such that $f_j \equiv T^{\deg f_j} \mod p$).

In the notation of the theorem, set

$$\mu(M) = \sum_{i=1}^{s} m_i, \qquad \lambda(M) = \sum_{j=1}^{t} l_j \deg f_j.$$

To each M, it is also possible to associate its annihilator, called the **characteristic ideal**

$$\operatorname{char}(M) = \left(p^{\mu}(M) \prod_{j=1}^{t} f_j^{l_j}\right).$$

Remark 2.1.3. Recall from the proof of Theorem 2.1.1: the conjugation action of Γ on $X \simeq \varprojlim_n A_n$ makes it a (compact) $\Lambda(\Gamma)$-module. It is called the unramified **Iwasawa module** and is a finitely generated torsion $\Lambda(\Gamma)$-module. In this case, $\lambda = \lambda(X)$ and $\mu = \mu(X)$ are as in the theorem.

2.1.2 Pseudo-nullity

We return to the situation considered in Equation 2.1. Let $\widetilde{F}$ be the compositum of all $\mathbb{Z}_p$-extensions of F. Pick a set of topological generators $\{\gamma_i\}_{i=1}^{d}$ of $\Gamma_d = \mathrm{Gal}(\widetilde{F}/F) \simeq \mathbb{Z}_p^d$. The maps $\gamma_i - 1 \mapsto T_i$ for each $1 \leq i \leq d$ extend to a $\mathbb{Z}_p$-algebra isomorphism

$$\Lambda(\Gamma_d) = \mathbb{Z}_p[\![\Gamma_d]\!] \xrightarrow{\sim} \mathbb{Z}_p[\![T_1, \ldots, T_d]\!].$$

As before, $\Lambda(\Gamma_d)$ is a complete regular local domain of dimension $d+1$. In particular, it is a Unique Factorization Domain (UFD). Consider the maximal Abelian unramified p-extension $\widetilde{L}$ of $\widetilde{F}$ and set $\widetilde{X} = \operatorname{Gal}(\widetilde{L}/\widetilde{F})$. $\widetilde{X}$ can be viewed as a $\mathbb{Z}_p$-module by the natural action of Γ_d. In [34], Greenberg proved that $\widetilde{X}$ is a Noetherian torsion $\Lambda(\Gamma_d)$-module.

Definition 2.1.4. *A finitely generated, torsion $\Lambda(\Gamma_d)$-module M is* ***pseudo-null*** *if its annihilator $\operatorname{Ann}_{\Lambda(\Gamma_d)}(M)$ has height atleast 2. Equivalently, $\operatorname{Ann}_{\Lambda(\Gamma_d)}(M)$ is generated by two co-prime elements.*

As before, there is a pseudo-isomorphism from M to a (unique) module $\bigoplus_{i=1}^{r} \Lambda(\Gamma_d)\big/(f_i^{e_i})$ where $f_i \in \Lambda(\Gamma_d)$ are irreducible; but now we require the kernel and cokernel are *pseudo-null*.

When $d=1$, a finitely generated $\Lambda(\Gamma)$-module is pseudo-null if and only if it finite. Indeed, consider a finitely generated, pseudo-null $\Lambda(\Gamma)$-module M. By definition, $\operatorname{char}(M) = \operatorname{Ann}_{\Lambda(\Gamma)}(M)$ has two relatively prime elements, hence it has finite index in $\Lambda(\Gamma)$. Conversely, if M is finite,

$$\operatorname{Ann}_{\Lambda(\Gamma)}(M) = \bigcap_{m\in M} \operatorname{Ann}_{\Lambda(\Gamma)}(m).$$

Since m generates a finite $\Lambda(\Gamma)$-module $\Lambda(\Gamma)\big/\operatorname{Ann}_{\Lambda(\Gamma)}(m)$, each $\operatorname{Ann}_{\Lambda(\Gamma)}(m)$ must be of finite index in $\Lambda(\Gamma)$. Thus $\operatorname{Ann}_{\Lambda(\Gamma)}(M)$ has finite index in $\Lambda(\Gamma)$ and is of height 2.

Greenberg observed that it appears as if for totally real fields, the Iwasawa module associated to the cyclotomic extension X_{cyc} is finite, i.e. $\lambda = \mu = 0$. He formulated the following general conjecture [35].

Generalized Greenberg's Conjecture. *Let F be a number field. Consider the compositum of all $\mathbb{Z}_p$-extensions $\widetilde{F}/F$ and let $\widetilde{L}$ denote its (pro)-p Hilbert class field. Then $\widetilde{X} = \operatorname{Gal}(\widetilde{L}/\widetilde{F})$ is a pseudo-null $\Lambda(\Gamma_d)$-module.*

2.2 Iwasawa Theory of Selmer Groups

Throughout this section $p \neq 2$. In [66], Mazur developed a theory that aimed at proving a result of the following flavour.

Conjecture 2.2.1. *Let A be an Abelian variety defined over a number field F. Assume p is such that A has good ordinary reduction at all primes above p. Let F_{cyc}/F be the cyclotomic $\mathbb{Z}_p$-extension, then the group of F_{cyc}-rational points of A, denoted $A(F_{\text{cyc}})$, is a finitely generated $\Lambda(\Gamma)$-module.*

2.2.1 Selmer Groups of Abelian Varieties

Let A be an Abelian variety defined over a fixed number field F. Let S be a finite set of primes in F containing the Archimedean primes, the primes above p, and the primes of bad reduction; for short write $S \supset S_\infty \cup S_p \cup S_{bad}$. For any extension L/F, denote by L_S the maximal extension of L unramified outside S; set the Galois group $\operatorname{Gal}(L_S/L)$ as $G_S(L)$. For a $G_S(L)$-module M, its i-th Galois cohomology group is denoted $H^i(G_S(L),\ M)$. If w is a place of L, we write L_w for its completion at w; when L/K is infinite, it is the union of completions of all finite sub-extensions of L. For local fields, $H^i(L_w,\ M)$ is the cohomology with respect to the absolute Galois group of L_w.

Let k be a positive integer. Kummer theory for Abelian varieties provides an injection

$$A(F)/p^k \hookrightarrow H^1\left(G_S(F),\ A[p^k]\right).$$

The classical p^k-**Selmer group** is the following kernel

$$0 \to \mathrm{Sel}_{p^k}\left(A/F\right) \to H^1\left(G_S\left(F\right),\ A[p^k]\right) \to \bigoplus_{v\in S} H^1\left(F_v,\ A\right)[p^k]. \tag{2.2}$$

Taking limit with respect to the maps induced by the inclusions $A[p^k] \hookrightarrow A[p^{k+1}]$, we obtain

$$\mathrm{Sel}(A/F) = \mathrm{Sel}_{p^\infty}(A/F) := \varinjlim_k \mathrm{Sel}_{p^k}(A/F). \tag{2.3}$$

This p-**primary Selmer group** fits into an exact sequence

$$0 \to A(F) \otimes {}^{\mathbb{Q}_p}\!\big/_{\mathbb{Z}_p} \to \mathrm{Sel}(A/F) \to Ш(A/F)(p) \to 0$$

where $A(F)$ is the group of F-rational points called the **Mordell-Weil group** and $Ш(A/F)$ is the **Shafarevich-Tate group**. This latter group measures the extent of failure of the local-global principle for rational equations with coefficients in F.

For an infinite Galois extension $\mathcal{L}/F$, the Selmer group $\mathrm{Sel}\left(A/\mathcal{L}\right)$ is defined as follows

$$0 \to \mathrm{Sel}\left(A/\mathcal{L}\right) \to H^1\left(G_S(\mathcal{L}),\ E_{p^\infty}\right) \to \bigoplus_{v\in S}\left(\varinjlim_L \bigoplus_{w|v} H^1\left(L_w,\ E\right)[p^\infty]\right).$$

The inductive limit is taken with respect to the restriction maps and L runs over all finite extensions of F contained in $\mathcal{L}$. Also note

$$\mathrm{Sel}\left(A/\mathcal{L}\right) = \varinjlim_L \mathrm{Sel}\left(A/L\right).$$

2.2.2 Cyclotomic Theory

Mostly, we restrict ourselves to the study of cyclotomic $\mathbb{Z}_p$-extension. The following result however is true in general. It is similar to the classical case and holds irrespective of the reduction type at p.

Proposition 2.2.2. *Let A be an Abelian variety over F. The Pontryagin dual of the p-primary Selmer group $\mathfrak{X}(A/F_\infty)$ is a finitely generated $\Lambda(\Gamma)$-module.*

When M is a discrete p-primary Abelian group or a compact pro-p Abelian group, its **Pontryagin dual** $M^\vee := \mathrm{Hom}_{\mathrm{cont}}(M,\ \mathbb{Q}_p/\mathbb{Z}_p)$. For a profinite group G and M a G-module, M^G is the subgroup of elements fixed by G and M_G is the largest quotient of M on which G acts trivially.

Sketch of Proof. By Nakayama's Lemma, it is enough to prove that $\mathfrak{X}(A/F_\infty)_\Gamma$ is a finitely generated $\mathbb{Z}_p$-module. By Pontryagin duality, it suffices to show $\mathrm{Sel}(A/F_\infty)^\Gamma$ is a co-finitely generated $\mathbb{Z}_p$-module. This is done by a careful analysis of the Fundamental Diagram.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}(A/F_\infty)^\Gamma \arrow[r] & H^1(G_S(F_\infty),\ A[p^\infty])^\Gamma \arrow[r] & \bigoplus_{v\in S} \varprojlim_L \left(\oplus_{w|v} H^1(L_w,\ A)(p)\right)^\Gamma \\
0 \arrow[r] & \mathrm{Sel}(A/F) \arrow[r] \arrow[u, "\alpha"] & H^1(G_S(F),\ A[p^\infty]) \arrow[r] \arrow[u, "\beta"] & \bigoplus_{v\in S} H^1(F_v,\ E)(p) \arrow[u, "\gamma"]
\end{tikzcd}$$

First, $H^1(G_S(F),\ A[p^\infty])$ has finite $\mathbb{Z}_p$-rank. It follows immediately that the same is true for $\mathrm{Sel}(A/F)$. Therefore, it is enough to show $\mathrm{coker}(\alpha)$ has finite $\mathbb{Z}_p$-rank.
Observe $\mathrm{coker}(\beta) = 0$ because the p-cohomological dimension of Γ is 1; by Hochschild-Serre spectral sequence $\mathrm{coker}(\beta) \hookrightarrow H^2(\Gamma,\ A[p^\infty](F_\infty))$. Lastly, $\ker(\gamma)$ has finite $\mathbb{Z}_p$-corank. Indeed, the dual of $\ker(\gamma)$ is a quotient of $\oplus_{v\in S} \varprojlim_n A(F_v)/p^n$; the structure of the latter group is known using the theory of formal groups. It is a finitely generated $\mathbb{Z}_p$-module. The claim for $\mathrm{coker}(\alpha)$ follows from the Snake Lemma. ☕

Remark 2.2.3. Even when $\mathfrak{X}(A/F_\infty)$ is a finitely generated $\Lambda(\Gamma)$-module it can fail to be $\Lambda(\Gamma)$-torsion.

1. Let F be an imaginary quadratic field and $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at p. Consider the anti-cyclotomic $\mathbb{Z}_p$-extension F_{ac}/F. It is possible $\mathrm{rank}_{\mathbb{Z}}(E(F_n))$ is unbounded, then $\mathfrak{X}(E/F_{\mathrm{ac}})$ is *not* $\Lambda(\Gamma)$-torsion.

2. Let F be a number field and E/F be an elliptic curve with good supersingular reduction at p. Then $\mathfrak{X}(E/F_{\mathrm{ac}})$ is *not* $\Lambda(\Gamma)$-torsion.

In [66], Mazur proved the **Control Theorem** for $\mathbb{Z}_p$-extensions of a number field.

Theorem 2.2.4. *Suppose A/F has good ordinary reduction at all primes above p. Let F_∞/F be any $\mathbb{Z}_p$-extension. The kernel and cokernel of the following natural maps are finite and bounded as $n \to 0$,*

$$\mathrm{Sel}(A/F_n) \to \mathrm{Sel}(F_\infty)^{\mathrm{Gal}(F_\infty/F_n)}.$$

Corollary 2.2.5. *Let A/F be an Abelian variety with good ordinary reduction at all primes above p. Suppose* $\mathrm{Sel}(A/F)$ *is finite. Then $\mathfrak{X}(A/F_\infty)$ is $\Lambda(\Gamma)$-torsion.*

Proof. By hypothesis, the Control Theorem implies $\mathrm{Sel}(A/F_\infty)^\Gamma$ is finite. The maximal quotient of $\mathfrak{X}(A/F_\infty)$ on which Γ acts trivially is $\mathfrak{X}(A/F_\infty)/T\mathfrak{X}(A/F_\infty)$. Therefore, it is the Pontryagin dual of $\mathrm{Sel}(A/F_\infty)^\Gamma$ and is also finite. By a variant of the Nakayama's Lemma (Theorem A.1.2), $\mathfrak{X}(A/F_\infty)$ is a finitely generated, torsion $\Lambda(\Gamma)$-module . ☕

Therefore, by the Structure Theorem $\mathfrak{X}(A/F_\infty)$ has finite $\mathbb{Z}_p$-corank, denoted $\lambda(\mathfrak{X}(A/F_\infty))$. The maximal divisible subgroup of $\mathrm{Sel}(A/F_\infty)$ is isomorphic to $\left(\mathbb{Q}_p\big/\mathbb{Z}_p\right)^{\lambda(\mathfrak{X}(A/F_\infty))}$. Then,

$$A(F_\infty) \otimes \mathbb{Q}_p\big/\mathbb{Z}_p \simeq \left(\mathbb{Q}_p\big/\mathbb{Z}_p\right)^r$$

where $0 \le r \le \lambda(\mathfrak{X}(A/F_\infty))$. For cyclotomic extensions, $A(F_{\mathrm{cyc}})_{\mathrm{tors}}$ is finite [83]. It follows that Conjecture 2.2.1 is true when $\mathrm{Sel}(A/F)$ is finite (see [66, Proposition 6.11] or [20, Theorem 2.8]). The above argument suggests more should be true, i.e. Conjecture 2.2.1 holds if the following is true.

Conjecture 2.2.6. *Let A be an Abelian variety defined over a number field F. Assume p is such that A has good ordinary reduction at all primes above p. Consider the cyclotomic $\mathbb{Z}_p$-extension F_{cyc}/F. Then $\mathfrak{X}(A/F_{\mathrm{cyc}})$ is a finitely generated torsion $\Lambda(\Gamma)$-module.*

Remark 2.2.7. In [66], Mazur gave a concrete example of an elliptic curve $E/\mathbb{Q}$ of conductor 11, namely

$$E : y^2 + y = x^3 - x^2 - 10x - 20$$

for which at the the prime $p = 5$ of good ordinary reduction, $\mathfrak{X}(E/\mathbb{Q}_{\mathrm{cyc}})$ is finitely generated and torsion as a $\Lambda(\Gamma)$-module *but* the associated μ-invariant is *positive*.

2.2.3 Iwasawa Theory of Elliptic Curves with CM

Let E be an elliptic curve over a number field F considered as a subfield of $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$. Denote by $\mathrm{End}_F(E)$ the ring of F-endomorphisms of F. It contains all the multiplication-by-$[n]$ maps where $n \in \mathbb{Z}$. Therefore $\mathbb{Z} \subseteq \mathrm{End}_F(E)$. We say that E *admits a complex multiplication (CM)* if

$$\mathrm{End}_{\overline{\mathbb{Q}}}(E) \neq \mathbb{Z}.$$

For an elliptic curve with CM, $\mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Q} = K$ is an imaginary quadratic field [97, Corollary III.9.4].

Elliptic curves which admit CM are very important from the point of view of Iwasawa theory. Their study goes back to two fundamental papers of Coates and Wiles [24], [25]. On the algebraic side of the story, the work of Perrin-Riou is highly influential [80]. In this section, we will introduce two extensions that are generally considered in the study of CM elliptic curves.

In view of the classical Iwasawa theory and the ubiquitous nature of elliptic curves, it is natural to expect an analogue for the field obtained by adjoining to $\mathbb{Q}$ all the p power torsion points on an elliptic curve E defined over $\mathbb{Q}$.

Split Prime $\mathbb{Z}_p$-Extensions

Let K be an imaginary quadratic field and $p \neq 2$ *splits* as $\mathfrak{p}\bar{\mathfrak{p}}$ in K. Let F/K be any finite Galois extension with an elliptic curve E defined over it. Let S be a finite set of primes in F, containing the archimedean primes, the primes of bad reduction of E and the primes above $\mathfrak{p}$. In this section, we consider elliptic curves E/F with good reduction at p and CM by $\mathcal{O}_K$, i.e. the ring of integers of K.

Remark 2.2.8. The hypotheses, $\mathrm{End}_F(E)$ is the maximal order of K, involves no real loss of generality since every E/F with $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_F(E) \simeq K$ is isogenous over F to one with this property.

Recall $\mathfrak{p}$ is a split prime above p in $K/\mathbb{Q}$, thus

$$E[\mathfrak{p}] \simeq \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \simeq \mathbb{Z}/p\mathbb{Z}.$$

It follows that, as Abelian groups,

$$E[\mathfrak{p}^\infty] = \bigcup_{n \geq 1} E[\mathfrak{p}^n] \simeq \mathbb{Z}_p.$$

We recall the construction of a non-cyclotomic $\mathbb{Z}_p$-extension from [15]. A natural way to define a non-cyclotomic $\mathbb{Z}_p$-extension is via points of finite order on E. Set $\widetilde{L} = F(E[\mathfrak{p}^\infty])$. The action of $\mathrm{Gal}(\widetilde{L}/F)$ on $E[\mathfrak{p}^\infty]$ gives a canonical injection

$$\chi_\infty : \mathrm{Gal}(\widetilde{L}/F) \hookrightarrow \mathbb{Z}_p^\times.$$

The image is of finite index in $\mathbb{Z}_p^\times$. We have the decomposition

$$\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$$

where μ_{p-1} is the group of $(p-1)$-th roots of unity. Via χ_∞, there is a corresponding decomposition of $\mathrm{Gal}(\widetilde{L}/F) = \Delta \times \Gamma$. The image of Δ is a subgroup of μ_{p-1} and that of Γ is a subgroup of $1 + p\mathbb{Z}_p$. The fixed field of Δ is a $\mathbb{Z}_p$ extension L/F whose Galois group can be identified with Γ.

By class field theory, there is a *unique* $\mathbb{Z}_p$-extension of K unramified outside of $\mathfrak{p}$. Denote this by K_∞ and call it the **split prime $\mathbb{Z}_p$-extension** of K. By the classical theory of CM, $L = FK_\infty$. Thus, L/F is unramified outside the set of primes above $\mathfrak{p}$ and each prime above $\mathfrak{p}$ is ramified in L/F.

Trivializing Extension

Keeping the same set up as before, further assume $p \neq 3$. Let E be an elliptic curve defined over F and F_∞ be the field obtained by adjoining all the p-power torsion points on E to F, i.e.

$$F_\infty = \bigcup_{n \geq 1} F(E[p^n]). \tag{2.4}$$

This is the **trivializing extension**. By the Weil pairing $F_\infty \supset F_{\mathrm{cyc}}$.

Suppose p does not ramify in K and $F = K(E[p])$. In the CM case, $G = \mathrm{Gal}(F_\infty/F)$ is a pro-p group isomorphic to $\mathbb{Z}_p^2$. By the theory of CM, $\mathrm{Gal}(F_\infty/K) = G \times \Delta$. Here $\Delta = \mathrm{Gal}(F/K)$ is a finite Abelian group, and $p \nmid |\Delta|$ as p does not ramify in K. Also $F_\infty = F\widetilde{K}$, where $\widetilde{K}/K$ is the unique $\mathbb{Z}_p^2$-extension.

We now draw the field diagram for convenience [80, Page 24].

$$\begin{tikzcd}
 & F_\infty \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K(E[\mathfrak{p}^\infty]) \arrow[dd, dash, swap, "\mathbb{Z}_p"] & F_{\mathrm{cyc}} \arrow[d, dash] & K(E[\overline{\mathfrak{p}}^\infty]) \arrow[dd, dash, swap, "\mathbb{Z}_p"] \\
 & F \arrow[dl, dash] \arrow[dr, dash] & \\
K(E[\mathfrak{p}]) \arrow[dr, dash] & & K(E[\overline{\mathfrak{p}}]) \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

2.3 Iwasawa Theory of Fine Selmer Groups

In view of Remark 2.2.7, it is clear that in the context of Iwasawa theory of (cyclotomic) $\mathbb{Z}_p$-extensions, the Selmer group is *not* the right analogue of the class group. It is believed that the right analogue is a subgroup of the classical Selmer group, called the *fine Selmer group* which is obtained by imposing stronger conditions at primes above p.

Let A be an Abelian variety defined over F, the p^k-**fine Selmer Group** is defined by the kernel

$$0 \to R_{p^k}\left(A/F\right) \to \mathrm{Sel}_{p^k}\left(A/F\right) \to \bigoplus_{v \mid p} H^1\left(F_v,\ A[p^k]\right). \tag{2.5}$$

As before, we consider the limit version, called the p-primary fine Selmer group. It is given by

$$R(A/F) = R_{p^\infty}(A/F) := \varinjlim R_{p^k}(A/F).$$

In fact, it is possible to define the p-**primary fine Selmer group** directly as the following kernel

$$0 \to R\left(A/F\right) \to H^1\left(G_S\left(F\right),\ A[p^\infty]\right) \to \bigoplus_{v\in S} H^1\left(F_v,\ A[p^\infty]\right).$$

It is okay to replace the sum to be over all primes in S. This is because by Kummer theory,

$$\ker\Big(H^1(F_v,\ A[p^\infty]) \to H^1(F_v,\ A)(p)\Big) = A(F_v)\otimes {}^{\mathbb{Q}_p}\Big/_{\mathbb{Z}_p}.$$

But the right hand side is trivial when $v \nmid p$.

For an infinite Galois extension $\mathcal{L}/F$, the Selmer group $R\left(A/\mathcal{L}\right)$ is defined as follows

$$0 \to R\left(A/\mathcal{L}\right) \to H^1\left(G_S(\mathcal{L}),\ E_{p^\infty}\right) \to \bigoplus_{v\in S}\left(\varinjlim_{L}\bigoplus_{w\mid v} H^1\left(L_w,\ E[p^\infty]\right)\right).$$

The inductive limit is taken with respect to the restriction maps and L runs over all finite extensions of F contained in $\mathcal{L}$. It is easy to observe that

$$R\left(A/\mathcal{L}\right) = \varinjlim_{L} R\left(A/L\right).$$

Consider a $\mathbb{Z}_p$-extension F_∞/F with $\mathrm{Gal}(F_\infty/F) = \Gamma$. The fine Selmer groups is a (discrete) subgroup of the classical Selmer group; therefore its Pontryagin dual, denoted by $\mathfrak{Y}(A/F_\infty)$, is a quotient of $\mathfrak{X}(A/F_\infty)$. By Proposition 2.2.2, it follows $\mathfrak{Y}(A/F_\infty)$ is also a finitely generated $\Lambda(\Gamma)$-module. However, more is believed to be true. For cyclotomic extensions, $\mathfrak{Y}(A/F_{\mathrm{cyc}})$ is *expected* to be $\Lambda(\Gamma)$-torsion irrespective of the reduction type at p. This is called the **weak Leopoldt Conjecture for elliptic curves**. By a result of Y. Ochi (see Lemma 2.5.1), the elliptic curve analogue of the weak Leopoldt conjecture over the cyclotomic extension can be formulated in terms of the vanishing of a certain Galois cohomology group. More precisely,

$$H^2\Big(G_S\left(F_{\mathrm{cyc}}\right),\ E[p^\infty]\Big) = 0. \tag{2.6}$$

Kato has proved this is indeed true when $F/\mathbb{Q}$ is an Abelian extension [54]. For CM elliptic curves this is known from the work of Rubin in the ordinary case [85] and McConnell in the supersingular case [70].

In [22], Coates and Sujatha studied the fine Selmer group over p-adic Lie extensions and posed two conjectures. In the rest of the chapter, we describe the necessary background to state these conjectures.

2.3.1 Conjecture A: Vanishing of the μ-Invariant

The following conjecture is the elliptic curve analogue of the Classical $\mu = 0$ Conjecture.

Conjecture A. *Let E be an elliptic curve over F. The Pontryagin dual of the fine Selmer group $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion and the associated μ-invariant is 0.*

A priori, it might not appear obvious, but Conjecture A is closely related to the Classical $\mu = 0$ Conjecture. This is evident from the following theorem [22, Theorem 3.4]. Using completely different techniques, this is also proven by Lim and Murty [60, Theorem 5.5].

Theorem 2.3.1. *Let $p \neq 2$. Suppose $F(E[p])/F$ is a finite p-extension. Then Conjecture A holds for $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ if and only if the Classical $\mu = 0$ Conjecture holds for F_{cyc}.*

2.4 Non-Commutative Iwasawa Theory

Let G be *any* compact p-adic Lie group without an element of order p; it is possible to visualize G as a *closed* subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$.

For a p-adic analytic, torsion-free, pro-p group G, the Iwasawa algebra over $\mathbb{Z}_p$, denoted by $\Lambda(G)$, is a left and right Noetherian ring without zero-divisors. In [102], Venjakob proved this is also Auslander regular. In particular, this property affords an associated dimension theory for finitely generated left (or right) modules over $\Lambda(G)$. If d is the dimension of G considered as a p-adic analytic manifold, the dimension of $\Lambda(G)$ is $d+1$.

In [44], Howson showed that for a finitely generated $\Lambda(G)$-module M,

$$\operatorname{rank}_{\Lambda(G)}(M) = \sum_{i\geq 0}(-1)^i \dim_{\mathbb{Z}_p}\left(H_i(G,\ M)\right). \tag{2.7}$$

Howson also considered the structure of modules over the $\mathbb{F}_p$-linear, completed group algebra

$$\Omega(G) := \varprojlim \mathbb{F}_p[G/U]$$

where U runs over all open normal subgroups of G. For a finitely generated $\Omega(G)$-module M, its $\Omega(G)$-**rank** is defined as

$$\operatorname{rank}_{\Omega(G)}(M) := \sum_{i\geq 0}(-1)^i \dim_{\mathbb{F}_p}\left(H_i(G, M)\right).$$

If M is a finitely generated $\Lambda(G)$-module, set $M(p)$ to denote the subset of M annihilated by some power of p. $M(p)$ is also finitely generated as a $\Lambda(G)$-module, it follows that there exists a non-negative integer r such that p^r annihilates $M(p)$. The μ_G-**invariant** of M is defined as

$$\begin{aligned}\mu_G(M) &:= \sum_{i\geq 0}\operatorname{rank}_{\Omega(G)}\left(p^i\left(M(p)\right)\Big/ p^{i+1}\right)\\ &= \operatorname{ord}_p\left(\prod_{i\geq 0}\left(\left|H_i(G,\ M(p))\right|\right)^{(-1)^i}\right)\end{aligned}$$

Before stating the *Non-Commutative Structure Theorem* established by Coates, Schneider, and Sujatha [19], we give a general definition of pseudo-nullity in this setting.

Definition 2.4.1. *Let M be a finitely generated $\Lambda(G)$-module of dimension $\dim(M)$. It is* ***torsion*** *if $\dim(M) \leq \dim\left(\Lambda(G)\right) - 1$ and is* ***pseudo-null*** *if $\dim(M) \leq \dim\left(\Lambda(G)\right) - 2$, i.e. if it has co-dimension at least 2.*

This definition coincides with the one in Definition 2.1.4, i.e. when $\Lambda(G)$ is a commutative local Noetherian regular ring via Grothendieck's local duality [9, Corollary 3.5.11]. It follows from the work of Björk that an equivalent definition can be given in terms of the Ext group [102, Proposition 3.4]. A finitely generated torsion $\Lambda(G)$-module M is a pseudo-null $\Lambda(G)$-module if

$$E^i := \mathrm{Ext}^i_{\Lambda(G)}\big(M,\ \Lambda(G)\big) = 0 \qquad \text{for } i = 0,\ 1. \tag{2.8}$$

Theorem 2.4.2 (Non-Commutative Structure Theorem). *For every torsion $\Lambda(G)$-module M there exist left ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ such that up to pseudo null modules, M decomposes into a product of cyclic modules*

$$M \to \prod_{i=1}^{r} {}^{\Lambda(G)}\big/_{\mathfrak{a}_i}.$$

2.4.1 Iwasawa Theory of Elliptic Curves Without CM

Given a number field F and an elliptic curve E/F, we denote the trivializing extension by F_∞. When E admits CM, $\mathrm{Gal}(F_\infty/F)$ contains an open subgroup which is Abelian and isomorphic to $\mathbb{Z}_p^2$. However, by Serre's Open Image Theorem, when E does not admit CM over the algebraic closure of F, the Galois group $\mathrm{Gal}(F_\infty/F)$ is isomorphic to an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. Thus, it is a non-Abelian, p-adic Lie extension of dimension 4. The methods of classical Iwasawa theory do not extend in the most obvious way to the GL_2 theory. The first results in this direction were proved by Coates and Howson [18].

2.4.2 Conjecture B: Pseudo-nullity Conjecture

Let F be a number field and $S \supseteq S_\infty \cup S_p$. A Galois extension $\mathcal{L}/F$ is called an **S-admissible p-adic Lie extension** if the following conditions are satisfied

(i) the Galois group $G_{\mathcal{L}} = \mathrm{Gal}(\mathcal{L}/F)$ is a p-adic Lie group.

(ii) $\mathcal{L} \subset F_S$.

(iii) $F_{\mathrm{cyc}} \subseteq \mathcal{L}$.

(iv) $G_{\mathcal{L}}$ is pro-p and has no element of order p.

In the last section, we saw some equivalent definitions of a pseudo-null module. There is yet another useful definition of pseudo-nullity which was given by Venjakob for p-adic Lie extensions “arising from geometry" [104]. Consider an S-admissible p-adic Lie extension $\mathcal{L}/F$, with the corresponding Galois group $\mathrm{Gal}(\mathcal{L}/F) = G_{\mathcal{L}}$. Denote $H_{\mathcal{L}} = \mathrm{Gal}(\mathcal{L}/F_{\mathrm{cyc}})$. A finitely generated $\Lambda(G_{\mathcal{L}})$-module M, which is also finitely generated over $\Lambda(H_{\mathcal{L}})$ is a **pseudo-null** $\Lambda(G_{\mathcal{L}})$-module if and only if it is $\Lambda(H_{\mathcal{L}})$-torsion.

In [22], Coates and Sujatha made a second conjecture in the spirit of generalising the Generalized Greenberg's Conjecture to elliptic curves. It concerns the phenomenon of certain arithmetic Iwasawa modules for p-adic Lie extensions of dimension greater than 1 being smaller than intuitively expected.

Conjecture B. *Let E be an elliptic curve defined over a number field F, such that Conjecture A holds for $\mathfrak{Y}(E/F_{\mathrm{cyc}})$. Let $\mathcal{L}/F$ be an admissible p-adic Lie extension and $G_{\mathcal{L}}$ be a pro-p p-adic Lie group of dimension strictly greater than 1. Then, $\mathfrak{Y}(E/\mathcal{L})$ is a pseudo-null $\Lambda(G_{\mathcal{L}})$-module.*

Remark 2.4.3. 1. This conjecture is *false* when dim(G)=1, i.e. when $G = \Gamma \simeq \mathbb{Z}_p$. If E is a rank 2 (or higher) elliptic curve defined over $\mathbb{Q}$, then $\mathfrak{Y}(E/\mathbb{Q}_{\mathrm{cyc}})$ has positive $\mathbb{Z}_p$-rank and hence can not be pseudo-null (equivalently finite) as a $\Lambda(\Gamma)$-module.

2. There exist p-adic Lie extensions $\mathcal{F}/F$ such that $F_{\text{cyc}} \not\subset \mathcal{F}$ and $\mathfrak{Y}(E/\mathcal{F})$ is not a pseudo-null module over the Iwasawa algebra.

3. Even though Conjecture B is formulated for *all* S-admissible p-adic Lie extensions $\mathcal{L}/F$, we will focus on those $\mathcal{L}$ for which the $G_S(\mathcal{L})$ action on $E[p^\infty]$ is trivial, i.e. those $\mathcal{L}/F$ which contain the trvializing extension $F_\infty = F(E[p^\infty])$.

2.5 Technical Tools

In this section we record some definitions and technical results which are heavily used in Iwasawa theory.

2.5.1 Hochschild-Serre Spectral Sequence

In studying cohomology of profinite groups, the **Hochschild–Serre spectral sequence** plays a major role. It is a spectral sequence relating the group cohomology of a normal subgroup H and the quotient group G/H to the cohomology of the group G. The concept is involved and we refer the reader to [76] for a detailed survey.

Let G be a profinite group, H be a closed normal subgroup, and M be a G-module. If $H^n(H,\ M) = 0$ for all $n \geq 1$, it follows from the five-term inflation-restriction exact sequence that

$$H^n\left({}^{G}\big/_{H},\ H^0(H,\ M)\right) \simeq H^n(G,\ M).$$

In fact, something far more general is true. We have a *spectral sequence*

$$H^p\left({}^{G}\big/_{H},\ H^q(H,\ M)\right) \Rightarrow H^{p+q}(G,\ M).$$

It *roughly says* that there is a canonical decreasing filtration of $H^n = H^n(G,\ M)$,

$$H^n = F^0H^n \supseteq F^1H^n \supseteq \ldots F^{n+1}H^n = 0$$

such that the quotient $F^pH^n/F^{p+1}H^n$ is isomorphic to a subquotient of $H^p\left(G/H,\ H^{n-q}(H,\ M)\right)$.

An easy consequence of the Hochschild-Serre Spectral sequence is the **inflation-restriction map**

$$\begin{array}{llllll} 0 & \to & H^1\left({}^{G}\big/_{H},\ M^H\right) & \xrightarrow{\text{inf}} & H^1(G,\ M) & \xrightarrow{\text{res}} & H^1(H,\ M)^{G/H} \\ & \to & H^2\left({}^{G}\big/_{H},\ M^H\right) & \xrightarrow{\text{inf}} & H^2(G,\ M) & & \end{array}$$

We record a special case of the Hochschild-Serre spectral sequence when $H^q(H,\ M) = 0$ for $q > 1$

$$\begin{array}{llllll} \cdots & \to H^1\left({}^{G}\big/_{H},\ H^0(H,\ M)\right) & \to H^1(G,\ M) & \to & H^0\left({}^{G}\big/_{H},\ H^1(H,\ M)\right) \to \\ & \to H^2\left({}^{G}\big/_{H},\ H^0(H,\ M)\right) & \to H^2(G,\ M) & \to & H^1\left({}^{G}\big/_{H},\ H^1(H,\ M)\right) \to \\ & \to H^3\left({}^{G}\big/_{H},\ H^0(H,\ M)\right) & \to H^3(G,\ M) & \to & H^2\left({}^{G}\big/_{H},\ H^1(H,\ M)\right) \to \end{array}$$

2.5.2 Iwasawa Cohomology of Elliptic Curves

The notion of Iwasawa cohomology will be mainly required in the last chapter.

Let E be an elliptic curve defined over F and consider its **Tate module**

$$T_p(E) := \varprojlim E[p^n].$$

Let S be a finite set of primes in F containing the Archimedean primes, the primes above p, and the primes of bad reduction of E. $T_p(E)$ is a finitely generated $\mathbb{Z}_p$-module with a continuous action of $G_S(F)$. For any S-admissible p-adic Lie extension $\mathcal{L}/F$, set $G = \mathrm{Gal}(\mathcal{L}/F)$. The i-th **Iwasawa cohomology groups** are compact $G_{\mathcal{L}}$-modules defined as

$$\mathcal{Z}^i(E/\mathcal{L}) := \varprojlim H^i(G_S(L),\ T_p(E)) \qquad i = 0,\ 1,\ 2$$

where the projective limit is taken with respect to co-restriction maps and L runs over all the finite extensions of F. It is known that $\mathcal{Z}^0(E/\mathcal{L}) = 0$.

Relation between Dual Fine Selmer Group and the Iwasawa Cohomology

Let v be a finite place of F. For each finite extension L/F contained in F_S, define

$$K_v^i(E/L) = \bigoplus_{w|v} H^i(L_w,\ E[p^\infty]) \qquad \text{when } i = 0,\ 1.$$

For an S-admissible p-adic Lie extension $\mathcal{L}/F$, define

$$K_v^i(E/\mathcal{L}) := \varinjlim_{L} K_v^i(E/L).$$

Taking direct limit of the standard Poitou-Tate sequence gives

$$0 \to H^0(\mathcal{L},\ E[p^\infty]) \to \bigoplus_{v\in S} K_v^0(E/\mathcal{L}) \to \mathcal{Z}^2(E/\mathcal{L})^\vee \to R(E/\mathcal{L}) \to 0. \tag{2.9}$$

The above equation suggests there is a close relation between $\mathfrak{Y}(E/\mathcal{L})$ and $\mathcal{Z}^2(E/\mathcal{L})$. The following lemma due to Y. Ochi makes explicit this relation [22, Lemma 3.1].

Lemma 2.5.1. *Let $\mathcal{L}$ be an S-admissible p-adic Lie extension of F with* $\mathrm{Gal}(\mathcal{L}/F) = G$. *For an elliptic curve E/F, the following are equivalent.*

(i) $\mathfrak{Y}(E/\mathcal{L})$ is $\Lambda(G)$-torsion.

(ii) $\mathcal{Z}^2(E/\mathcal{L})$ is $\Lambda(G)$-torsion.

(iii) The elliptic curve analogue of the weak Leopoldt conjecture holds, i.e. $H^2(G_S(\mathcal{L}),\ E[p^\infty]) = 0$.

When these assertions hold

$$\mu_G\left(\mathfrak{Y}\left(E/\mathcal{L}\right)\right) = \mu_G\left(\mathcal{Z}^2\left(E/\mathcal{L}\right)\right).$$

Sketch of proof. To see the equivalence of (i) and (ii), by Exact Sequence 2.9 it suffices to show the Pontryagin dual of $K_v^0(E/\mathcal{L})$ (denoted U_v) is $\Lambda(G)$-torsion.

Recall the decomposition group G_v has dimension at least 1. Set A_v to be the Pontryagin dual of $E(\mathcal{L}_v)[p^\infty]$. It is known that A_v is a finitely generated $\mathbb{Z}_p$-module. Further,

$$U_v = \Lambda(G) \otimes_{\Lambda(G_v)} A_v. \tag{2.10}$$

By an application of Shapiro's Lemma, $\Lambda(G)$-torsion-ness of U_v follows.
Equivalence of (ii) and (iii) is a consequence of Jannsen's spectral sequence. Denote by X_i the Pontryagin dual of $H^i(G_S(\mathcal{L}),\ E[p^\infty])$. Assuming (iii), X_i are finitely generated $\Lambda(G)$-modules and the implication follows from the exact sequence

$$E^2(X_0) \to \mathscr{Z}^2(E/\mathcal{L}) \to E^1(X_1).$$

Conversely, it follows from the exact sequence

$$\mathscr{Z}^2(E/\mathcal{L}) \to E^0(X_2) \to E^2(X_1)$$

that the middle term is $\Lambda(G)$-torsion, in fact it is trivial. Moreover, because X_2 has no $\Lambda(G)$-torsion, $X_2 = 0$ and (iii) follows.
To prove the final assertion, we need to show that $\mu_G(U_v) = 0$ for all $v \in S$. This follows from Equation 2.10 upon noticing that $\mu_{G_v}(A_v(p)) = 0$ for all v since $A_v(p)$ is finite. ☕

Remark 2.5.2. By Poitou-Tate duality, for *any* $\mathbb{Z}_p$-extension F_∞/F, the dual fine Selmer group $\mathfrak{Y}(E/F_\infty)$ is $\Lambda(\Gamma)$-torsion if and only if the analogue of the weak Leoplodt conjecture holds [64, Theorem 2.2].

Chapter 3

Growth Of Fine Selmer Groups

In the fundamental paper of Coates and Sujatha [22], it is explained that the fine Selmer group has stronger finiteness properties than the classical Selmer group. They showed that in the cyclotomic extension, the growth of the fine Selmer group is parallel to that of the ideal class group under some restrictive hypothesis. In [60], Lim and Murty further studied the strong analogy between the growth of the fine Selmer group and that of the class group. In this chapter we pursue a similar idea and understand the growth of fine Selmer groups in four different situations, namely

(i) in $\mathbb{Z}/p\mathbb{Z}$-extensions of number fields.

(ii) in $\mathbb{Z}_p^d$-extensions of number fields.

(iii) in non cyclotomic $\mathbb{Z}_p$-extensions of number fields.

(iv) in certain non-p-adic analytic towers, such as the p-class field tower.

3.1 Growth of p-Fine Selmer Groups in Extensions of Fixed Degree

Using genus theory, Gauss proved that the 2-torsion of the ideal class group of a quadratic number field can be arbitrarily large. If p is a fixed odd prime, it is a folklore result that the p-torsion of the ideal class group can become arbitrarily large in $\mathbb{Z}/p\mathbb{Z}$ extensions of a given number field [7]. Class groups and Selmer groups of Abelian varieties have similar properties; their close relationship was studied for global fields by Česnavičius [11]. Using arithmetic duality and a general version of the Cassels-Poitou-Tate exact sequence, he proved that the p-Selmer group can become arbitrarily large as one varies over all $\mathbb{Z}/p\mathbb{Z}$-extensions of a global field [12].

We show that the p-fine Selmer group of an Abelian variety has unbounded growth as one varies over $\mathbb{Z}/p\mathbb{Z}$ extensions of a fixed number field F. Our approach is similar to [60], where Lim and Murty showed that the p-primary fine Selmer group has unbounded growth as one varies over $\mathbb{Z}/p\mathbb{Z}$ extensions of F. Our results will imply the results of Lim-Murty and also of Česnavičius (for the number field case). Indeed, the p-fine Selmer group is contained in the p-primary fine Selmer group and is a subgroup of the p-Selmer group. Our proof provides an effective estimate on the conductor of such a $\mathbb{Z}/p\mathbb{Z}$-extension. Such bounds can not be obtained by the method of proof in [12].

For a fixed number field F, we do not know at present how to show that the p-fine Selmer group has unbounded growth as one varies over all $\mathbb{Z}/n\mathbb{Z}$-extensions of F where $1 < n < p$. Analogous results are conjectured to be true for the p-torsion of the ideal class group; in fact even when $n = 2$. We prove that under some mild hypothesis, the two questions are in fact equivalent.

3.1.1 Growth of p-Fine Selmer Groups in $\mathbb{Z}/p\mathbb{Z}$-Extensions

Definition 3.1.1. *For an Abelian group, G, define its p-**rank** $r_p(G)$ as $\dim_{\mathbb{Z}/p\mathbb{Z}} G[p]$.*

As a first step, we improve upon a result of Lim and Murty [60, Theorem 6.2]. This will also imply the theorem of Česnavičius (for the number field case) [12, Theorem 1.2].

Proposition 3.1.2. *Let A be a d-dimensional Abelian variety defined over a number field F. Suppose $A(F)[p] \neq 0$. Then*

$$\sup\{r_p\left(R_p(A/L)\right) \mid L/F \text{ is a cyclic extension of degree } p\} = \infty.$$

The method employed to prove the above proposition paves the way for the following theorem.

Theorem 3.1.3. *Let A be an Abelian variety of dimension d, defined over a number field F. Consider a finite set of primes $S \supseteq S_\infty \cup S_p \cup S_{bad}$. Suppose $A(F)[p] \neq 0$. Given a non-negative integer N, there exists a $\mathbb{Z}/p\mathbb{Z}$ extension L/F with norm of the conductor, $N_{F/\mathbb{Q}}\left(\mathfrak{f}\left(L/F\right)\right) \sim \kappa^N$ where κ is a constant depending on S, A and F, such that $r_p(R_p(A/L)) \geq N$.*

Technical Lemmas

We begin by proving a few technical lemmas. These will be used in proving the main results of this section and will often be used in future arguments.

Lemma 3.1.4. *Let G be a pro-p group. Every discrete simple p-primary G-module M is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ with trivial G-action. In particular, for a p-primary G-module M, $M = 0$ if and only if $M^G = 0$.*

Proof. Given a discrete p-primary G-module M, $pM = 0$. If U is an open normal subgroup of G, $M^U \neq 0$. G/U is finite and it is known

$$H^0\left({}^{G}\!\big/_{U},\ M^U\right) = M^G \subseteq M.$$

Note $M^G \neq 0$, since $M^U \neq 0$. Since M is a simple module, $M = M^G$. Thus, M is a dimension 1 $\mathbb{F}_p$-vector space with trivial action of G. ☕

We record the following estimate which will be used repeatedly.

Lemma 3.1.5. *[60, Lemma 3.2] Consider the following short exact sequence of of co-finitely generated Abelian groups*

$$P \to Q \to R \to S.$$

Then

$$\left|r_p\left(Q\right) - r_p\left(R\right)\right| \leq 2r_p\left(P\right) + r_p\left(S\right).$$

Lemma 3.1.6. *[59, Lemma 3.2] Let G be a pro-p group and M be a discrete G-module co-finitely generated over $\mathbb{Z}_p$. If $h_1(G) := r_p\left(H^1\left(G,\ \mathbb{Z}/p\mathbb{Z}\right)\right)$ is finite, then $r_p\left(H^1\left(G,\ M\right)\right)$ is finite and*

$$\begin{aligned} h_1(G)r_p(M^G) - r_p\left(\left({}^{M}\big/_{M^G}\right)^G\right) &\leq r_p\left(H^1\left(G,\ M\right)\right) \\ &\leq h_1(G)\left(\operatorname{corank}_{\mathbb{Z}_p}(M) + \log_p\left|{}^{M}\big/_{M_{\text{div}}}\right|\right) \end{aligned}$$

Moreover, when M is a trivial G-module,

$$r_p\left(H^1\left(G,\ M\right)\right) = h_1(G)r_p(M).$$

Proof. Upper bound: For *finite* M, by *dévissage* it suffices to consider M is simple. By Lemma 3.1.4,

$$r_p\left(H^1(G, M)\right) \leq h_1(G)\log_p\left(|M|\right). \tag{3.1}$$

For *general* M, consider the maximal p-divisible module M_{div} of M; it is a G-submodule. There is the standard short exact sequence,

$$0 \to M_{\text{div}} \to M \to {}^{M}\big/_{M_{\text{div}}} \to 0.$$

Set $N = M/M_{\text{div}}$. The above short exact sequence induces the following exact sequence,

$$H^1\left(G,\ M_{\text{div}}\right) \to H^1\left(G,\ M\right) \to H^1\left(G,\ N\right). \tag{3.2}$$

By hypothesis, N is finite. Thus $r_p\left(H^1\left(G,\ N\right)\right)$ is finite and by Inequality 3.1,

$$r_p\left(H^1\left(G,\ N\right)\right) \leq h_1(G)\log_p\left(|N|\right). \tag{3.3}$$

Now consider the multiplication-by-p map of G-modules,

$$0 \to M_{\text{div}}[p] \to M_{\text{div}} \xrightarrow{p} M_{\text{div}} \to 0.$$

This gives the following surjection

$$H^1\left(G,\ M_{\text{div}}[p]\right) \to H^1\left(G,\ M_{\text{div}}\right)[p] \to 0.$$

This proves

$$\begin{aligned} r_p\left(H^1\left(G,\ M_{\text{div}}\right)\right) &\leq r_p\left(H^1\left(G,\ M_{\text{div}}\right)[p]\right) && (3.4) \\ &\leq h_1(G)\log_p\left(\left|M_{\text{div}}[p]\right|\right) \qquad \text{by Inequality 3.1} && (3.5) \\ &= h_1(G)\operatorname{corank}_{\mathbb{Z}_p}(M). && (3.6) \end{aligned}$$

By Exact Sequence 3.2, we see that

$$r_p\left(H^1(G,\ M)\right) \leq r_p\left(H^1\left(G,\ M_{\text{div}}\right)\right) + r_p\left(H^1\left(G,\ N\right)\right)$$

Thus, the upper bound follows from Inequalities 3.3 and 3.6.
Second assertion: Suppose M is a trivial G-module. Since cohomology commutes with finite direct sums, it suffices to show

$$h_1(G) = r_p\left(H^1\left(G,\ \mathbb{Z}/p^r\mathbb{Z}\right)\right) = r_p\left(H^1\left(G,\ {}^{\mathbb{Q}_p}\!\big/_{\mathbb{Z}_p}\right)\right).$$

Consider the natural inclusion maps

$$H^1\left(G,\ \mathbb{Z}/p\mathbb{Z}\right) \hookrightarrow H^1\left(G,\ \mathbb{Z}/p^r\mathbb{Z}\right) \hookrightarrow H^1\left(G,\ {}^{\mathbb{Q}_p}\!\big/_{\mathbb{Z}_p}\right).$$

From the upper bound estimates and the above inclusions, we have

$$h_1(G) \leq r_p\left(H^1\left(G,\ \mathbb{Z}/p^r\mathbb{Z}\right)\right) \leq r_p\left(H^1\left(G,\ {}^{\mathbb{Q}_p}\!\big/_{\mathbb{Z}_p}\right)\right) \leq h_1(G).$$

The result follows.
Lower bound: Consider the short exact sequence,

$$0 \to M^G \to M \to {}^{M}\!\big/_{M^G} \to 0.$$

Taking the cohomology sequence gives

$$0 \to \left({}^{M}\!\big/_{M^G}\right)^G \to H^1\left(G,\ M^G\right) \to H^1\left(G,\ M\right).$$

This gives the following:

$$\begin{aligned} r_p\left(H^1(G,\ M)\right) &\geq r_p\left(H^1\left(G,\ M^G\right)\right) - r_p\left(\left({}^{M}\!\big/_{M^G}\right)^G\right) \\ &= h_1(G) r_p\left(M^G\right) - r_p\left(\left({}^{M}\!\big/_{M^G}\right)^G\right) \end{aligned}$$

The equality in the last line follows from the second assertion. ☕

Definition 3.1.7. *Let F be a number field and S be a finite set of primes containing $S_\infty \cup S_p$. The maximal Abelian unramified p-extension of a number field F in which all primes in S split completely is the **p-Hilbert S-class field** of F. It is denoted by $H_S(F)$ or even H_S.*

The following lemma is a variant of [60, Lemma 4.3]. We give a lower bound for the p-rank of p-fine Selmer group in terms of the p-rank of the S-class group.

Lemma 3.1.8. *Let A be a d-dimensional Abelian variety defined over a number field F. Consider a finite set of primes S containing $S_p \cup S_{bad} \cup S_\infty$. Suppose $A(F)[p] \neq 0$. Then*

$$r_p\left(R_p\left(A/F\right)\right) \geq r_p\left(\mathrm{Cl}_S\left(F\right)\right) r_p\left(A\left(F\right)[p]\right) - 2d.$$

Proof. Consider the following diagram with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & R_p(A/F) \arrow[r] \arrow[d, "\alpha"] & H^1(G_S(F),\ A[p]) \arrow[r] \arrow[d, "\beta"] & \bigoplus_{v\in S} H^1(F_v,\ A[p]) \arrow[d, "\gamma"] \\
0 \arrow[r] & R_p(A/H_S) \arrow[r] & H^1(G_S(H_S),\ A[p]) \arrow[r] & \bigoplus_{v\in S} \bigoplus_{w\mid v} H^1(H_{S,w},\ A[p])
\end{tikzcd}$$

The vertical maps are given by restriction maps. Write $\gamma = \oplus_v \gamma_v$ where

$$\gamma_v : H^1\left(F_v,\ A[p]\right) \to \bigoplus_{w\mid v} H^1\left(H_{S,w},\ A[p]\right).$$

From the inflation-restriction sequence, one gets that $\ker \gamma_v = H^1\left(G_v,\ A[p]\right)$, where G_v is the decomposition group of $G = \mathrm{Gal}(H_S/F)$ at v. By the definition of the p-Hilbert S-class field, all primes in $S(F)$ split completely in H_S; hence $G_v = 1$. This forces $\ker \gamma$ to be trivial.

By the inflation-restriction sequence, $\ker \beta = H^1\Big(\mathrm{Gal}\left(H_S/F\right),\ A\left(H_S\right)[p]\Big)$. This gives

$$H^1\Big(\mathrm{Gal}\left(H_S/F\right),\ A\left(H_S\right)[p]\Big) \hookrightarrow R_p(A/F).$$

This implies

$$r_p\left(R_p(A/F)\right) \geq r_p\bigg(H^1\Big(\mathrm{Gal}\left(H_S/F\right),\ A\left(H_S\right)[p]\Big)\bigg).$$

Lemma 3.1.6 implies that

$$r_p\bigg(H^1\Big(\mathrm{Gal}\left(H_S/F\right),\ A\left(H_S\right)[p]\Big)\bigg) \geq h_1\Big(\mathrm{Gal}\left(H_S/F\right)\Big)\, r_p\left(A\left(F\right)[p]\right) - 2d.$$

From class field theory, $\mathrm{Gal}(H_S/F) \simeq \mathrm{Cl}_S(F)$. The result follows since the class group (and hence the S-class group) is always finite; therefore

$$h_1\left(\mathrm{Gal}(H_S/F)\right) = r_p\left(\mathrm{Cl}_S(F)\right).$$

This finishes the proof of the lemma. ☕

Remark 3.1.9. Under the stronger assumption $A[p] \subseteq A(F)$, it is possible to show a stronger relationship between p-fine Selmer groups and p-torsion of class groups. The assumption forces $A[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{2d}$ as $G_S(F)$-modules. Note that $G_S(F)$ acts trivially on $A[p]$, hence

$$H^1\left(G_S(F),\ A[p]\right) = \mathrm{Hom}\left(G_S(F),\ A[p]\right).$$

We have similar equalities for the local cohomology groups as well. Thus,

$$R_p(A/F) = \mathrm{Hom}\left(\mathrm{Cl}_S(F),\ A[p]\right) \simeq \mathrm{Cl}_S(F)[p]^{2d}$$

as Abelian groups. Therefore

$$r_p\left(R_p(A/F)\right) = 2d r_p\left(\mathrm{Cl}_S(F)\right).$$

Observe $R_p(A/F)$ *depends* on the choice of S, even though in the limit, $R(A/F)$ does not. For ease of notation, we avoid writing $R_p^S(A/F)$; but the dependence of $R_p(A/F)$ on S is crucial in our proofs.

Proof of Proposition 3.1.2

We first recall the statement of the Grunwald-Wang Theorem [76, Theorem 9.2.8].

Grunwald-Wang Theorem. *Let S be a finite set of primes of a global field F and let G be a finite Abelian group. For all $\mathfrak{p} \in S$, let the finite Abelian extensions $\mathcal{F}_{\mathfrak{p}} \mid F_{\mathfrak{p}}$ be given such that $\operatorname{Gal}(\mathcal{F}_{\mathfrak{p}} \mid F_{\mathfrak{p}})$ may be embedded into G. Then there exists a global Abelian extension $\mathcal{F} \mid F$ with Galois group G such that $\mathcal{F}$ has the given completions $\mathcal{F}_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$.*

Proposition 3.1.10. *[60, Proposition 6.1] Let S be a finite set of primes of F containing the Archimedean primes. Then there exists a sequence $\{L_n\}$ of distinct number fields such that each L_n is a $\mathbb{Z}/p\mathbb{Z}$ extension of F and such that for every $n \geq 1$,*

$$r_p\left(\mathrm{Cl}_S\left(L_n\right)\right) \geq n.$$

Proof. Set r_1 and r_2 to denote the number of real and the number of pairs of complex embeddings of F. Let S_1 be a set of primes of F containing S such that

$$|S_1| = |S| + r_1 + r_2 + \delta + 1$$

where $\delta = 1$ if F contains a primitive p-root of unity, and is 0 otherwise.

By the Grunwald-Wang theorem, there exists a $\mathbb{Z}/p\mathbb{Z}$ extension L_1/F such that it is ramified at all finite places of S_1 and is unramified outside of it. It follows (see [76, Proposition 10.10.3]),

$$r_p\left(\mathrm{Cl}_S\left(L_1\right)\right) \geq |S_1| - |S| - r_1 - r_2 - \delta = 1.$$

Repeat the above process; choose a set S_2 containing S_1 with the property

$$|S_2| = |S_1| + 1 = |S| + r_1 + r_2 + \delta + 2.$$

By the Grunwald-Wang theorem, there exists a $\mathbb{Z}/p\mathbb{Z}$-extension L_2/F ramified at all finite places of S_2 and unramified outside of it. L_2 is distinct from L_1 by construction. For this field,

$$r_p\left(\mathrm{Cl}_S\left(L_2\right)\right) \geq 2.$$

Since F has infinitely many primes, we can continue this process indefinitely. Each of the L_i's are distinct by construction. This proves the proposition. ☕

Remark 3.1.11. We emphasize that in using [76, Proposition 10.10.3] we need L_i/F is a $\mathbb{Z}/p\mathbb{Z}$-extension.

Proposition 3.1.10 combined with Lemma 3.1.8 proves Proposition 3.1.2. We recall the statement

Proposition. *Let A be a d-dimensional Abelian variety defined over a number field F. Let S be a finite set of primes of F including the infinite primes, the primes where A has bad reduction and the primes above p. Suppose $A(F)[p] \neq 0$. Then*

$$\sup\{r_p\left(R_p(A/L)\right) \mid L/F \textit{ is a cyclic extension of degree } p\} = \infty.$$

Corollary 3.1.12. *Let A be an Abelian variety of dimension d defined over F. If $A(F)[p] = 0$, define*

$$m = \min\{[F' : F] \mid A(F')[p] \neq 0\}.$$

Then

$$\sup\{r_p(R_p(A/L)) \mid L/F \textit{ is an extension of degree } pm\} = \infty.$$

Remark 3.1.13. By hypothesis, $1 < m \leq \left|\mathrm{GL}_{2d}(\mathbb{Z}/p\mathbb{Z})\right|$. Consider the Galois group $\mathrm{Gal}(F(A[p])/F)$ which is a subgroup of $\mathrm{GL}_{2d}(\mathbb{Z}/p\mathbb{Z})$. Let P be a non-trivial point in $A[p]$ and H be the subgroup of G that fixes P. Consider the extension $F' = F\left(A[p]\right)^H$. By Galois theory,

$$[F' : F] = [G : H] = \left|\mathrm{orb}_G(P)\right|.$$

But $\mathrm{orb}_G(P) \subseteq A[P] \setminus \{0\}$. Thus

$$m \leq [F' : F] = \left|\mathrm{orb}_G(P)\right| \leq p^{2d} - 1.$$

Proof of Theorem 3.1.3

In Proposition 3.1.2, we saw that the size of $R_p(A/F)$ becomes arbitrarily large as we vary over all $\mathbb{Z}/p\mathbb{Z}$-extensions of F. The proof of Proposition 3.1.10 suggests it should be possible to find an effective estimate on the conductor. Indeed, we can prove the following theorem.

Theorem. *Let A be an Abelian variety of dimension d, defined over a number field F. Let S be a finite set of primes as defined above. Suppose $A(F)[p] \neq 0$. Given a non-negative integer N, there exists a $\mathbb{Z}/p\mathbb{Z}$ extension L/F with norm of the conductor, $N_{F/\mathbb{Q}}\left(\mathfrak{f}\left(L/F\right)\right) \sim \kappa^N$ where κ is a constant depending on S, A and F, such that $r_p\left(R_p\left(A/L\right)\right) \geq N$.*

When $F = \mathbb{Q}$, the notation simplifies considerably. We prove the theorem in detail for this case.

Theorem 3.1.14. *Let A be an Abelian variety of dimension d defined over $\mathbb{Q}$. Let $S = S_p \cup S_{bad} \cup S_\infty$. Suppose $A(\mathbb{Q})[p] \neq 0$. Given a non-negative integer N, there exists a $\mathbb{Z}/p\mathbb{Z}$ extension $L/\mathbb{Q}$ of conductor $\mathfrak{f}(L/\mathbb{Q}) \sim \kappa^N$ where κ is a constant depending on S and A, such that $r_p(R_p(A/L)) \geq N$.*

Proof. Let $L/\mathbb{Q}$ be a $\mathbb{Z}/p\mathbb{Z}$-extension and P be the set of ramified primes in L. Since $L/\mathbb{Q}$ is a Galois extension, there is a unique $\mathfrak{p} \mid p$ for a $p \in P$. The conductor $\mathfrak{f}(L/\mathbb{Q}) = \prod_{q\in P} \mathfrak{f}_q$ where

$$\mathfrak{f}_q = \begin{cases} q^{p-1}, & \text{when } (q,p) = 1 \\ p^{p-1+\mathfrak{s}_{\mathfrak{p}|p}}, & \text{otherwise.} \end{cases}$$

Note $1 \leq \mathfrak{s}_{\mathfrak{p}|p} \leq \mathrm{val}_{\mathfrak{p}}(p) = p$. The first is called tame ramification and the second is wild ramification. Taking natural log,

$$\log\left(\mathfrak{f}\left(L/\mathbb{Q}\right)\right) = (p-1)\sum_{q\in P} \log q + \mathfrak{s}_{\mathfrak{p}|p} \log p. \tag{3.7}$$

Given a non-negative integer N, we wish to find the minimal conductor of a $\mathbb{Z}/p\mathbb{Z}$ extension $L/\mathbb{Q}$ such that $r_p(R_p(A/L)) \geq N$. By Lemma 3.1.8, it suffices to find a $\mathbb{Z}/p\mathbb{Z}$-extension $L_{n(N)}/\mathbb{Q}$ such that

$$r_p\left(\mathrm{Cl}_S\left(L_n\right)\right) \geq \frac{2d+N}{r_p\left(A\left(L_n\right)[p]\right)} =: n(N) = n.$$

Note that $r_p\left(A\left(L_n\right)[p]\right)$ is a positive constant, less than or equal to $2d$.

Let $S = \{v_1, \ldots, v_k\} \cup S_\infty$ be the finite set of primes containing the Archimedean primes, the primes above p, and the primes of bad reduction of A. We construct S_n as in the proof of Proposition 3.1.10. Here, $r_1 = 1$, $r_2 = 0$ and $\delta = 0$. Therefore we must choose S_n such that $|S_n| = |S| + 1 + n$.

Define $M = \prod_{i=1}^{k} v_i$. Then $\log M \sim k \log k$. To construct S_n from the given set S, we need to add $n+1$ many primes. Choose the first prime $p_1 \nmid M$. By the Prime Number Theorem we know we can find $p_1 \sim \log M$. Now choose $p_2 \nmid Mp_1$; here $p_2 \sim \log(M \log M)$. We have $S \cup \{p_1, p_2\} = S_1$. Continue to choose in the same way as many primes as required to form S_n. By Equation 3.7, as $n \to \infty$,

$$\log\left(\mathfrak{f}(L_n/\mathbb{Q})\right) \sim (p-1)n \log\log M.$$

Equivalently, $\mathfrak{f}(L_n/\mathbb{Q}) \sim c^n$ with c a constant that depends on the given set S. By definition of $n(N)$, $\mathfrak{f}(L_{n(N)}/\mathbb{Q}) \sim \kappa^N$ for a constant κ that depends on S and A. ☕

Proving the general case is similar. We point out some similarities and differences one needs to keep in mind. Consider the tower of number fields, $L \supset F \supset \mathbb{Q}$ where $[L : F] = p$. By hypothesis, L/F is Galois. If $\mathfrak{q} \mid q$ is a prime in F that ramifies in L, there will be a unique prime $\mathfrak{Q} \mid \mathfrak{q}$. The definition of the conductor carries through. Now we are interested in the norm $N_{F/\mathbb{Q}}(\mathfrak{f}(L/F))$ so as to be able to do estimates. Define $M = \prod_i N(v_i)$ and construct S_n from S by adding $r_1 + r_2 + \delta + n$ many primes. Choose $p_1 \nmid M$ as before and the required element of S_n is $\mathfrak{p}_1 \mid p_1$. From here, the proof follows as before.

Remark 3.1.15. From Equation 2.5, $r_p\left(\mathrm{Sel}_p(A/F)\right) \geq r_p\left(R_p(A/F)\right)$. It follows that Theorem 3.1.3 holds if we replace $r_p(R_p(A/L)) \geq N$ by $r_p(\mathrm{Sel}_p(A/L)) \geq N$.

3.1.2 Growth of p-Fine Selmer Groups in $\mathbb{Z}/2\mathbb{Z}$-Extensions

Even though we can not prove that the p-(fine) Selmer group can be arbitrarily large in quadratic extensions of $\mathbb{Q}$, we believe it should be true. We can show that this question is equivalent to a well-known conjecture about class groups of quadratic equations. We prove this for the case of elliptic curves, a more general statement for Abelian varieties is mentioned later.

Theorem 3.1.16. *Fix an odd prime p. Let E/F be an elliptic curve such that $E(F)[p] \neq 0$. Let S be a finite set of primes in F containing the primes above p, the primes of bad reduction of E and the Archimedean primes. As we vary over all $\mathbb{Z}/2\mathbb{Z}$-extensions L/F,*

$$\sup\{r_p\left(R_p(E/L)\right) \mid \ L/F \textit{ is a quadratic extension}\} = \infty$$

if and only if

$$\sup\{r_p\left(\mathrm{Cl}(L)\right) \mid \ L/F \textit{ is a quadratic extension}\} = \infty.$$

To prove the theorem we will need a few lemmas.

Lemma 3.1.17. *With the same setting as in Theorem 3.1.16,*

$$r_p\left(R_p(E/L)\right) \geq r_p\left(\mathrm{Cl}(L)\right) r_p\left(E(L)[p]\right) + O(1)$$

Proof. It follows immediately from Lemma 3.1.8 upon observing that

$$\Big| r_p\left(\mathrm{Cl}(L)\right) - r_p\left(\mathrm{Cl}_S(L)\right) \Big| = O(1). \tag{3.8}$$

Indeed, set the notation $S_f(L)$ to denote the set of finite primes of L above non-Archimedean primes of S. We have the following exact sequence (see [76, Lemma 10.3.12])

$$\mathbb{Z}^{\left|S_f(L)\right|} \to \mathrm{Cl}(L) \xrightarrow{\alpha} \mathrm{Cl}_S(L) \to 0.$$

Since $\ker(\alpha) \subseteq \mathrm{Cl}(L)$, it is finite with p-rank less than equal to $\left|S_f(L)\right|$. Equation 3.8 follows from Lemma 3.1.5 since $\left|S_f(L)\right|$ is finite and bounded, in fact always less than $|S|^2$. ☕

Let us define a slight variant of the fine Selmer group. Set $B = E(L)[p]$. Define $R_p(B/L)$ by replacing $E[p]$ with $E(L)[p]$ in Equation 2.5. In the following lemma, we show that the p-fine Selmer group and the modified fine Selmer group have the same order of growth in an extension of fixed degree.

Lemma 3.1.18. *With the setting as Theorem 3.1.16,*

$$\left| r_p\left(R_p(B/L)\right) - r_p\left(R_p(E/L)\right)\right| \leq \cdot r_p\left(\mathrm{Cl}_S(L)\right) + O(1).$$

Proof. If $B = E(L)[p] = E[p]$, there is nothing to prove. So, assume $B \neq E[p]$.
Consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & R_p\left(B/L\right) \arrow[r] \arrow[d, "s"] & H^1\left(G_S\left(L\right),\ B\right) \arrow[r] \arrow[d, "f"] & \bigoplus_v H^1\left(L_v,\ B\right) \arrow[d, "g"] \\
0 \arrow[r] & R_p\left(E/L\right) \arrow[r] & H^1\left(G_S\left(L\right),\ E[p]\right) \arrow[r] & \bigoplus_v H^1\left(L_v,\ E[p]\right)
\end{tikzcd}$$

where v runs over all the primes in the finite set $S(L)$.

By hypothesis, E has an L-rational p-torsion point. This gives the short exact sequence

$$0 \to B \to E[p] \to \mu_p \to 0. \tag{3.9}$$

Taking its $G_S(L)$-cohomology, $\ker(f) = H^0(G_S(L),\ \mu_p)$. Also $r_p\left(\ker(s)\right) \leq r_p\left(\ker(f)\right) = O(1)$, as $\left|\mu_p\right|$ is finite and bounded,. A similar argument for the local cohomology yields $r_p\left(\ker(g)\right) = O(1)$.

We will show $r_p\left(\mathrm{coker}(s)\right) \leq r_p\left(\mathrm{coker}\left(f\right)\right) \leq r_p\left(\mathrm{Cl}_S\left(L\right)\right) + O(1)$. This suffices; by Lemma 3.1.5 applied to the map s,

$$\begin{aligned}
\left| r_p\left(R_p\left(B/L\right)\right) - r_p\left(R_p\left(A/L\right)\right)\right| &\leq 2r_p\left(\ker(s)\right) + r_p\left(\mathrm{coker}(s)\right) \\
&= r_p\left(\mathrm{coker}(s)\right) + O(1).
\end{aligned}$$

Let $\mathcal{O}_S^\times$ be the set of S-units of L_S, the maximal unramified outside S extension of L. We know $\mu_p \subseteq \mathcal{O}_S^\times$ and there exists a short exact sequence (see [76, Theorem 8.3.18])

$$0 \to \mu_p \to \mathcal{O}_S^\times \xrightarrow{p} \mathcal{O}_S^\times \to 0.$$

This yields a long exact sequence which can be rewritten as

$$0 \to \mathcal{O}_{L,S}^\times / \left(\mathcal{O}_{L,S}^\times\right)^p \to H^1\left(G_S(L),\ \mu_p\right) \to \mathrm{Cl}_S(L)[p] \to 0, \tag{3.10}$$

where $\mathcal{O}_{L,S}^\times$ is the notation for the S-units of L. We remark, Exact Sequence 3.10 follows from standard results $H^0\left(G_S(L),\ \mathcal{O}_S^\times\right) \simeq \mathcal{O}_{L,S}^\times$ and $H^1\left(G_S(L),\ \mathcal{O}_S^\times\right) \simeq \mathrm{Cl}_S(L)$ (see [76, Theorem 8.3.11]). Therefore, (p-rank of) $\operatorname{coker}(f) = H^1(G_S(L),\ \mu_p)$ is finite.

Furthermore,

$$\Big| r_p\left(\operatorname{coker}(f)\right) - r_p\left(\mathrm{Cl}_S(L)\right) \Big| \le r_p\left(\mathcal{O}_{L,S}^\times \Big/ \left(\mathcal{O}_{L,S}^\times\right)^p \right).$$

Since $\big|S(L)\big|$ is bounded by an absolute constant, the S-units analogue of Dirichlet's Unit Theorem yields

$$\Big| r_p\left(\operatorname{coker}(f)\right) - r_p\left(\mathrm{Cl}_S(L)\right) \Big| = O(1).$$

Equivalently,

$$r_p\left(\operatorname{coker}(f)\right) = r_p\left(\mathrm{Cl}_S(L)\right) + O(1).$$

Therefore,

$$\Big| r_p\left(R_p(B/L)\right) - r_p\left(R_p(E/L)\right) \Big| \le r_p\left(\mathrm{Cl}_S(L)\right) + O(1).$$

This finishes the proof. ☕

Proof of the Theorem. In Lemma 3.1.17, we proved

$$r_p\left(R_p(E/L)\right) \ge r_p\left(\mathrm{Cl}(L)\right) r_p\left(E(L)[p]\right) + O(1)$$

This proves one direction of the theorem: if $r_p\left(\mathrm{Cl}\left(L\right)\right)$ is arbitrarily large then so is the $r_p\left(R_p\left(E/L\right)\right)$. Equivalently, if $r_p\left(R_p\left(E/L\right)\right)$ is bounded then so is $r_p\left(\mathrm{Cl}\left(L\right)\right)$.

We now prove the other direction.

Claim: If $r_p(\mathrm{Cl}(L))$ is bounded, the same is true for the $r_p(R_p(E/L))$.

Justification: Suppose that $r_p\left(\mathrm{Cl}(L)\right) = O(1)$. By Equation 3.8, the $r_p\left(\mathrm{Cl}(L)\right)$ is bounded if and only if $r_p\left(\mathrm{Cl}_S(L)\right)$ is bounded.

By hypothesis, the Galois action of $G_S(L)$ on $E(L)[p]$ is trivial; the argument in Remark 3.1.9 yields

$$r_p\left(R_p(B/L)\right) \le 2 r_p\left(\mathrm{Cl}_S(L)\right) = O(1).$$

By Lemma 3.1.18,

$$\Big| r_p\left(R_p(B/L)\right) - r_p\left(R_p(E/L)\right) \Big| = O(1).$$

From the above two inequalities, the claim follows. This finishes the proof of the theorem. ☕

Remark 3.1.19. It is possible to prove an analogue of Theorem 3.1.16 for an Abelian variety A/F provided it has subquotients isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or μ_p.

3.2 Growth of p-Fine Shafarevich-Tate Group in $\mathbb{Z}/p\mathbb{Z}$-Extensions

For an Abelian variety A over F, by Kummer theory, we have the short exact sequence

$$0 \to A(F)/p^k \to \mathrm{Sel}_{p^k}(A/F) \to Ш(A/F)[p^k] \to 0.$$

In [107], Wuthrich defined a fine subgroup of the Mordell-Weil group; it is the following kernel

$$0 \to M_{p^k}(A/F) \to A(F)/p^k \to \bigoplus_{v|p} A(F_v)/p^k.$$

It is now natural to define the p^k-**fine Shafarevich-Tate group** by the exact sequence,

$$0 \to M_{p^k}(A/F) \to R_{p^k}(A/F) \to \text{Ж}_{p^k}(A/F) \to 0.$$

One can view $\text{Ж}_{p^k}(A/F)$ as a subgroup of $\text{Ш}(A/F)[p^k]$. Consider the following diagram

$$\begin{tikzcd}
0 \arrow[r] & A(F)/p^k \arrow[r] \arrow[d] & \mathrm{Sel}_{p^k}(A/F) \arrow[r] \arrow[d] & \text{Ш}(A/F)[p^k] \arrow[r] \arrow[d, "0"] & 0 \\
0 \arrow[r] & \bigoplus_{v|p} A(F_v)/p^k \arrow[r] & \bigoplus_{v|p} H^1(F_v,\ A[p^k]) \arrow[r] & \bigoplus_{v|p} H^1(F_v,\ A)[p^k] \arrow[r] & 0
\end{tikzcd}$$

By an application of the Snake Lemma, one obtains the following exact sequence

$$0 \to M_{p^k}(A/F) \to R_{p^k}(A/F) \to \text{Ш}(A/F)[p^k] \to C_{p^k}$$

where C_{p^k} is the cokernel of the left vertical map in the above diagram. Thus, $\text{Ж}_{p^k}(A/F)$ is a subgroup of $\text{Ш}(A/F)[p^k]$ with quotient in C_{p^k}.

Clark and Sharif proved that the p-torsion of the classical Shafarevich-Tate group of an elliptic curve has unbounded growth in $\mathbb{Z}/p\mathbb{Z}$-extensions of a fixed number field [14]. Inspired by this result, Lim and Murty asked the following natural question

Question. *Let A be an Abelian variety defined over a number field F. Suppose $A(F)[p] \neq 0$. Is*

$$\sup\{r_p\left(\text{Ж}_{p^\infty}(A/L)\right) \mid \ L/F \textit{ is a cyclic extension of degree } p\} = \infty?$$

For the case of elliptic curves, using the unboundedness result of Clark and Sharif, we provide an affirmative answer to the above question. It would be interesting to give an independent proof.

Lemma 3.2.1. *[107, Lemma 3.1] Let $v \mid p$ and $F_v/\mathbb{Q}_p$ be a finite extension of degree n_v. Then*

$$\left|\left(E(F_v)/p^k\right)\right| = p^{k\cdot n_v} \cdot \left|\left(E(F_v)[p^k]\right)\right|.$$

Sketch of Proof. Observe that $E(F_v)$ has finite index in $\widehat{E}(\mathfrak{m}_v^a)$ where, $\widehat{E}$ is the formal group associated to E and $\mathfrak{m}_v^a$ is any power of the maximal ideal in the ring of integers in F_v. Therefore,

$$\frac{\#E(F_v)/p^k}{\#E(F_v)[p^k]} = \frac{\#\widehat{E}(\mathfrak{m}_v^a)/p^k}{\#\widehat{E}(\mathfrak{m}_v^a)[p^k]}.$$

For sufficiently large a, $\widehat{E}(\mathfrak{m}_v^a) \simeq \mathfrak{m}_v^a$ where the isomorphism is given by the formal logarithm [97, Theorem IV.6.4b]. The lemma follows since $\widehat{E}(\mathfrak{m}_v^a)[p^k] = 0$ and $\left|\widehat{E}(\mathfrak{m}_v^a)/p^k\right| = p^{k\cdot n_v}$. ☕

From our earlier discussion, the quotient of $\text{Ш}(E/F)[p^k]$ and $\text{Ж}_{p^k}(E/F)$ is contained in the cokernel

C_{p^k} of the map $E(F)/p \to \oplus_{v|p} E(F_v)/p^k$. By Lemma 3.2.1, the codomain of this map has size bounded by $p^{k[F:\mathbb{Q}]} \prod_{v|p} \left|E(F_v)[p^k]\right|$. This proves the following result.

Proposition 3.2.2. *[107, Proposition 3.2] The index of $\text{Ж}_{p^k}(E/F)$ inside $\text{Ш}(E/F)[p^k]$ is bounded by*

$$\left[\text{Ш}(E/F)[p^k] : \text{Ж}_{p^k}(E/F)\right] \leq p^{k[F:\mathbb{Q}]} \prod_{v|p} \left|E(F_v)[p^k]\right| \tag{3.11}$$

The question asked by Lim-Murty concerns the case $k = 1$. Consider an elliptic curve E over a number field F. Let L/F be a degree p cyclic extension and w be a prime above p in L. For $w|p$, $\left|E(L_w)[p]\right|$ is finite and bounded [97, Corollary III.6.4b]. Since L is a number field, there are finitely many primes $w|p$ in L. Therefore, $\prod_{w|p} \left|E(L_w)[p]\right|$ is finite and bounded, as we vary over all $\mathbb{Z}/p\mathbb{Z}$-extensions L/F.

In [14], Clark and Sharif proved the following theorem on the unboundedness of the Shafarevich-Tate group of elliptic curves.

Theorem 3.2.3. *Let E/F be an elliptic curve. For any positive integer r, there exists $\mathbb{Z}/p\mathbb{Z}$ field extensions L/F such that $\text{Ш}(E/L)$ contains at least r elements of order p i.e. there exists a $\mathbb{Z}/p\mathbb{Z}$ field extension L/F such that $\text{Ш}(E/L)[p]$ is arbitrarily large.*

The above results together give an affirmative answer to the question of Lim-Murty for elliptic curves.

Theorem 3.2.4. *Let E be an elliptic curve defined over a number field F with $E(F)[p] \neq 0$. Varying over all $\mathbb{Z}/p\mathbb{Z}$-extensions L/F, the p-fine Shafarevich-Tate group $\text{Ж}_p(E/L)$ can be arbitrarily large.*

More generally for Abelian varieties, we know $\text{Ж}_p(A/F)$ is a subgroup of $\text{Ш}(A/F)[p]$ with quotient in C_p. We have $\left|C_p\right| \leq \left|A(F_v)/pA(F_v)\right| \leq \left|H^1(F_v, A[p])\right|$. The right hand side of the inequality is finite and bounded independent of the discriminant [76, Theorem 7.1.8(iii)]. The following result is immediate.

Proposition 3.2.5. *Let A be an Abelian variety defined over a number field F. Varying over all $\mathbb{Z}/p\mathbb{Z}$-extensions L/F, $\text{Ж}_p(A/L)$ is unbounded if and only if $\text{Ш}(A/L)[p]$ is unbounded.*

Remark 3.2.6.

1. Theorem 3.2.4 can be obtained independent of the results of Wuthrich [107]. It follows from Proposition 3.2.5 and the result of Clark-Sharif (Theorem 3.2.3).
2. In [26], Creutz has proven results on the unboundedness of $\text{Ш}(A/L)[p]$ under certain hypothesis.

3.3 Growth in $\mathbb{Z}_p^d$-Extensions

In a series of papers in the 1980s, Cuoco and Monsky studied the growth of ideal class groups in $\mathbb{Z}_p^d$ extensions of number fields. More precisely, they studied the analogue of Iwasawa's theorem when $d > 1$.

Let F be a number field and d be a fixed positive integer greater than 1. Consider a $\mathbb{Z}_p^d$-extension F_∞/F with $\Gamma_d = \operatorname{Gal}(F_\infty/F) \simeq \mathbb{Z}_p^d$. Let L_∞ (resp. L_∞^S) be the maximal Abelian unramified pro-p extension of F_∞ (resp. with additional property that primes in S are split completely). Write $\Gamma_{d,n} = \Gamma_d^{p^n}$ and $F_n = F_\infty^{\Gamma_{d,n}}$, then F_n/F is the unique $(\mathbb{Z}/p^n\mathbb{Z})^d$-extension of F inside F_∞. If p^{e_n} is the largest power of p that divides the class number of F_n, Monsky proved the following formula [71]

$$e_n = \left(m_0 p^n + l_0 n + \alpha^*\right) p^{(d-1)n} + O(np^{(d-2)n}),$$

for non-negative constants m_0, l_0, and a real constant α^*. If $d = 2$, α^* is rational.

The Iwasawa algebra $\Lambda_d := \Lambda(\Gamma_d) \simeq \mathbb{Z}_p[\![T_1, T_2, \ldots, T_d]\!]$. Furthermore, we know $X_\infty := \mathrm{Gal}(L_\infty/F_\infty)$ and $X_\infty^S := \mathrm{Gal}(L_\infty^S/F_\infty)$ are modules over this Iwasawa algebra. Set $\overline{\Lambda}_d$ to be the completion with respect to the powers of the augmentation ideal of the $\mathbb{Z}/p\mathbb{Z}$ group ring of Γ_d, i.e.

$$\overline{\Lambda}_d \simeq \mathbb{Z}/p\mathbb{Z}[\![T_1,\ T_2,\ \ldots,\ T_d]\!].$$

Let $\overline{X_\infty}$ (resp. $\overline{X_\infty^S}$) be the reduction mod p of the Iwasawa-Greenberg module X_∞ (resp. S-Iwasawa-Greenberg module X_∞^S). Define a (resp. a') to be the *height* of the local ring $\overline{\Lambda}_d/\operatorname{Ann}(\overline{X_\infty})$ (resp. $\overline{\Lambda}_d/\operatorname{Ann}(\overline{X_\infty^S})$); so $1 \leq a$ (resp. a') $\leq d$.

We state without proof the main result on p-ranks of ideal class groups proved by Monsky.

Theorem 3.3.1. *[73, Theorem 1.9] With notation as described in the last paragraph, there is a positive real constant c, such that*

$$r_p\left(\mathrm{Cl}(F_n)\right) = cp^{an} + O\left(p^{(a-1)n}\right).$$

When $a = 1$, c is an integer. When $a = d$, c is the rank of $\overline{X_\infty}$ over $\overline{\Lambda}_d$.

We prove two results on the p-rank growth in $\mathbb{Z}_p^d$-extension of a number field. In a specific $\mathbb{Z}_p^2$ extension, we obtain a precise formula for the p-rank growth of fine Selmer groups. In the general setting, we can only show that the growth of the p-rank is unbounded.

3.3.1 Growth in a Certain $\mathbb{Z}_p^2$-Extension

Consider the setting of Section 2.2.3. We prove the following result.

Proposition 3.3.2. *Let E be an elliptic curve over the imaginary quadratic field K, such that it has CM by $\mathcal{O}_K$. Set $F = K(E[p])$ and F_∞ be the trivialising extension. Then*

$$\left| r_p\left(R\left(E/F_n\right)\right) - 2r_p\left(\mathrm{Cl}\left(F_n\right)\right)\right| = O(1)$$

where $F_n = K(E[p^n])$ is a $(\mathbb{Z}/p^n\mathbb{Z})^2$-extension of F contained in F_∞.

By [87, Lemma 2] (or [95]), it is guaranteed that E attains good reduction at *all* primes of F. Since the definition of $R(E/F_n)$ is independent of S, we choose $S = S_p \cup S_\infty$. In the $\mathbb{Z}_p^2$-extension $\mathrm{Gal}(F_\infty/F)$, the primes above p ramify and *all* ramified primes are finitely decomposed. In fact, in this setting all primes are finitely decomposed but we will not require this more general fact.

Proof of Proposition 3.3.2. The proposition is proved in three steps. First, we show

$$\left| r_p\left(\mathrm{Cl}(F_n)\right) - r_p\left(\mathrm{Cl}_S(F_n)\right)\right| = O(1). \tag{3.12}$$

In the second step we prove

$$\left| r_p\left(R_p(E/F_n)\right) - r_p\left(R(E/F_n)\right)\right| = O(1). \tag{3.13}$$

In the last step, we draw the final conclusion using Remark 3.1.9.
Step 1: The proof is *almost* identical to that of Equation 3.8. The key point is that primes above p are finitely decomposed in this multiple $\mathbb{Z}_p$-extension.

Set the notation $S_f(F_n)$ to denote the set of finite primes of F_n above the non-Archimedean primes of S. In our case, $S_f(F_n)$ is the set of primes above p in F_n. For each n, we have the exact sequence

$$\mathbb{Z}^{|S_f(F_n)|} \to \mathrm{Cl}(F_n) \xrightarrow{\alpha_n} \mathrm{Cl}_S(F_n) \to 0.$$

Since $\ker(\alpha_n) \subseteq \mathrm{Cl}(F_n)$, it is finite with p-rank less than equal to $\big|S_f(F_n)\big|$. Equation 3.12 follows from Lemma 3.1.5 and noticing the primes above p are finitely decomposed.

Step 2: Consider the commutative diagram below.

$$\begin{tikzcd}
0 \arrow[r] & R_p(E/F_n) \arrow[r] \arrow[d, "s_n"] & H^1(G_S(F_n),\ E[p]) \arrow[r] \arrow[d, "f_n"] & \bigoplus_{v\in S(F_n)} H^1(F_{n,v_n},\ E[p]) \arrow[d, "\gamma_n"] \\
0 \arrow[r] & R(E/F_n)[p] \arrow[r] & H^1(G_S(F_n),\ E[p^\infty])[p] \arrow[r] & \bigoplus_{v_n\in S(F_n)} H^1(F_{n,v_n},\ E[p^\infty])[p]
\end{tikzcd}$$

Both f_n and γ_n are surjective. The kernel of these maps are

$$\ker(f_n) = {E(F_n)[p^\infty]}\Big/{p}$$
$$\ker(\gamma_n) = \bigoplus_{v_n\in S(F_n)} {E(F_{n,v_n})[p^\infty]}\Big/{p}$$

Observe that $r_p\left(\ker\left(s_n\right)\right) \leq r_p\left(\ker\left(f_n\right)\right) \leq 2$. It follows that $r_p\left(\ker\left(\gamma_n\right)\right) \leq 2\big|S_f(F_n)\big|$. It follows that $r_p\left(\mathrm{coker}\left(s_n\right)\right)$ is finite and bounded. Lemma 3.1.5 for the map s_n gives Equation 3.13.

Step 3: In Remark 3.1.9 we showed $r_p\left(R_p(E/F_n)\right) = 2r_p\left(\mathrm{Cl}_S(F_n)\right)$. The proposition follows from this equality and the previous two steps. ☕

The following result is a straightforward corollary of Monsky's theorem (Theorem 3.3.1).

Theorem 3.3.3. *Let E be an elliptic curve over an imaginary quadratic field K, such that it has CM by $\mathcal{O}_K$. Set $F = K(E[p])$ and F_∞ be the trivialising extension. Then for F_n and a as defined before,*

$$r_p\left(R(E/F_n)\right) = cp^{an} + O(p^{(a-1)n}).$$

When $a = 1$, c is an integer and when $a = 2$, $c = \mathrm{rank}_{\overline{\Lambda}_2}(\overline{X_\infty})$.

Proof. Consider Theorem 3.3.1 with $d = 2$. Apply this to Proposition 3.3.2. ☕

Remark 3.3.4. When $a = 1$, by [73, Theorem 1.18] there exists a *periodic function* δ_n such that

$$r_p\left(R(E/F_n)\right) = cp^{an} + \delta_n.$$

3.3.2 Growth in a General $\mathbb{Z}_p^d$ Extension

Using [73], we prove that in a general $\mathbb{Z}_p^d$-extension, the fine Selmer rank growth is unbounded.

Lemma 3.3.5. *Let F_∞ be a $\mathbb{Z}_p^d$ extension of F and F_n be a subfield of F_∞ such that $[F_n : F] = p^{nd}$. Let $S = S_p \cup S_\infty$. Then*

$$\Big| r_p\left(\mathrm{Cl}(F_n)\right) - r_p\left(\mathrm{Cl}_S(F_n)\right) \Big| = O(1).$$

Proof. The proof is the same as that of *Step 1* of Proposition 3.3.2, since primes above p undergo finite decomposition in F_∞/F (see [27, Page 249]). ☕

Remark 3.3.6. If F_∞/F is the compositum of $\mathbb{Z}_p$-extensions where *all* primes are finitely decomposed, it is possible to drop the hypothesis $S = S_p \cup S_\infty$.

Proposition 3.3.7. *Let A be an Abelian variety defined over F and p be an odd prime. Suppose A has good reduction everywhere over F and $A(F)[p] \neq 0$. Let F_∞ be a $\mathbb{Z}_p^d$-extension of F and F_n be a subfield of F_∞ such that $[F_n : F] = p^{nd}$. Then*

$$r_p\left(R(A/F_n)\right) \geq r_p\left(\mathrm{Cl}(F_n)\right) r_p\left(A(F_n)[p]\right) + O(1) \tag{3.14}$$

Proof. Recall Lemma 3.1.8. We had shown that

$$r_p\left(R_p(A/F)\right) \geq r_p\left(\mathrm{Cl}_S(F)\right) r_p(A(F)[p]) - 2d$$

holds for any d-dimensional Abelian variety A defined over F and p an odd prime such that $A(F)[p] \neq 0$. The set S was a finite set of primes in F chosen to contain the Archimedean primes, the primes of bad reduction of A, and the primes above p. But, $r_p\left(R(A/F)\right) \geq r_p\left(R_p(A/F)\right)$. Therefore

$$r_p\left(R(A/F)\right) \geq r_p\left(\mathrm{Cl}_S(F)\right) r_p(A(F)[p]) - 2d. \tag{3.15}$$

If an Abelian variety A has good reduction everywhere over F, then it also has good reduction everywhere over F_n. The same argument is valid at every layer F_n/F in the $\mathbb{Z}_p^d$-tower.

The definition of $R(A/F_n)$ is independent of S. By hypothesis, we may choose $S = S(F_n) = S_\infty \cup S_p$. For each layer, the result follows from Inequality 3.15 and Lemma 3.3.5. ☕

Remark 3.3.8. In view of Remark 3.3.6, if F_∞/F is the compositum of $\mathbb{Z}_p$-extensions where *all* primes are finitely decomposed, we may drop the hypothesis that A has good reduction everywhere over F.

Theorem 3.3.9. *Let A be an Abelian variety defined over F, p be an odd prime such that $A(F)[p] \neq 0$. Suppose A has good reduction everywhere over F. Let F_∞/F be a $\mathbb{Z}_p^d$ extension such that $\overline{X_\infty}$ is infinite. Let F_n/F be the n-th layer of this tower. Then as $n \to \infty$, $r_p\left(R(A/F_n)\right)$ is unbounded.*

Proof. We are in the same setting as Proposition 3.3.7. By Monsky's theorem on p-ranks, $\overline{X_\infty}$ being infinite implies that $r_p\left(\mathrm{Cl}(F_n)\right)$ is unbounded as $n \to \infty$. The theorem follows. ☕

Remark 3.3.10. In view of Proposition 3.3.8, if F_∞/F is the compositum of $\mathbb{Z}_p$-extensions where *all* primes are finitely decomposed, we do not need to assume that A has good reduction everywhere over F. By the same argument, if F_∞/F is any $\mathbb{Z}_p^d$-extension such that all primes in S_{bad} are finitely decomposed, we can drop the hypothesis A has good reduction everywhere over F and choose $S = S_p \cup S_{bad} \cup S_\infty$.

The following version of Monsky's Theorem will allow us to prove a variant of Theorem 3.3.9 for all $\mathbb{Z}_p^d$-extensions of F without assuming A has good reduction everywhere.

Theorem 3.3.11. *With notation introduced at the start of the section, there is a positive real constant c, such that*

$$r_p\left(\mathrm{Cl}_S(F_n)\right) = cp^{a'n} + O\left(p^{(a'-1)n}\right).$$

The fact that $c > 0$, follows from [72, Corollary to Theorem 1.8].

Theorem 3.3.12. *Let A be an Abelian variety defined over F, p be an odd prime such that $A(F)[p] \neq 0$. Let F_∞/F be a $\mathbb{Z}_p^d$ extension such that $\overline{X_\infty^S}$ is infinite. Let F_n/F be the n-th layer of this tower. Then as $n \to \infty$, $r_p\left(R(A/F_n)\right)$ goes to infinity.*

Proof. By Theorem 3.3.11, if $\overline{X_\infty^S}$ is infinite then $r_p\left(\mathrm{Cl}_S(F_n)\right)$ approaches infinity as $n \to \infty$. The conclusion follows from Inequality 3.15 which is independent of the reduction type at p. ☕

Remark 3.3.13. In Theorem 3.3.12, we do not impose any restrictions on the reduction type at p. This comes at a cost that we require a smaller group $\overline{X_\infty^S}$ to be infinite.

3.3.3 Growth in Non-Cyclotomic $\mathbb{Z}_p$-Extensions

Growth of fine Selmer groups in cyclotomic $\mathbb{Z}_p$-extensions will be studied in Chapter 5. Here, we deduce an immediate variant of Proposition 3.3.7 with interesting consequences in non-cyclotomic towers.

Let F be a number field and F_∞/F be *any* $\mathbb{Z}_p$-extension with $\Gamma = \mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}_p$. We know that the Iwasawa algebra $\Lambda(\Gamma)$ can be identified with a formal power series ring in one variable $\mathbb{Z}_p[\![T]\!]$. The structure theorem asserts that for a finitely generated $\Lambda(\Gamma)$-module M, there is a pseudo-isomorphism

$$M \to \Lambda(\Gamma)^r \oplus \bigoplus_{i=1}^{s} {\Lambda(\Gamma)}\Big/{(p^{m_i})} \oplus \bigoplus_{j=1}^{t} {\Lambda(\Gamma)}\Big/{\left(f_j^{l_j}\right)} \tag{3.16}$$

where $s,\ t$ are finite, $m_i,\ l_j > 0$, and each f_j is a distinguished polynomial.

The following lemma is an easy consequence of the structure theorem.

Lemma 3.3.14. *[59, Lemma 5.3] Let M be a finitely generated $\Lambda(\Gamma)$-module and $w_n = (1+T)^{p^n} - 1$. For $n \gg 0$,*

$$r_p\left({M}\Big/{(p, w_n)\, M}\right) = \left(r(M) + s(M)\right) p^n + O(1)$$

Proof. Computing the terms in the summands, for $n \gg 0$

$$\begin{aligned}
r_p\left({\Lambda(\Gamma)}\Big/{(p, w_n)\Lambda(\Gamma)}\right) &= r_p\left({\mathbb{Z}/p\mathbb{Z}[T]}\Big/{T^{p^n}}\right) && = p^n \\
r_p\left({\left(\Lambda(\Gamma)/p^{m_i}\right)}\Big/{(p, w_n)}\right) &= r_p\left({\mathbb{Z}/p\mathbb{Z}[T]}\Big/{T^{p^n}}\right) && = p^n \\
r_p\left({\left(\Lambda(\Gamma)/f_j^{l_j}\right)}\Big/{(p, w_n)}\right) &= r_p\left({\mathbb{Z}/p\mathbb{Z}[T]}\Big/{\left(T^{p^n},\ f_j^{l_j}\right)}\right) && = l_j \deg(f_j)
\end{aligned}$$

The lemma is now immediate. ☕

Let A/F be an Abelian variety. The Pontryagin dual of the fine Selmer group over the $\mathbb{Z}_p$-extension F_∞/F is denoted by $\mathfrak{Y}(A/F_\infty)$. Note

$${\mathfrak{Y}(A/F_\infty)}\Big/{p\mathfrak{Y}(A/F_\infty)} \simeq \left(R(A/F_\infty)[p]\right)^\vee .$$

Proposition 3.3.7 for finitely generated $\Lambda(\Gamma)$-modules will allow us to prove a fine version of a theorem of Lim and Murty [59, Theorem 5.6] and Česnavičius [11, Proposition 7.1].

Theorem 3.3.15. *Let $p \neq 2$. Let A be an Abelian variety defined over F with good reduction everywhere over F and $A(F)[p] \neq 0$. Let F_∞ be any $\mathbb{Z}_p$-extension of F. Then*

$$r\left(\mathfrak{Y}(A/F_\infty)\right) + s\left(\mathfrak{Y}(A/F_\infty)\right) \geq s\left(X(F_\infty)\right) r_p\left(A(F_\infty)[p]\right)$$

where $X(F_\infty)$ is the Iwasawa module over the $\mathbb{Z}_p$-extension.

Proof. Set $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$. Consider the following commutative diagram with the vertical maps given by restriction

$$\begin{tikzcd}
0 \arrow[r] & R(A/F_n) \arrow[r] \arrow[d, "s_n"] & H^1(G_S(F_n),\ A[p^\infty]) \arrow[r] \arrow[d, "f_n"] & \bigoplus_{v_n} H^1(F_{n,v_n},\ A[p^\infty]) \arrow[d, "\gamma_n"] \\
0 \arrow[r] & R(A/F_\infty)^{\Gamma_n} \arrow[r] & H^1(G_S(F_\infty),\ A[p^\infty])^{\Gamma_n} \arrow[r] & \left(\varinjlim_n \bigoplus_{v_n} H^1(F_{n,v_n},\ A[p^\infty])\right)^{\Gamma_n}
\end{tikzcd}$$

Note that $r_p\left(\ker(f_n)\right) \leq 2d$. Thus, $\ker(s_n)$ has bounded p-rank. Using Lemma 3.3.14

$$\begin{aligned}\left(r\left(\mathfrak{Y}(A/F_\infty)\right) + s\left(\mathfrak{Y}(A/F_\infty)\right)\right)p^n &\geq r_p\left(R(A/F_n)\right) + O(1)\\ &\geq r_p\left(\mathrm{Cl}(F_n)\right) r_p\left(A(F_n)[p]\right) + O(1)\end{aligned}$$

where the last inequality follows from Proposition 3.3.7. There exists n_0, such that for $n \geq n_0$

$$\mathrm{Cl}(F)\Big/ p\,\mathrm{Cl}(F) \to X(F_\infty)\Big/\left(p,\, \tfrac{w_n}{w_{n_0}}\right) \to 0.$$

The kernel of this map is bounded independent of n (see [76, Lemma 11.1.5]). Since $X(F_\infty)$ is *always* a finitely generated *torsion* $\Lambda(\Gamma)$-module, it follows from Lemma 3.3.14 that

$$r_p\left(\mathrm{Cl}(F_n)\right) = s(X(F_\infty))p^n + O(1).$$

The result follows since $r_p(A(F_\infty)[p]) = r_p(A(F_n)[p])$ for n sufficiently large. ☕

Corollary 3.3.16. *Let $p \neq 2$. Given an Abelian variety A over a number field F, there exists a finite extension L/F and a $\mathbb{Z}_p$-extension L_∞/L, such that $\mathfrak{Y}(A/L_\infty)$ is not $\Lambda(\Gamma)$-torsion or $\mu(\mathfrak{Y}(A/L_\infty)) > 0$.*

Proof. Given a fixed positive integer N, there exists a finite extension F'/F and a $\mathbb{Z}_p$-extension F'_∞/F', such that μ-invariant of the corresponding Iwasawa module $X(F'_\infty)$ is positive; in fact $\mu\left(X(F'_\infty)\right) > N$ [49, Theorem 1]. Therefore, $s\left(X(F'_\infty)\right)$ must be positive.

Consider a finite extension L/F' such that A has good reduction everywhere over L and $A[p] \subseteq A(L)$. Consider $L_\infty = LF'_\infty$, this is a $\mathbb{Z}_p$-extension of L. We know $\mu\left(X(L_\infty)\right) \geq \mu\left(X(F'_\infty)\right)$ [49]. Thus,

$$\begin{aligned}r\left(\mathfrak{Y}(A/L_\infty)\right) + \mu\left(\mathfrak{Y}(A/L_\infty)\right) &\geq r\left(\mathfrak{Y}(A/L_\infty)\right) + s\left(\mathfrak{Y}(A/L_\infty)\right)\\ &\geq s\left(X(L_\infty)\right) r_p(A(L_\infty)[p])\\ &\geq s\left(X(F'_\infty)\right) r_p(A(L_\infty)[p])\\ &> 0.\end{aligned}$$

If $r\left(\mathfrak{Y}(A/L_\infty)\right)$ is positive, it follows $\mathfrak{Y}(A/L_\infty)$ is not $\Lambda(\Gamma)$-torsion. Else, $s\left(\mathfrak{Y}(A/L_\infty)\right)$ is positive, hence the μ-invariant is positive. With this the proof is complete. ☕

Remark 3.3.17. The Abelian variety analogue of the weak Leopoldt Conjecture is believed to be true for all $\mathbb{Z}_p$-extensions of a number field F. By Remark 2.5.2, this is equivalent to $\mathfrak{Y}(A/F_\infty)$ being $\Lambda(\Gamma)$-torsion; conjecturally $r\left(\mathfrak{Y}(A/F_\infty)\right)$ should always be 0. However, there is little unconditional evidence towards this claim for an anti-cyclotomic $\mathbb{Z}_p$-extension. Conditional on the *Heegner hypothesis*, Bertolini proved the elliptic curve analogue of the weak Leopoldt Conjecture for the anti-cyclotomic extension of an imaginary quadratic field [4].

The close relationship between fine Selmer groups and class groups in $\mathbb{Z}_p$-extensions raises the following natural question: does an analogue of Iwasawa's theorem for anti-cyclotomic $\mathbb{Z}_p$-extensions [49, Theorem 1] hold for fine Selmer groups, i.e. can the μ-invariant associated with a fine Selmer group be arbitrarily large in an anti-cyclotomic $\mathbb{Z}_p$-extension. For the rest of this section, we focus on this question and answer it in the affirmative.

Review of Iwasawa's Result

We will begin by recalling a result of Chevalley [13] on *ambiguous class number formula* which was crucially used in Iwasawa's proof.

Definition 3.3.18. *Let F be a number field and L/F be a cyclic $\mathbb{Z}/p\mathbb{Z}$-extension with σ a generator of the Galois group $G = \mathrm{Gal}(L/F)$. An ideal class $[\mathfrak{a}] \in \mathrm{Cl}(L)$ is called*

- ***ambiguous** if $[\mathfrak{a}]^\sigma = [\mathfrak{a}]$, i.e. there exists an element $\alpha \in L^\times$ such that $\mathfrak{a}^{\sigma-1} = (\alpha)$.*
- ***strongly ambiguous** if $\mathfrak{a}^{\sigma-1} = (1)$.*

The subgroup of the class group $\mathrm{Cl}(L)$ consisting of ambiguous ideal classes is denoted by $\mathrm{Am}(L/F)$. The subgroup of strongly ambiguous ideal classes is denoted $\mathrm{Am}_{\mathrm{st}}(L/K)$.

Ambiguous Class Number Formula. *The number of ambiguous ideal classes is given by*

$$\#\,\mathrm{Am}(L/F) = h(F) \times \frac{p^{T-1}}{[E_F : E_F \cap NL^\times]} \tag{3.17}$$

$$\#\,\mathrm{Am}_{\mathrm{st}}(L/F) = h(F) \times \frac{p^{T-1}}{[E_F : NE_L]} \tag{3.18}$$

where $h(F)$ is the class number of the base field F, T is the number of ramified primes, E_F is the unit group of F, and $E_F \cap NL^\times$ is the subgroup of units that are norms of elements of L. Moreover, the above two formulas are equivalent.

Proof. See [58, Theorem 1]. ☕

We will require a p-rank version of the (ambiguous) class number formula.

Proposition 3.3.19. *Let F be a number field and L/F be a cyclic $\mathbb{Z}/p\mathbb{Z}$-extension with σ a generator of the Galois group $G = \mathrm{Gal}(L/F)$. Let D be the degree of the extension $F/\mathbb{Q}$ and T be the number of primes of F that ramify in L. Then,*

$$r_p\left(\mathrm{Cl}\left(L\right)\right) \geq T - 1 - D.$$

Sketch. The following inequality of p-ranks is a standard fact [91, Proposition 3.1]

$$r_p\left(\mathrm{Cl}\left(L\right)\right) \geq T - 1 - r_p\left({}^{E_F}\Big/_{E_F \cap N_{L/F}U_L}\right)$$

where U_L is the notation for idéle units.

The proposition follows from the above fact combined with the observations that

$$E_F^p \subseteq E_F \cap N_{L/F}L^\times \subseteq E_F \cap N_{L/F}U_L.$$

Therefore, one can see that

$$r_p\left({}^{E_F}\Big/_{E_F \cap N_{L/F}U_L}\right) \leq r_p\left({}^{E_F}\Big/_{E_F^p}\right) \leq [F:\mathbb{Q}].$$

The last inequality is a consequence of the fact that the quotient ${}^{E_F}\Big/_{E_F^p}$ has order $p^{[F:\mathbb{Q}]}$. ☕

We now sketch the proof of Iwasawa's theorem for non-cyclotomic $\mathbb{Z}_p$-extensions.

Theorem 3.3.20. *[49, Theorem 1] Let F be the cyclotomic field of p-th or 4-th roots of unity according as $p > 2$ or $p = 2$. For any given integer $N \geq 1$, there exists a cyclic extension L/F of degree p and a $\mathbb{Z}_p$-extension L_∞/L such that*

$$\mu\left(X\left(L_\infty\right)\right) \geq N.$$

Sketch of the Proof: The proof can be divided into three main steps.

Step 1: Let F_{ac}/F be an anti-cyclotomic $\mathbb{Z}_p$-extension. Let F_+ be the maximal totally real subfield of F. The anti-cyclotomic $\mathbb{Z}_p$-extension satisfies a special property: if F_n^{ac} is the n-th layer of the $\mathbb{Z}_p$-tower, then F_n^{ac} is Galois over F_+. Furthermore, $G_n = \mathrm{Gal}(F_n^{\mathrm{ac}}/F_+)$ is the dihedral group of order $2p^n$.

Step 2: Let $\mathfrak{l}_+ \nmid p$ be a prime ideal of F_+ which is inert in F, and $\mathfrak{l}$ be the unique prime ideal of F above $\mathfrak{l}_+$. Note $\mathfrak{l}_+$ is unramified in F_n^{ac}. Using group theoretic properties of the dihedral group and class field theory, it can be shown that $\mathfrak{l}$ is *totally split* in F_n^{ac}. This holds for every n, therefore $\mathfrak{l}$ is totally split in F_{ac}/F. By Chebotarev density theorem, there are infinitely many prime ideals $\mathfrak{l}_+$ in F_+ which are inert in F. Thus, there are infinitely many prime ideals $\mathfrak{l}$ in F which split completely in F_{ac}/F.

Step 3: Choose prime ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$, $t \geq 1$, in F which are prime to p and are totally split in F_{ac}/F. We know from Step 2 that there are infinitely many such primes. Let η be a non-zero element of F which is divisible exactly by the first power of $\mathfrak{l}_i$ for $1 \leq i \leq t$. Set

$$L = F\left(\sqrt[p]{\eta}\right); \qquad L_\infty = LF_{\mathrm{ac}}.$$

Note $F_{\mathrm{ac}} \cap L = F$ and L_∞/L is a $\mathbb{Z}_p$-extension. Let L_n be the n-th layer of the $\mathbb{Z}_p$ tower L_∞/L, then

$$L_n = F_n^{\mathrm{ac}}\left(\sqrt[p]{\eta}\right), \qquad n \geq 0.$$

Thus, L_n/F_n is a cyclic extension of degree p. If $p^{e_n^L}$ is the largest power of p dividing the $h(L_n)$, by Theorem 2.1.1, we know that for sufficiently large n,

$$e_n^L = \lambda_L n + \mu_L p^n + \nu_L$$

where $\lambda_L = \lambda(X(L_\infty))$, $\mu_L = \mu(X(L_\infty))$, and $\nu_L = \nu(X(L_\infty))$. Since $\mathfrak{l}_i$ is totally split in F_{ac}/F, it has p^n prime ideal factors in F_n^{ac}. By construction, these prime ideals are ramified in L_n. Let the number of such prime divisors be T_n. It follows that

$$T_n \geq tp^n \qquad n \geq 0.$$

Using Chevalley's ambiguous class number formula,

$$h(L_n) \geq \# \operatorname{Am}(L_n/F_n) \geq h(F_n) \times \frac{p^{T_n - 1}}{p^{d_n}}$$

where $d_n = (p-1)p^n = [F_n : \mathbb{Q}]$. The manipulation of the denominator of the formula follows from the observation that $E_{F_n}^p$ is contained in the subset of units of E_{F_n} which are norms of elements in L_n. Now comparing the p-parts of the above inequality,

$$\begin{aligned} e_n^L &\geq e_n^F + T_n - 1 - d_n \\ &\geq \Big(\mu\left(X\left(F_\infty\right)\right) + t - p + 1\Big) p^n. \end{aligned}$$

Therefore,

$$\mu\left(X\left(L_\infty\right)\right) \geq t - p + 1.$$

The theorem follows, since we know t can be arbitrarily large. ☕

Remark 3.3.21. Theorem 3.3.20 is true for *any* field F which has an anti-cyclotomic $\mathbb{Z}_p$-extension F_{ac}/F. In particular, it is true for all CM fields.

We can now state and prove the main theorem of this section.

Theorem 3.3.22. *Let F be the cyclotomic field of p-th roots of unity for $p > 2$. Let A/F be an Abelian variety of dimension d such that $A(F)[p] \neq 0$. Suppose the analogue of the weak Leopoldt conjecture holds. Given integer $N \geq 1$, there exists a cyclic Galois extension L/F of degree p and a $\mathbb{Z}_p$-extension L_∞/L such that*

$$\mu\Big(\mathfrak{Y}\left(A/L_\infty\right)\Big) \geq N.$$

To prove the theorem, we will need the following lemma. Since the definition of the p-primary fine Selmer group is independent of the choice of S, we set $S = S(L) = S_p \cup S_{bad} \cup S_\infty$. Denote the subset of finite primes of S by S_f. Further, we set $\left|S_f\right| = s_0$

Lemma 3.3.23. *Let F be the cyclotomic field of p-th roots of unity for $p > 2$. Let A/F be an Abelian variety of dimension d such that $A(F)[p] \neq 0$. Suppose the analogue of the weak Leopoldt conjecture holds. Let L/F be a $\mathbb{Z}/p\mathbb{Z}$ extension as constructed in Theorem 3.3.20. Then,*

$$r_p\left(R(A/L_n)\right) \geq r_p\left(A\left(L_n\right)[p]\right)\Big(s\left(X(L_\infty)\right)p^n\Big) - 4ds_0p^n + c$$

where c is a constant.

Proof. The proof follows the same steps as Proposition 3.3.2. Since primes in the $\mathbb{Z}_p$-extension L_∞/L no longer satisfy the condition that primes are finitely decomposed, our analysis will be more intricate.

Step 1: By [76, Lemma 10.3.12], we have the following short exact sequence for all n,

$$\mathbb{Z}^{|S_f(L_n)|} \to \mathrm{Cl}(L_n) \xrightarrow{\alpha_n} \mathrm{Cl}_S(L_n) \to 0.$$

Since primes in S are no longer finitely decomposed in $\mathbb{Z}_p$-extension L_∞/L, by Lemma 3.1.5 we obtain

$$\left| r_p\left(\mathrm{Cl}\left(L_n\right)\right) - r_p\left(\mathrm{Cl}_S\left(L_n\right)\right)\right| \leq 2s_0p^n.$$

Step 2: We imitate the proof of Step 2 of Proposition 3.3.2. This gives

$$\left| r_p\left(R\left(A/L_n\right)\right) - r_p\left(R_p\left(A/L_n\right)\right)\right| \leq 2ds_0p^n.$$

Step 3: Lemma 3.1.8 applied to the number field L_n yields

$$r_p\left(R_p\left(A/L_n\right)\right) \geq r_p\left(\mathrm{Cl}_S\left(L_n\right)\right) r_p\left(A\left(L_n\right)[p]\right) - 2d.$$

From the above two steps, it is evident that

$$\begin{aligned} r_p\left(R\left(A/L_n\right)\right) &\geq r_p\left(R_p\left(A/L_n\right)\right) \\ &\geq r_p\left(\mathrm{Cl}\left(L_n\right) - 2s_0p^n\right) r_p\left(A\left(L_n\right)[p]\right) - 2d \\ &\geq r_p\left(\mathrm{Cl}\left(L_n\right)\right) r_p\left(A\left(L_n\right)[p]\right) - 4ds_0p^n - 2d. \end{aligned}$$

By the Structure Theorem (in particular Lemma 3.3.14), we know that

$$r_p\left(\mathrm{Cl}\left(L_n\right)\right) = s\left(X(L_\infty)\right)p^n + O(1).$$

Plugging this back into the above inequality, proves the lemma. ☕

We will now prove Theorem 3.3.22. The condition A/F is an Abelian variety such that $A(F)[p] \neq 0$ is a mild one. We can base change to an extension F'/F such that $A(F')[p] \neq 0$. Theorem 3.3.22 can then be stated (and proved) in terms of this extension F'.

Proof of Theorem 3.3.22. Let L/F be a cyclic extension of degree p as constructed in Iwasawa's theorem (cf. Theorem 3.3.20). The choice of L/F determines t, the minimum number of primes of F which ramify in L and are totally decomposed in F_{ac}/F. We are assuming that the analogue of the weak Leopoldt Conjecture hold for the $\mathbb{Z}_p$-extension L_∞/L where $L_\infty = LF_{\mathrm{ac}}$. Now,

$$\begin{aligned} s\left(\mathfrak{Y}(A/L_\infty)\right)p^n &\geq r_p\left(R\left(A/L_n\right)\right) + O(1) \\ &\geq r_p\left(A\left(L_n\right)[p]\right)\left(s\left(X(L_\infty)\right)p^n\right) - 4ds_0p^n + O(1) \\ &\geq r_p\left(A\left(L_n\right)[p]\right)\left(t-(p-1)-4ds_0\right)p^n + O(1) \end{aligned}$$

The first inequality follows from Lemma 3.3.14. The last line follows from Proposition 3.3.19 by observing that at least tp^n primes of F_n ramify in L_n (by construction) and $[F_n : \mathbb{Q}] = (p-1)p^n$. We discussed while sketching the proof of Theorem 3.3.20 that t can be chosen to be arbitrarily large. Therefore, given

$N \geq 1$ there exists L/F such that

$$s\left(\mathfrak{Y}(A/L_\infty)\right) \geq N.$$

Since $\mu\left(\mathfrak{Y}(A/L_\infty)\right) \geq s\left(\mathfrak{Y}(A/L_\infty)\right)$, the theorem follows.

Remark 3.3.24. In view of recent results of Hajir-Maire [42], we believe it might be possible to extend Theorem 3.3.22 to more general situations.

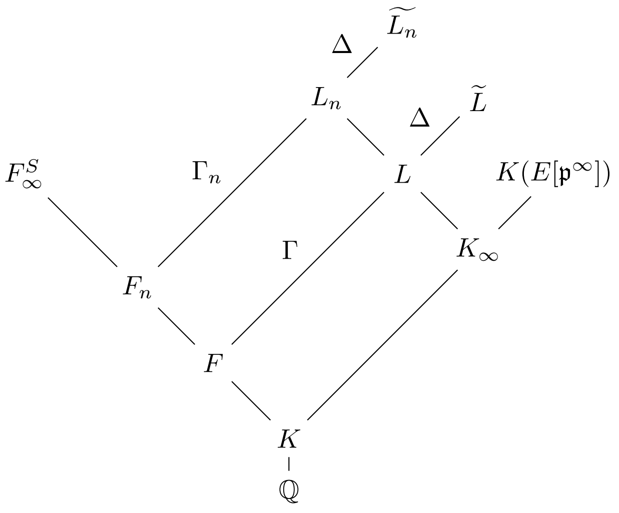
3.4 Growth in p-Hilbert Class Field Tower

Recall the setting of Section 2.2.3: F is a finite Galois extension over the imaginary quadratic field K, $\mathfrak{p}|p$ is an unramified prime in F, and E is an elliptic curve defined over F with CM by $\mathcal{O}_K$.

Denote by F_∞^S the maximal unramified p-extension of F such that all primes in S split completely. Set $\Sigma = \Sigma_F = \mathrm{Gal}(F_\infty^S/F)$ and write $\{\Sigma_n\}_{n\geq 0}$ for its derived series. Here, for each $n \geq 0$, the fixed field F_n corresponding to Σ_n is the p-Hilbert S-class field of F_{n-1}.

Set $L_n = F_nL$ for every $n \geq 0$. Note L_n is the ***unique*** $\mathbb{Z}_p$-extension of F_n inside $\widetilde{L_n} = F_n(E[\mathfrak{p}^\infty])$, which is unramified outside $\mathfrak{p}$. Denote by Γ_n the Galois group $\mathrm{Gal}(L_n/F_n)$; note $\Gamma_n \simeq \mathbb{Z}_p$. We emphasize Γ_n is not a multiple $\mathbb{Z}_p$-extension in this section.

The field diagram is drawn below for convenience.



For every $n \geq 0$ we have the following isomorphisms

$$\mathrm{Gal}(\widetilde{L_n}/L_n) \simeq \mathrm{Gal}(\widetilde{L}/L) = \Delta; \quad \mathrm{Gal}(\widetilde{L_n}/F_n) \simeq \Delta \times \Gamma_n,$$

where Δ is a subgroup of μ_{p-1}.

Set $r_1(F)$ and $r_2(F)$ to denote the number of real and complex embeddings of F respectively. In [33], Golod and Shafarevich proved that if the following inequality holds

$$r_p\left(\mathrm{Cl}_S(F)\right) \geq 2 + 2\sqrt{r_1(F) + r_2(F) + \delta + \left|S \setminus S_\infty\right|},$$

then Σ_F is infinite. This is referred to as the **Golod-Shafarevich inequality**. Here,

$$\delta = \begin{cases} 1 & \text{if } \mu_p \subseteq F \\ 0 & \text{otherwise.} \end{cases}$$

Little is known about the structure of the Galois group Σ_F. Stark posed the following natural question.

Question. *Assume the Golod-Shafarevich inequality holds. Is $r_p(\mathrm{Cl}_S(F_n))$ bounded as $n \to \infty$?*

This question is equivalent to asking

Question. *Assume the Golod-Shafarevich inequality holds. Is Σ_F a p-adic analytic group, i.e. is Σ_F a pro-p group which is a Lie group over the field of p-adic numbers?*

The equivalent formulation can be understood as follows. For any pro-p group G, $\mathbb{Z}/p\mathbb{Z}$ is a trivial G-module. In particular, take $G = \Sigma_n$, the n-th term of the derived series. By class field theory and finiteness of $\mathrm{Cl}(F_n)$ (and hence of $\mathrm{Cl}_S(F_n)$)

$$\begin{aligned} r_p\left(\mathrm{Cl}_S(F_n)\right) &= r_p\left(\mathrm{Cl}_S\left(F_n\right)/p\right) \\ &= \dim_{\mathbb{Z}/p\mathbb{Z}}\left(H^1\left(\mathrm{Gal}\left(H_S\left(F_n\right)/F_n\right),\ \mathbb{Z}/p\mathbb{Z}\right)\right) \\ &= \dim_{\mathbb{Z}/p\mathbb{Z}}\left(H^1\left(\Sigma_n,\ \mathbb{Z}/p\mathbb{Z}\right)\right) \\ &= \dim_{\mathbb{Z}/p\mathbb{Z}} \mathrm{Hom}\left(\Sigma_n,\ \mathbb{Z}/p\mathbb{Z}\right). \end{aligned}$$

This is the number of *minimal generators* of Σ_n. By the following theorem of Lubotzky and Mann, the two questions are equivalent.

Theorem 3.4.1. *[62, Theorem A] A pro-p group is p-adic analytic if and only if the ranks of its open subgroups are bounded.*

This question posed by Stark is in fact closely related to the Fontaine-Mazur conjecture. In [31], Fontaine and Mazur conjectured (as a special case of a vast principle) that Σ_F can not be an infinite pro-p analytic group. There are unconditional answers to Stark's question. The following theorem was proven independently by Boston [8], Hajir [41], and Matar [63].

Theorem 3.4.2. *Let F be a number field. If the Golod-Shafarevic inequality holds, then Σ_F is not p-adic analytic.*

3.4.1 Main Result and its Proof

In view of Theorem 3.4.2, we can not hope to study the growth of fine Selmer groups in the p-Hilbert class field tower using traditional Iwasawa theoretic tools.

Before we can state the main result of this section, we will make a few definitions.

(i) Analogous to the definition of p-fine Selmer group and p-primary fine Selmer group, define $\mathfrak{p}$-fine Selmer group and $\mathfrak{p}$-primary fine Selmer group by replacing p with $\mathfrak{p}$ everywhere in the definitions.

(ii) When M is an $\mathcal{O}$-module, write $M_{\mathfrak{p}}$ for its $\mathfrak{p}$-primary part. Define the $\mathbb{Z}/p\mathbb{Z}$-rank of $M_{\mathfrak{p}}[\mathfrak{p}]$ as the **$\mathfrak{p}$-rank** of M, and denote it by $r_{\mathfrak{p}}(M)$.

Theorem 3.4.3. *Let F be a finite Galois extension of the imaginary quadratic field K. Let $p \neq 2,\ 3$ be a prime that splits in K as $\mathfrak{p}\bar{\mathfrak{p}}$ such that $\mathfrak{p}$ is unramified in F/K. Let E be an elliptic curve over F with CM by $\mathcal{O}_K$ such that $E(F)[\mathfrak{p}] \neq 0$. Choose S to be a finite set of primes in F containing the Archimedean primes, primes above $\mathfrak{p}$, and primes where E has bad reduction. Assume F satisfies the Golod-Shafarevich inequality. Let F_∞^S be the maximal unramified non-constant pro-p extension of F where primes in S split completely; let F_n be the n-th layer of this class field tower. Then the $\mathfrak{p}$-rank of the fine Selmer group of E/F_n is unbounded as $n \to \infty$.*

Remark 3.4.4.

1. The result of Lim-Murty [59, Theorem 6.2] crucially needs $E(F)[\mathfrak{p}] \neq 0$ (else, the inequality they establish is vacuous). We expect Theorem 3.4.3 should hold without assuming $E(F)[\mathfrak{p}] \neq 0$. This assumption in our theorem forces $L_n = \widetilde{L_n}$, which simplifies notation considerably.
2. Theorem 3.4.3 is the fine Selmer variant of a result of Murty-Ouyang [75, Theorem 4]. Our result implies their result; indeed, we show the fine Selmer rank (hence the Selmer rank) is unbounded in the p-Hilbert S-class field tower (hence in the p-Hilbert class field tower).
3. Theorem 3.4.3 also implies the result of Lim-Murty [59, Theorem 6.2].

We begin by making the following observations.

Lemma 3.4.5. *If $E(F)[\mathfrak{p}]$ is trivial, then $L_n \neq \widetilde{L_n}$ and $E(L_n)[\mathfrak{p}] = 0$ for every $n \geq 0$. If $E[\mathfrak{p}] \subset E(F)$, then $L_n = \widetilde{L_n}$ and for every $n \geq 0$, $E(L_n)[\mathfrak{p}] = E[\mathfrak{p}^\infty]$.*

Proof. Either $E(F)[\mathfrak{p}]$ is trivial or it is all of $E[\mathfrak{p}]$. Therefore, by Lemma 3.1.4 there are only two possibilities for $E(L_n)[\mathfrak{p}]$. ☕

Lemma 3.4.6. *The intersection of F_∞^S and L is a finite extension of F. In particular, if $E[\mathfrak{p}] \subseteq E(F)$ then F_∞^S and L are disjoint over F.*

Proof. Consider the intersection $F_\infty^S \cap L$. This is an Abelian extension of F as L/F is a $\mathbb{Z}_p$-extension and hence Abelian. By construction, the maximal Abelian quotient of F_∞^S/F is the p-Hilbert S-class field F_1/F. Thus, $F_\infty^S \cap L \subset F_1$.

When $E[\mathfrak{p}] \subset E(F)$, $L = \widetilde{L}$. Further, the prime $\mathfrak{p}$ is totally ramified in the split prime $\mathbb{Z}_p$-extension L/F. But F_∞^S/F is totally unramified, so the two extensions are disjoint over F. ☕

Thus, we see that the hypothesis in the theorem implies $L_n = \widetilde{L_n}$. Let M_n^S be the maximal Abelian pro-p unramified extension of L_n such that all primes of $S(L_n)$ split completely. Here, $S(L_n)$ is the set of primes in L_n which are above the primes in the finite set S. Note $S(L_n)$ is a finite set. Indeed, L_n/F_n is a split prime $\mathbb{Z}_p$ extension; hence primes of $S(F_n)$ are finitely decomposed in L_n/F_n. Set $\mathfrak{X}_n^S = \mathrm{Gal}(M_n^S/L_n)$. Using standard Iwasawa theory techniques, we have $\mathfrak{X}_n^S$ is a $\mathbb{Z}_p[\Delta][\![T]\!]$-module.

Lemma 3.4.7. *$\mathbb{Z}_p$-corank of $R_{\mathfrak{p}^\infty}(E/L_n) \to \infty$ as $n \to \infty$.*

Proof. Since the Galois action is trivial on $E[\mathfrak{p}^\infty]$, we know by [89, 6.1]

$$R_{\mathfrak{p}^\infty}(E/L_n) = \mathrm{Hom}\left(\mathfrak{X}_n^S,\ E[\mathfrak{p}^\infty]\right).$$

It is therefore enough to show that the $\mathbb{Z}_p[\Delta]$-rank of $\mathfrak{X}_n^S$ tends to ∞.

F_{n+1}/F_n is an Abelian extension where primes in $S(F_n)$ split completely and L_n/F_n is an Abelian extension unramified outside $\mathfrak{p}$. Their compositum is L_{n+1}. Note that the finitely many primes in $S(L_n)$ split completely in L_{n+1}. L_{n+1}/L_n is therefore a subextension of M_n^S/L_n. We have

$$\operatorname{Gal}\big(L_{n+1}/L_n\big) = \operatorname{Gal}\big(F_{n+1}/F_{n+1} \cap L_n\big) = \operatorname{Gal}\big(F_{n+1}/F_n\big)\,;$$

the last equality follows from hypothesis. Theorem 3.4.2 implies that the p-rank of $\operatorname{Gal}(F_{n+1}/F_n)$ approaches ∞. Thus, the p-rank of $\operatorname{Gal}(L_{n+1}/L_n)$ tends to ∞. ☕

Remark 3.4.8. Note $(\mathfrak{X}_n^S)_{\Gamma_n}$ contains the Galois group $\operatorname{Gal}(L_{n+1}/L_n)$. Therefore Lemma 3.4.7 implies $\mathfrak{p}$-rank of $R_{\mathfrak{p}^\infty}(E/L_n)^{\Gamma_n}$ is unbounded as n tends to ∞.

In Chapter 2, we introduced Mazur's Control Theorem for Selmer groups (Theorem 2.2.4). Rubin [89, chapter VII] and Wuthrich [106] have proven a fine analogue of the Control Theorem.

Theorem 3.4.9. *(Control Theorem for fine Selmer groups) The following map*

$$s_n : R_{\mathfrak{p}^\infty}(E/F_n) \to R_{\mathfrak{p}^\infty}(E/L_n)^{\Gamma_n}$$

induced by the natural restriction is a pseudo-isomorphism with a finite kernel and cokernel whose orders are bounded as $n \to \infty$. More precisely,

$$\begin{aligned} \big|\ker(s_n)\big| &\leq \big|E(F)(p)\big| \\ \big|\operatorname{coker}(s_n)\big| &\leq \prod_{v \mid p} \big|(F_v)(p)\big| \prod_{v \nmid p} c_v^{(p)} \end{aligned}$$

where $c_v^{(p)}$ denotes the maximum power of p that divides the Tamagawa number.

The fine analogue of the Control Theorem and Remark 3.4.8 prove that $\mathfrak{p}$-rank of $R_{\mathfrak{p}^\infty}(E/F_n)$ is unbounded in the p-Hilbert S-class field tower. This completes the proof of Theorem 3.4.3.

Remark 3.4.10. An analogue of the main theorem holds for any d-dimensional CM Abelian variety.

Chapter 4

Riemann-Hurwitz Type Formula for λ Invariant of Fine Selmer Groups

4.1 Kida's Formula

The classical *Riemann-Hurwitz formula* gives the relationship of the Euler characteristics of two surfaces when one is a ramified covering of the other. Let $\pi : R_1 \to R_2$ be an n-fold covering of compact, connected Riemann surfaces and $g_1,\ g_2$ be their respective genus; the Riemann-Hurwitz formula is

$$2g_2 - 2 = (2g_1 - 2)\, n + \sum \big(e\,(P_2) - 1\big)$$

where the sum is over all points P_2 on R_2 and $e(P_2)$ denotes the ramification index of P_2 for the covering π [97, Chapter II Theorem 5.9]. Kida proved an analogous formula for algebraic number fields [55]. Kida's formula describes the change of Iwasawa λ-invariants in a p-extension in terms of the degree and the ramification index. Soon after Kida published his results, Iwasawa proved this formula using the theory of Galois cohomology for extensions of $\mathbb{Q}$ which are not necessarily finite. More precisely,

Theorem 4.1.1 (Kida's Formula)**.** *[51, Theorem 6] Let $p \geq 2$ and F be a number field. Let F_{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F and $\mathcal{L}/F_{\text{cyc}}$ be a cyclic extension of degree p, unramified at every infinite place of F_{cyc}. Assume that the classical μ-invariant $\mu(X(F_{\text{cyc}})) = 0$. Then*

$$\lambda\left(X\left(\mathcal{L}\right)\right) = p\lambda\Big(X\left(F_{\text{cyc}}\right)\Big) + \sum_{w}\Big(e\left(w \mid v\right) - 1\Big) + (p-1)\left(h_2 - h_1\right)$$

where w ranges over all non-p places of $\mathcal{L}$ and h_i is the rank of the Abelian group $H^i(\mathcal{L}/F_{\text{cyc}},\ E_{\mathcal{L}})$; here $E_{\mathcal{L}}$ is the group of all units of $\mathcal{L}$.

In [39], Hachimori and Matsuno proved an analogue of Kida's formula and described the behaviour of the Selmer groups of elliptic curves in p-extensions of the cyclotomic $\mathbb{Z}_p$-extension of a number field. In [82], Pollack and Weston proved a similar formula for Selmer groups of a general class of Galois representations including the case of p-ordinary Hilbert modular forms and p-supersingular modular forms. In this chapter, we use Galois cohomology theory to prove an analogue of Kida's formula for the fine Selmer group. We prove an interesting corollary in the spirit of results proved in [18] and [43]. Finally in Section 4.5, we prove an analogue of Kida's formula in the false Tate curve extension.

4.2 Main Result

In this section we mention the main theorem and reduce the proof to the calculation of Herbrand quotients. For computational simplicity we assume $p \geq 5$. If $p = 3$, the same proof goes through under the additional assumption that E/F is semi-stable.

Throughout this chapter we assume that Conjecture A holds for $\mathfrak{Y}(E/F_{\text{cyc}})$. Since the dual fine Selmer group is a Noetherian torsion $\Lambda(\Gamma)$-module, its $\mathbb{Z}_p$-rank is equal to $\lambda\left(\mathfrak{Y}\left(E/F_{\text{cyc}}\right)\right)$.

4.2.1 Statement of the Theorem and a Reduction Step

The main theorem proved in this chapter is the following.

Theorem 4.2.1. *Let $p \geq 5$ be a prime. Let E/F be an elliptic curve with good ordinary reduction at all primes above p. Let L/F be a finite Galois p-extension. Assume the dual fine Selmer group $\mathfrak{Y}(E/F_{\text{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module. Then $\mathfrak{Y}(E/L_{\text{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module. Also,*

$$\lambda\left(\mathfrak{Y}\left(E/L_{\text{cyc}}\right)\right) = [L_{\text{cyc}} : F_{\text{cyc}}]\lambda\left(\mathfrak{Y}\left(E/F_{\text{cyc}}\right)\right) + \sum_{w \in P_1(L)} \left(e_{L_{\text{cyc}}/F_{\text{cyc}}}(w) - 1\right) + 2 \sum_{w \in P_2(L)} \left(e_{L_{\text{cyc}}/F_{\text{cyc}}}(w) - 1\right)$$

where $e_{L_{\text{cyc}}/F_{\text{cyc}}}(w)$ is the ramification index of w in $L_{\text{cyc}}/F_{\text{cyc}}$ and $P_1(L)$, $P_2(L)$ are sets of primes in L_{cyc} defined as

$$P_1(L) = \{w : w \nmid p \text{ and } E \text{ has split multiplicative reduction at } w\}$$
$$P_2(L) = \{w : w \nmid p \text{ and } E \text{ has good reduction at } w,\ E(L_{\text{cyc},w})[p] \neq 0\}.$$

The fact that E has good ordinary reduction at primes above p is used only in proving Lemma 4.3.3.

Set the notation $G = \text{Gal}(L_{\text{cyc}}/F_{\text{cyc}})$. The first step in proving this theorem is a reduction step. The following lemma shows it is enough to prove the main theorem for the case $G = \mathbb{Z}/p\mathbb{Z}$.

Lemma 4.2.2. *[65] Let $F \subset L \subset M$ be number fields such that M/F is a Galois p-extension. If Theorem 4.2.1 is true for any two extensions M/L, M/F, L/F it is true for the third one.*

Proof. Let $v \nmid p$ be a prime in the cyclotomic $\mathbb{Z}_p$-extension L_{cyc}/L. Let w be primes lying above v in M_{cyc}. Suppose there are g many primes above v in M_{cyc}. Since there is no p-extension of the residue field of L_{cyc} at v, $[M_{\text{cyc}} : L_{\text{cyc}}] = e_{M_{\text{cyc}}/L_{\text{cyc}}}(w)g$. Thus,

$$[M_{\text{cyc}} : L_{\text{cyc}}]\left(e_{L_{\text{cyc}}/F_{\text{cyc}}}(v) - 1\right) = \sum_w \left(e_{M_{\text{cyc}}/F_{\text{cyc}}}(w) - e_{M_{\text{cyc}}/L_{\text{cyc}}}(w)\right).$$

This proves the lemma. ☕

From here on, we assume $G = \text{Gal}(L_{\text{cyc}}/F_{\text{cyc}}) = \mathbb{Z}/p\mathbb{Z}$. Since the definition of the p-primary fine Selmer group is independent of S, we can choose it to include all primes of F that are ramified in L/F. Therefore, by our choice of S the maximal extension of L unramified outside $S(L)$ is F_S.

The next proposition is the fine Selmer variant of a well-known result of Iwasawa [49, Theorem 2]. This will finish the proof of the first part of the main theorem.

Proposition 4.2.3. *Assume Conjecture A holds for $\mathfrak{Y}(E/F_{\mathrm{cyc}})$. Then Conjecture A holds for $\mathfrak{Y}(E/L_{\mathrm{cyc}})$.*

Proof. Consider the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & R(E/F_{\mathrm{cyc}}) \arrow[r] \arrow[d, "\alpha"] & H^1(G_S(F_{\mathrm{cyc}}),\ E[p^\infty]) \arrow[r] \arrow[d, "\beta"] & \bigoplus_{v\in S(F_{\mathrm{cyc}})} H^1\left(F_{\mathrm{cyc},v},\ E[p^\infty]\right) \arrow[d, "\gamma"] \\
0 \arrow[r] & R(E/L_{\mathrm{cyc}})^G \arrow[r] & H^1(G_S(L_{\mathrm{cyc}}),\ E[p^\infty])^G \arrow[r] & \left(\bigoplus_{w\in S(L_{\mathrm{cyc}})} H^1\left(L_{\mathrm{cyc},w},\ E[p^\infty]\right)\right)^G
\end{tikzcd}$$

Here, $\ker(\beta) = H^1\left(G,\ E(L_{\mathrm{cyc}})[p^\infty]\right)$ and $\mathrm{coker}(\beta) = H^2\left(G,\ E(L_{\mathrm{cyc}})[p^\infty]\right)$. Both $\ker(\beta)$ and $\mathrm{coker}(\beta)$ are finite; indeed, if M is a $\mathbb{Z}_p[G]$-module of co-finite type, $H^i(G,\ M)$ is finite for $i = 1, 2$.

For each v, $\ker(\gamma_v) = \oplus_{w|v} H^1\left(G_v,\ E(L_{\mathrm{cyc},w})[p^\infty]\right)$. Here, $G_v = \mathrm{Gal}(L_{\mathrm{cyc},w}/F_{\mathrm{cyc},v})$ is the decomposition group of G. The dual of $E(L_{\mathrm{cyc}})[p^\infty]$ (resp. $E(L_{\mathrm{cyc},w})[p^\infty]$) are finitely generated over $\mathbb{Z}_p$ and hence over $\Lambda(G)$ (resp. $\Lambda(G_v)$). The dual of the map α gives rise to the following map

$$\mathfrak{Y}(E/L_{\mathrm{cyc}})_G \xrightarrow{\alpha^\vee} \mathfrak{Y}(E/F_{\mathrm{cyc}})$$

where the kernel and cokernel are finitely generated $\mathbb{Z}_p$-modules. Since $\mathfrak{Y}(E/L_{\mathrm{cyc}})$ is compact, by the Nakayama's lemma for compact local rings it is finitely generated as a $\mathbb{Z}_p[G]$-module. But G is finite, so $\mathfrak{Y}(E/L_{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module. Equivalently, Conjecture A holds for $\mathfrak{Y}(E/L_{\mathrm{cyc}})$ (see Proposition 5.2.1). ☕

4.3 Proof via Calculation of Herbrand Quotients

In this section we will prove the remainder of the main theorem. We emphasize that even though the idea behind the proof is very similar to that of [39], the details are significantly different, specially in the simplification of the Herbrand quotient.

4.3.1 Reduction to Calculation of Herbrand Quotients

The next step is to reduce the proof to the calculation of the Herbrand quotient. Since we are assuming that $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ (and hence $\mathfrak{Y}(E/L_{\mathrm{cyc}})$) is a finitely generated $\mathbb{Z}_p$-module, we have

$$\begin{aligned}
\lambda\left(\mathfrak{Y}\left(E/L_{\mathrm{cyc}}\right)\right) &= \mathrm{corank}_{\mathbb{Z}_p}\left(R\left(E/L_{\mathrm{cyc}}\right)\right);\\
\lambda\left(\mathfrak{Y}(E/F_{\mathrm{cyc}})\right) &= \mathrm{corank}_{\mathbb{Z}_p}\left(R\left(E/F_{\mathrm{cyc}}\right)\right)\\
&= \mathrm{corank}_{\mathbb{Z}_p}\left(R\left(E/L_{\mathrm{cyc}}\right)^G\right)
\end{aligned}$$

The last equality is not obvious. It requires the restriction map, α to have a finite kernel and cokernel. This follows from an application of the Snake Lemma once we know $\ker(\beta)$, $\ker(\gamma)$ and $\mathrm{coker}(\beta)$ are finite. From the proof of Proposition 4.2.3 above, we have $\ker(\beta)$ and $\mathrm{coker}(\beta)$ are finite. We are yet to show that $\ker(\gamma)$ is finite. When $v \nmid p$, it is obvious. When $v \mid p$, it follows from [92, Cor 2, page 130]. This can also be seen from the proof of Lemma 4.3.3.

Classical Theory of $\mathbb{Z}_p$-Modules

Before proceeding any further, we recall some classical theory of $\mathbb{Z}_p$-modules [51, section 9].

Let G be a cyclic group of order p and M be a divisible $\mathbb{Z}_p[G]$-module of co-finite type. Write

$$M \simeq M_1^a \oplus M_{p-1}^b \oplus M_p^c \tag{4.1}$$

where each M_i is indecomposable and defined as

$$M_1 = \mathbb{Z}_p^\vee = \mathbb{Q}_p/\mathbb{Z}_p, \qquad M_{p-1} = I\left(\mathbb{Z}_p[G]\right)^\vee, \qquad M_p = \mathbb{Z}_p[G]^\vee.$$

$I\left(\mathbb{Z}_p[G]\right)$ is the notation for the augmentation ideal and as before $(-)^\vee = \operatorname{Hom}_{\mathbb{Z}_p}(-,\ \mathbb{Q}_p/\mathbb{Z}_p)$ denotes the Pontryagin dual. Note that $\mathbb{Z}_p = \mathbb{Z}_p[G]/I\left(\mathbb{Z}_p[G]\right)$.

For each torsion $\mathbb{Z}_p$-module T, define

$$\begin{aligned} V(T) &:= \operatorname{Hom}_{\mathbb{Z}_p}\left(T,\ \mathbb{Q}_p/\mathbb{Z}_p\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \\ &= T^\vee \otimes_{\mathbb{Z}_p} \mathbb{Q}_p. \end{aligned}$$

The map $T \mapsto V(T)$ is an exact contravariant functor from torsion $\mathbb{Z}_p$-modules into vector spaces over $\mathbb{Q}_p$. With this definition in hand, set

$$V_i = V(M_i), \qquad \pi_i : G \to \mathrm{GL}(V_i) \quad \text{for } i = 1,\ p-1,\ p.$$

Here π_1 is the *trivial representation* of G over $\mathbb{Q}_p$, π_{p-1} is the unique *faithful irreducible representation* of G over $\mathbb{Q}_p$, and

$$\pi_p = \pi_1 \oplus \pi_{p-1} = \pi_G \tag{4.2}$$

where π_G is the *regular representation* of G over $\mathbb{Q}_p$.

For the representation π of G on the space $V(M)$, we get the following from Equation 4.1.

$$\pi = a\pi_1 \oplus b\pi_{p-1} \oplus c\pi_p. \tag{4.3}$$

The task is to compute the integers $a,\ b,\ c$.

Since G is cyclic of order p, the cohomology groups of G are Abelian groups of exponent p. The ranks $r_{n,i}$ of the Abelian groups $H^n\left(G,\ M_i\right)$ are

$$\begin{aligned} r_{1,1} = 1, \quad r_{1,p-1} = 0, \quad r_{1,p} = 0, \\ r_{2,1} = 0, \quad r_{2,p-1} = 1, \quad r_{2,p} = 0. \end{aligned}$$

Combining this with Equation 4.1, one obtains

$$r\left(H^1\left(G,\ M\right)\right) = a, \qquad r\left(H^2\left(G,\ M\right)\right) = b.$$

The first and second cohomology groups of M are finite. Thus, the **Herbrand quotient** defined as follows

$$h_G(M) := \frac{\#H^2(G,\ M)}{\#H^1(G,\ M)}$$

exists and equals p^{b-a}. Since Equation 4.1 implies

$$M^G \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{a+c} \oplus (\mathbb{Z}/p\mathbb{Z})^b,$$

the $\operatorname{corank}_{\mathbb{Z}_p}(M^G) = a + c$. Rewrite Equation 4.3 as

$$\begin{aligned}\pi &= a\pi_1 \oplus b\pi_{p-1} \oplus c\pi_p \\ &= (a+c)\pi_p \oplus (b-a)\pi_{p-1} \\ &= \operatorname{corank}_{\mathbb{Z}_p}(M^G)\pi_G \oplus \operatorname{ord}_p\left(h_G(M)\right)\pi_{p-1}.\end{aligned}$$

The second equality follows from Equation 4.2. Now, comparing the degrees of the representations,

$$\operatorname{corank}_{\mathbb{Z}_p}(M) = p \operatorname{corank}_{\mathbb{Z}_p}(M^G) + (p-1)\operatorname{ord}_p\left(h_G\left(M\right)\right).$$

In our case, $M = R(E/L_{\mathrm{cyc}})$. This gives us the main formula which we will need to evaluate.

$$\lambda\left(\mathfrak{Y}\left(E/L_{\mathrm{cyc}}\right)\right) = p\lambda\left(\mathfrak{Y}\left(E/F_{\mathrm{cyc}}\right)\right) + (p-1)\operatorname{ord}_p\left(h_G\left(R\left(E/L_{\mathrm{cyc}}\right)\right)\right). \tag{4.4}$$

4.3.2 Herbrand Quotient Calculation

We need to calculate $h_G\left(R\left(E/L_{\mathrm{cyc}}\right)\right)$ obtained in Equation 4.4. From the definition of fine Selmer groups and an elementary property of Herbrand quotients we have

$$h_G\left(R\left(E/L_{\mathrm{cyc}}\right)\right) = \frac{h_G\left(H^1\left(G_S\left(L_{\mathrm{cyc}}\right),\ E[p^\infty]\right)\right)}{h_G\left(\bigoplus_w H^1\left(L_{\mathrm{cyc},w},\ E[p^\infty]\right)\right)} \tag{4.5}$$

Simplify the Numerator

We first simplify the numerator using the Hochschild-Serre spectral sequences.

Lemma 4.3.1. $h_G\left(H^1\left(G_S\left(L_{\mathrm{cyc}}\right),\ E[p^\infty]\right)\right) = h_G\left(E\left(L_{\mathrm{cyc}}\right)[p^\infty]\right) = 1.$

Proof. Note the first equality follows, if for $i = 1,\ 2$ we can prove

$$H^i\left(G,\ H^1\left(G_S\left(L_{\mathrm{cyc}}\right),\ E[p^\infty]\right)\right) \simeq H^i\left(G,\ E\left(L_{\mathrm{cyc}}\right)[p^\infty]\right). \tag{4.6}$$

Since we are assuming that Conjecture A holds for $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ (hence also for $\mathfrak{Y}(E/L_{\mathrm{cyc}})$), it follows that the dual fine Selmer group is $\Lambda(\Gamma)$-torsion. Equivalently, the analogue of the weak Leopoldt Conjecture holds. By Equation 2.6,

$$H^2\left(G_S\left(F_{\mathrm{cyc}}\right),\ E[p^\infty]\right) = H^2\left(G_S\left(L_{\mathrm{cyc}}\right),\ E[p^\infty]\right) = 0.$$

We know that $G_S\left(L_{\mathrm{cyc}}\right)$ and $G_S\left(F_{\mathrm{cyc}}\right)$ have p-cohomological dimension less than equal to 2, i.e.

$$H^i\left(G_S\left(L_{\mathrm{cyc}}\right),\ E[p^\infty]\right) = H^i\left(G_S\left(F_{\mathrm{cyc}}\right),\ E[p^\infty]\right) = 0 \qquad \text{for } i \geq 3.$$

Now by Hochschild-Serre spectral sequences, we obtain the following exact sequence

$$\begin{aligned}\cdots \quad &\to H^2\left(G_S\left(F_{\text{cyc}}\right),\ E[p^\infty]\right) &&\to H^1\left(G,\ H^1\left(G_S\left(L_{\text{cyc}}\right),\ E[p^\infty]\right)\right) &&\xrightarrow{f_1}\ H^3\left(G,\ E\left(L_{\text{cyc}}\right)[p^\infty]\right)\\ &\to H^3\left(G_S\left(F_{\text{cyc}}\right),\ E[p^\infty]\right) &&\to H^2\left(G,\ H^1\left(G_S\left(L_{\text{cyc}}\right),\ E[p^\infty]\right)\right) &&\xrightarrow{f_2}\ H^4\left(G,\ E\left(L_{\text{cyc}}\right)[p^\infty]\right)\\ &\to H^4\left(G_S\left(F_{\text{cyc}}\right),\ E[p^\infty]\right) &&\to \cdots\end{aligned} \tag{4.7}$$

From the above discussion, $f_1,\ f_2$ are isomorphisms. Equation 4.6 follows; indeed, since G is cyclic we have $H^i\left(G,\ E\left(L_{\text{cyc}}\right)[p^\infty]\right) = H^{i+2}\left(G,\ E\left(L_{\text{cyc}}\right)[p^\infty]\right)$. This gives the first equality.

The second equality follows from a result in [45]. Imai proved that $E(L_{\text{cyc}})[p^\infty]$ is finite; hence we have $h_G\left(E\left(L_{\text{cyc}}\right)[p^\infty]\right) = 1$ [92, Proposition 8, page 134]. ☕

Simplify the Denominator

To simplify the denominator of Equation 4.5, we divide it into two cases, when $v \nmid p$ and when $v \mid p$. First rewrite

$$h_G\left(\bigoplus_{w\in S\left(L_{\text{cyc}}\right)} H^1\left(L_{\text{cyc},w},\ E[p^\infty]\right)\right) = \bigoplus_{v\in S\left(F_{\text{cyc}}\right)} h_G\left(\bigoplus_{w|v} H^1\left(L_{\text{cyc},w},\ E[p^\infty]\right)\right).$$

Lemma 4.3.2. *Let $v \in S(F_{\text{cyc}})$ be a prime not above p. For $i = 1, 2$, we have*

$$H^i\left(G,\ \bigoplus_{w|v} H^1\left(L_{\text{cyc},w},\ E[p^\infty]\right)\right) = \begin{cases} 0 & \textit{if } v \textit{ splits in } L_{\text{cyc}}/F_{\text{cyc}} \\ H^i\left(G,\ E\left(L_{\text{cyc},w}\right)[p^\infty]\right) & \textit{otherwise}\end{cases}$$

Proof. We divide it into two cases. First when $w \mid v$ is *totally split*. We have

$$\bigoplus_{w|v} H^1\left(L_{\text{cyc},w},\ E[p^\infty]\right) \simeq H^1\left(F_{\text{cyc},v},\ E[p^\infty]\right) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]$$

The right hand side is cohomologically trivial.

Consider the *non-split* case. The p-primary part of the Brauer group $\mathrm{Br}(L_{\text{cyc},w})(p) = 0$ [94, Ch II, Lemma 3]. Thus, the p-cohomological dimension of $L_{\text{cyc},w}$ is 1. By the same argument, the p-cohomological dimension of $F_{\text{cyc},v}$ is also 1. An application of Hochschild-Serre spectral sequence gives a diagram similar to Exact Sequence 4.7. From this we conclude

$$H^i\left(G,\ H^1\left(L_{\text{cyc},w},\ E[p^\infty]\right)\right) \simeq H^i\left(G,\ E\left(L_{\text{cyc},w}\right)[p^\infty]\right).$$

This finishes the proof of the lemma. ☕

When $v \mid p$, we have the following lemma.

Lemma 4.3.3. *Let $v \in S(F_{\text{cyc}})$ be a prime lying above p. Then for $i = 1, 2$, the Herbrand quotient $h_G\left(\bigoplus_{w|v} H^1\left(L_{\text{cyc},w},\ E[p^\infty]\right)\right) = 1$*

Proof. When v *splits* completely in $L_{\text{cyc}}/F_{\text{cyc}}$, $H^i\left(G,\ \bigoplus_{w|v} H^1\left(L_{\text{cyc},w},\ E[p^\infty]\right)\right)$ is trivial using the same argument as above. We need to study the case when v *does not split* in the extension $L_{\text{cyc}}/F_{\text{cyc}}$.

The absolute Galois group of $F_{\text{cyc},v}$ and $L_{\text{cyc},w}$ have p-cohomological dimension at most 2. Further, by Tate duality, $H^2(L_{\text{cyc},w},\ E[p^\infty]) = H^2(F_{\text{cyc},v},\ E[p^\infty])) = 0$ [20, Proof of Theorem 1.12]. Using the Hochschild-Serre spectral sequence argument we arrive at the following isomorphism for $i = 1, 2$,

$$H^i\left(G,\ H^1\left(L_{\text{cyc},w},\ E[p^\infty]\right)\right) \simeq H^i\left(G,\ E\left(L_{\text{cyc},w}\right)[p^\infty]\right).$$

Observe it is enough to show that $E(L_{\text{cyc},w})[p^\infty]$ is finite. This is known to be true by a result of Imai [45]. Therefore, the required Herbrand quotient is 1 by the same argument as in Lemma 4.3.1.

☕

Putting it Together

The series of lemmas above simplifies Equation 4.5 to

$$h_G\left(R\left(E/L_{\text{cyc}}\right)\right) = \frac{1}{\bigoplus_{w\in S'(L_{\text{cyc}})} h_G\left(E\left(L_{\text{cyc},w}\right)[p^\infty]\right)}. \tag{4.8}$$

In the above equation, w runs over those primes of $S(L_{\text{cyc}})$ which are not above p and which do not split in the extension $L_{\text{cyc}}/F_{\text{cyc}}$. Set $H_w = \operatorname{ord}_p\left(h_G\left(E\left(L_{\text{cyc},w}\right)[p^\infty]\right)\right)$. We can rewrite Equation 4.4 as

$$\lambda\left(\mathfrak{Y}\left(E/L_{\text{cyc}}\right)\right) = [L_{\text{cyc}} : F_{\text{cyc}}]\lambda\left(\mathfrak{Y}\left(E/F_{\text{cyc}}\right)\right) - (p-1)\sum_w H_w$$

The final task to finish the proof of Theorem 4.2.1 is to explicitly solve for H_w.

Calculating H_w

The calculation of H_w is exactly as done in the paper of Hachimori and Matsuno [39, Section 5]. We need to study the p-primary torsion points of E in the unramified $\mathbb{Z}_p$-extension of an ℓ-adic field. By the computations we have done so far, we can focus only on the case $p \neq \ell$. We prove

Proposition 4.3.4. *[39, Corollary 5.2] For $w \in S'(L_{\text{cyc}})$, we have*

$$H_w = \begin{cases} -1 & \textit{if } w \in P_1(L) \\ -2 & \textit{if } w \in P_2(L) \\ 0 & \textit{otherwise} \end{cases}$$

where $P_1(L)$, $P_2(L)$ were defined in Theorem 4.2.1.

To prove Proposition 4.3.4 we need the next lemma.

Lemma 4.3.5. *[39, Proposition 5.1] Let p, ℓ be distinct primes. Let $k/\mathbb{Q}_\ell$ be a finite extension and $k \supseteq \mu_p$. Set $k_\infty = k(\mu_{p^\infty})$ and E be defined over k.*

(i) If E has good reduction over k_∞, then

$$E(k_\infty)[p^\infty] \simeq \begin{cases} E[p^\infty] & \textit{if } E(k)[p] \neq 0 \\ 0 & \textit{if } E(k)[p] = 0 \end{cases}$$

(ii) If E has split multiplicative reduction over k_∞, there exists an element $q \in k^\times$ and a non-negative integer m such that $E(k_\infty)[p^\infty]$ is isomorphic to the subgroup of $k_\infty^\times/q^{\mathbb{Z}}$ generated by μ_{p^∞} and q^{1/p^m} as a $\mathrm{Gal}(k_\infty/k)$*-module.*

(iii) If E has non-split multiplicative reduction or additive reduction over k_∞, then $E(k_\infty)[p^\infty]$ is finite.

Proof. Since k is an ℓ-adic field, k_∞/k is unramified at primes above p and therefore the reduction type of E does not change since $p \geq 5$.

(i) By Nakayama's lemma, it follows that $E(k)[p] = 0$ implies $E(k_\infty)[p^\infty] = 0$. When $E(k)[p] \neq 0$, by the Weil pairing we know $k\left(E[p]\right)/k$ is a p-extension because $k \supseteq \mu_p$. Therefore, $k\left(E[p^\infty]\right)/k$ is a pro-p extension. Since E has good reduction, $k\left(E[p^\infty]\right)/k$ is unramified. The field k_∞ is the maximal unramified pro-p extension of k, thus $k\left(E[p^\infty]\right) \subseteq k_\infty$. This gives the necessary isomorphism, $E(k_\infty)[p^\infty] \simeq E[p^\infty]$.

(ii) E is isomorphic to a Tate curve over k with Tate period $q \in k^\times$ [97, Theorem C14.1]. As $\mathrm{Gal}(k_\infty/k)$-modules, $E(k_\infty) \simeq k_\infty^\times/q^{\mathbb{Z}}$. Let q_n be the p^n-th root of q. Then, $q_n^p = q_{n-1}$. Since, q is a unit in an ℓ-adic field, $\mathrm{ord}_\ell(q) > 0$; there is an integer m such that $q_m \in k_\infty$ but $q_{m+1} \notin k_\infty$. By assumption, $\mu_{p^\infty} \subset k_\infty$, we get the desired assertion.

(iii) Let $\widetilde{k_n}$ be the residue field of k_n and $\widetilde{E_{ns}}(\widetilde{k_n})$ be the group of non-singular points of the reduction of E on $\widetilde{k_n}$. There exists a short exact sequence of Abelian groups

$$0 \to E_1(k_n) \to E_0(k_n) \xrightarrow{\text{red}} \widetilde{E_{ns}}(\widetilde{k_n}) \to 0$$

where $E_0(k_n)$ is the subgroup of $E(k_n)$ consisting of points with non-singular reduction and $E_1(k_n)$ is the kernel of the reduction map, red [97, VII.2.1].

By assumption, $k \supseteq \mu_p$ so $\left|\widetilde{k_n}\right| \equiv 1 \mod p$, and $\left(\left|\widetilde{E_{ns}}\left(\widetilde{k_n}\right)\right|, p\right) = 1$ [97, Prop II.2.5]. Since $\ell \neq p$, the subgroup $E_1(k_n)$ has no non-trivial points of of order p [97, Prop VII.3.1]. The above exact sequence implies $E_0(k_n)[p^\infty]$ is trivial. To finish the proof, we need to show $E(k_n)/E_0(k_n)$ is bounded. By the Kodaira-Neron theorem [97, Theorem VII.6.1], $E(k_n)/E_0(k_n)$ is finite and independent of n. It has order at most 4. Thus, $E(k_n)[p^\infty]$ must be bounded independent of n for all n. This gives the desired result.

☕

Proof of Proposition 4.3.4. Recall the notation $v = w\mid_{F_{\mathrm{cyc}}}$, $v \nmid p$, and v does not split in $L_{\mathrm{cyc}}/F_{\mathrm{cyc}}$. $L_{\mathrm{cyc},w}/F_{\mathrm{cyc},v}$ is a Galois extension of degree p. By local class field theory, it is in fact a unique ramified extension. Furthermore, $F_{\mathrm{cyc},v} \supset \mu_{p^\infty}$.

- When E has *good reduction* at w: If $w \notin P_2(L)$, there is no point of order p, i.e.

  $$E(L_{\mathrm{cyc},w})[p] = E(F_{\mathrm{cyc},v})[p] = 0.$$

  Thus, there is nothing to prove. When $w \in P_2(L)$, the above lemma gives

  $$E(L_{\mathrm{cyc},w})[p^\infty] = E(F_{\mathrm{cyc},w})[p^\infty] = E[p^\infty] \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^2$$

  with trivial G-action. Now note that

  $$H_w = \mathrm{ord}_p\left(\frac{\# H^2(G,\ E(L_{\mathrm{cyc},w})[p^\infty])}{\# H^1(G,\ E(L_{\mathrm{cyc},w})[p^\infty])}\right) = \mathrm{ord}_p\left(\frac{\#\{0\}}{\#(\mathbb{Z}/p\mathbb{Z})^2}\right) = -2$$

- When E has *split multiplicative reduction* at w: $w \in P_1(L)$. There is an exact sequence

  $$0 \to \mu_{p^\infty} \to E(L_{\mathrm{cyc},w})[p^\infty] \to T \to 0$$

  where T is a finite group. Action of G on μ_{p^∞} is trivial and hence

  $$H_w = \mathrm{ord}_p\left(h_G(\mu_{p^\infty})\right) = -1.$$

- When E has *non-split or additive reduction* at w: $w \notin P_1(L) \cup P_2(L)$. By Lemma 4.3.5, $E(L_{\mathrm{cyc},w})[p^\infty]$ is finite and hence $H_w = 0$.

With this, the proof of the theorem is complete. ☕

4.4 Application

Let F be a number field, E/F be an elliptic curve, and p be an odd prime. Set $F_n = F(E[p^{n+1}])$, i.e. the field obtained by adjoining the p^{n+1}-torsion points of E to F. Let F_∞ be the field obtained by adjoining all the p-power torsion points on E to F. Set $G = \mathrm{Gal}(F_\infty/F)$. As discussed earlier, when E has CM by the ring of integers of an imaginary quadratic field, G contains an (Abelian) open subgroup isomorphic to $\mathbb{Z}_p^2$. Thus, it is a p-adic Lie group of dimension 2. When E does not have CM, G is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$; the Galois group is a non-Abelian, p-adic Lie group of dimension 4.

The following assertions are consequences of asymptotic results proved by Harris [43, Lemma 3.4.1]. For an elliptic curve E without CM, let $p \geq 5$ and suppose $R(E/F_n^{\mathrm{cyc}})$ is co-finitely generated as a $\mathbb{Z}_p$-module; as $n \to \infty$,

$$\mathrm{corank}_{\mathbb{Z}_p}(R(E/F_n^{\mathrm{cyc}})) = O(p^{3n}).$$

In the CM case, under the same assumptions as above, as $n \to \infty$,

$$\mathrm{corank}_{\mathbb{Z}_p}(R(E/F_n^{\mathrm{cyc}})) = O(p^{n}).$$

More precise results are obtained using Theorem 4.2.1. The following result is inspired by results of Coates and Howson [18, Proposition 6.9]. The proof in the CM and non-CM case are identical. We provide a proof in the non-CM case.

Proposition 4.4.1. *Assume the following*

(i) $p \geq 5$

(ii) $\mathcal{G} = \mathrm{Gal}(F_\infty/F)$ *is a pro-p group*

(iii) $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ *is a finitely generated* $\mathbb{Z}_p$*-module, i.e. Conjecture A holds for* $\mathfrak{Y}(E/F_{\mathrm{cyc}})$.

Let $r(n)$ *be the number of primes of* F_n^{cyc} *not dividing* p *and at which* E *has split multiplicative reduction. Let* m *be the smallest non-negative integer such that*

$$\mathrm{Gal}(F_\infty/F_n) = \ker\left(\mathrm{GL}_2(\mathbb{Z}_p) \xrightarrow{red} \mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})\right).$$

Then, for $n \geq m$,

$$\lambda\left(\mathfrak{Y}\left(E/F_n^{\mathrm{cyc}}\right)\right) = \left[\lambda\left(\mathfrak{Y}\left(E/F_m^{\mathrm{cyc}}\right)\right) + r(m)\right] p^{3(n-m)} - r(n).$$

Proof. By hypothesis, Theorem 4.2.1 gives the formula

$$\lambda\left(\mathfrak{Y}\left(E/F_n^{\mathrm{cyc}}\right)\right) = [F_n^{\mathrm{cyc}} : F_m^{\mathrm{cyc}}]\,\lambda\left(\mathfrak{Y}\left(E/F_m^{\mathrm{cyc}}\right)\right) + \sum_{w \in P_1(L)} \left(e_{n,m}(w) - 1\right).$$

The third term in the general formula gives no contribution for the extension F_n/F_m. Since $w \nmid p$, therefore $F_{n,w}^{\mathrm{cyc}}/F_{m,w}^{\mathrm{cyc}}$ is a totally ramified extension. The assumptions force that E has split multiplicative reduction over $F_{n,w}^{\mathrm{cyc}}$ if and only if E has split multiplicative reduction over $F_{m,w}^{\mathrm{cyc}}$. $P_1(L)$ is the set of those $r(n)$ primes of F_n^{cyc} which divide the $r(m)$ primes of F_m^{cyc}, do not divide p, and at which E has split multiplicative reduction. So,

$$\sum_{w \in P_1(L)} \left(e_{n,m}(w) - 1\right) = [F_n^{\mathrm{cyc}} : F_m^{\mathrm{cyc}}]r(m) - r(n).$$

The formula follows from the choice of m.
Justification: for $n \geq m$, F_{n+1}/F_n has degree p^4. By the Weil pairing, the intersection $F_n^{\mathrm{cyc}} \cap F_{n+1}$ is the field generated over F_n by the p^{n+2}-th roots of unity. Therefore, $[F_{n+1}^{\mathrm{cyc}} : F_n^{\mathrm{cyc}}] = p^3$ for all $n \geq m$. This finishes the proof. ☕

4.5 Kida's Formula in the False Tate Curve Extension

We begin by recalling the definition of a false Tate curve extension. Let p be a fixed odd prime and F be a number field containing μ_p. The *false Tate curve extension* denoted $\mathcal{F}_\infty$ is obtained by adjoining the p-power roots of a fixed integer $m > 1$ to F_{cyc}, i.e.

$$\mathcal{F}_\infty = F\left(\mu_{p^\infty},\ m^{\frac{1}{p^n}} : n = 1, 2, \ldots\right).$$

The Galois group $\mathrm{Gal}\left(\mathcal{F}_\infty/F\right) \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$. This is a non-Abelian p-adic Lie extension. Further, set $H_F = \mathrm{Gal}\left(\mathcal{F}_\infty/F_{\mathrm{cyc}}\right) \simeq \mathbb{Z}_p$.

Let E/F be an elliptic curve such that p is a prime of good reduction. Let S be any finite set of primes of F containing the Archimedean primes, the primes above p, the primes of bad reduction of E, and primes dividing m. Then, $\mathcal{F}_\infty$ is an S-admissible extension. The fine Selmer group $R\left(E/\mathcal{F}_\infty\right)$ is defined as in Section 2.3. Throughout this section, we assume Conjecture A holds for $\mathfrak{Y}\left(E/F_{\text{cyc}}\right)$.

The following fact is well-known.

Theorem 4.5.1. *With notation as above, $\mathfrak{Y}\left(E/\mathcal{F}_\infty\right)$ is a finitely generated $\Lambda(H_F)$-module.*

When G is a pro-p, p-adic Lie group without any elements of order p, we had defined the rank of a finitely generated $\Lambda(G)$-module M, in Section 2.4 as

$$\operatorname{rank}_{\Lambda(G)} M := \sum_{i\geq 0} (-1)^i \operatorname{rank}_{\mathbb{Z}_p} H^i\left(G,\ M\right).$$

For finitely generated $\Lambda(H_F)$-modules, it was proposed by Coates and Howson that $\Lambda(H_F)$-rank is the right analogue of the classical λ-invariant [18].

Recall the i-th Iwasawa cohomology groups are defined as

$$\mathcal{Z}^i\left(E/\mathcal{F}_\infty\right) := \varprojlim_L H^i\left(G_S\left(L\right),\ T_p\left(E\right)\right),$$

where $i \geq 0$. The natural map from $\mathcal{Z}^1\left(E/\mathcal{F}_\infty\right)$ to $\mathcal{Z}^1\left(E/F_{\text{cyc}}\right)$ induces a canonical map

$$\rho_F : \mathcal{Z}^1\left(E/\mathcal{F}_\infty\right)_{H_F} \to \mathcal{Z}^1\left(E/F_{\text{cyc}}\right).$$

Let $T(F)$ be the set of primes of F_{cyc} which are ramified in $\mathcal{F}_\infty$. This set consists of primes of F_{cyc} which either divide p or divide m. Define the subsets

$$T_1(F) = \{w \in T(F_{\text{cyc}}),\ w \nmid p:\ E \text{ has split multiplicative reduction at } w\}$$
$$T_2(F) = \{w \in T(F_{\text{cyc}}),\ w \nmid p:\ E \text{ has good reduction at } w, E(F_{\infty,w})[p] \neq 0\}.$$

Theorem 4.5.2. *[22, Theorem 4.11] Let $\mathcal{F}_\infty$ be the false Tate curve extension of F and p be an odd prime such that E/F has good reduction at p. Suppose Conjecture A holds for $\mathfrak{Y}\left(E/F_{\text{cyc}}\right)$. Then*

$$\operatorname{rank}_{\Lambda(H_F)}\left(\mathfrak{Y}\left(E/\mathcal{F}_\infty\right)\right) + \operatorname{rank}_{\mathbb{Z}_p}\left(\operatorname{coker}\left(\rho_F\right)\right) = \lambda\left(\mathfrak{Y}\left(E/F_{\text{cyc}}\right)\right) + t_1(F) + 2t_2(F),$$

where $t_i(F) = \#T_i\left(F\right)$.

Theorem 4.5.3. *Let p be fixed odd prime and F be a number field containing μ_p. Let L/F be a Galois extension of degree p. Consider the false Tate curve extensions $\mathcal{F}_\infty/F$ and $\mathcal{L}_\infty/L$. Assume Conjecture A holds for $\mathfrak{Y}(E/F_{\text{cyc}})$. Then*

$$\begin{aligned}\operatorname{rank}_{\Lambda(H_L)}\left(\mathfrak{Y}\left(E/\mathcal{L}_\infty\right)\right) + \operatorname{rank}_{\mathbb{Z}_p}\left(\operatorname{coker}\left(\rho_L\right)\right) = p\Big(&\operatorname{rank}_{\Lambda(H_F)}\left(\mathfrak{Y}\left(E/\mathcal{F}_\infty\right)\right) + \operatorname{rank}_{\mathbb{Z}_p}\left(\operatorname{coker}\left(\rho_F\right)\right)\Big)\\ &+ \sum_{w\nmid m, w\in P_1(L)}\left(e_{L_{\text{cyc}}/F_{\text{cyc}}}(w) - 1\right)\\ &+ 2\sum_{w\nmid m, w\in P_2(L)}\left(e_{L_{\text{cyc}}/F_{\text{cyc}}}(w) - 1\right)\end{aligned}$$

Lemma 4.5.4. *With notation as in Theorem 4.5.3,*

$$\sum_{w\in P_i(L)}\Big(e_{L_{\mathrm{cyc}}/F_{\mathrm{cyc}}}(w)-1\Big) = pt_i(F)-t_i(L)+\sum_{w\in P_i(L),w\nmid m}\Big(e_{L_{\mathrm{cyc}}/F_{\mathrm{cyc}}}(w)-1\Big).$$

Proof. Suppose v is a prime of F_{cyc} and $w \mid v$ be a prime of L_{cyc}. Observe that $v\in T_i(F)$ if and only if $w\in T_i(L)$. Further, since $w\nmid p$, the residue degree $f_w\left(L_{\mathrm{cyc}}/F_{\mathrm{cyc}}\right)=1$ for primes in $T_i(L)$. Thus,

$$\begin{aligned}\sum_{w\in P_i(L)}\Big(e_{L_{\mathrm{cyc}}/F_{\mathrm{cyc}}}(w)-1\Big) &= \sum_{w\in T_i(L)}\Big(e_{L_{\mathrm{cyc}}/F_{\mathrm{cyc}}}(w)-1\Big)+\sum_{w\in P_i(L),w\nmid m}\Big(e_{L_{\mathrm{cyc}}/F_{\mathrm{cyc}}}(w)-1\Big)\\ &= pt_i(F)\ -t_i(L)\ +\sum_{w\in P_i(L),w\nmid m}\Big(e_{L_{\mathrm{cyc}}/F_{\mathrm{cyc}}}(w)-1\Big)\end{aligned}$$

This completes the proof of the lemma. ☕

Proof of Theorem 4.5.3. Theorem 4.5.2 for $\mathcal{L}_\infty/L$ yields,

$$\operatorname{rank}_{\Lambda(H_L)}\Big(\mathfrak{Y}\left(E/\mathcal{L}_\infty\right)\Big)+\operatorname{rank}_{\mathbb{Z}_p}\left(\operatorname{coker}\left(\rho_L\right)\right)=\lambda\Big(\mathfrak{Y}\left(E/L_{\mathrm{cyc}}\right)\Big)+t_1(L)+2t_2(L). \tag{4.9}$$

Using Theorem 4.2.1, it is possible to rewrite $\lambda\Big(\mathfrak{Y}\left(E/L_{\mathrm{cyc}}\right)\Big)$,

$$\lambda\Big(\mathfrak{Y}\left(E/L_{\mathrm{cyc}}\right)\Big)=p\lambda\Big(\mathfrak{Y}\left(E/F_{\mathrm{cyc}}\right)\Big)+\sum_{w\in P_1(L)}\Big(e_{L_{\mathrm{cyc}}/F_{\mathrm{cyc}}}(w)-1\Big)+2\sum_{w\in P_2(L)}\Big(e_{L_{\mathrm{cyc}}/F_{\mathrm{cyc}}}(w)-1\Big). \tag{4.10}$$

By rearranging terms and multiplying throughout by p, Theorem 4.5.2 for $\mathcal{F}_\infty/F$ yields,

$$p\lambda\Big(\mathfrak{Y}\left(E/F_{\mathrm{cyc}}\right)\Big)=p\operatorname{rank}_{\Lambda(H_F)}\Big(\mathfrak{Y}\left(E/\mathcal{F}_\infty\right)\Big)+p\operatorname{rank}_{\mathbb{Z}_p}\left(\operatorname{coker}\left(\rho_F\right)\right)-pt_1(F)-2pt_2(F). \tag{4.11}$$

Substituting the formula in Lemma 4.5.4 and Equation 4.11 into Equation 4.10 and plugging this expression of $\lambda\Big(\mathfrak{Y}\left(E/L_{\mathrm{cyc}}\right)\Big)$ into Equation 4.9, proves the theorem. ☕

Remark 4.5.5. Theorem 4.5.2 holds any pro-p, p-adic Lie extension of F of dimension 2 (see [96]). Therefore, Theorem 4.5.3 can be proven for any such extension in exactly the same way. In particular, if E/F is an elliptic curve with CM by an imaginary quadratic field, an analogous Kida's formula exists over the trivializing extension F_∞/F.

Chapter 5

Conjecture A and its Relation with the Classical Conjecture

In this chapter, we prove two kinds of results. First we provide some evidence towards Conjecture A. Second, we show that there is a deep relationship between Conjecture A and the Classical $\mu = 0$ Conjecture. This is not surprising, given that in Chapter 3 we have seen that in a large number of cases the p-ranks of ideal class groups and the p-ranks of fine Selmer groups have the same order of growth.

5.1 Trivial Selmer Groups over the Cyclotomic Extension

We begin by reminding the reader the precise formulation of Conjecture A.

Conjecture A. *Let E be an elliptic curve defined over a number field F. The Pontryagin dual of the fine Selmer group $\mathfrak{Y}(E/F_{\text{cyc}})$ is $\Lambda(\Gamma)$-torsion and the associated μ-invariant is 0.*

Throughout this section we assume that the following hypothesis holds.

Hypothesis. *The Shafarevich-Tate group of an elliptic curve is finite.*

Let E be a rank 0 elliptic curve defined over a number field F. In this section, we prove that for density one primes of good ordinary reduction, $\operatorname{Sel}(E/F_{\text{cyc}})$ (and hence $R(E/F_{\text{cyc}})$) is trivial in the cyclotomic $\mathbb{Z}_p$-extension.

Fix a number field F and an odd prime p. Let E be an elliptic curve over F with good ordinary reduction at all primes above p. In Corollary 2.2.5, we saw the following consequence of the Control Theorem: when $\operatorname{Sel}(E/F)$ is finite, $\operatorname{Sel}(E/F_{\text{cyc}})$ is $\Lambda(\Gamma)$-cotorsion, where $\Gamma = \operatorname{Gal}(F_{\text{cyc}}/F)$. The hypothesis $\operatorname{Sel}(E/F)$ is finite holds for example, if E is a rank 0 elliptic curve over F.

Let $f_E(T)$ be the characteristic polynomial generating the characteristic ideal of $\mathfrak{X}(E/F_{\text{cyc}})$. When $\operatorname{Sel}(E/F)$ is finite, by the Control Theorem we know $\operatorname{Sel}(E/F_{\text{cyc}})^{\Gamma}$ is finite. By Nakayama's Lemma, it follows that $\mathfrak{X}(E/F_{\text{cyc}})/T\mathfrak{X}(E/F_{\text{cyc}})$ is finite. Therefore, $T \nmid f_E(T)$ and $f_E(0) \neq 0$ [17].

The reduction of E modulo v over the residue field κ_v is denoted by $\widetilde{E}_v$. Recall v is called an **anomalous prime** if p divides $\left|\widetilde{E}_v(f_v)\right|$ [66, Section 1(b)]. Also,

$$\left|\widetilde{E}_v(f_v)\right| = (1-\alpha_v)(1-\beta_v)$$

where $\alpha_v\beta_v = N(v)$, $\alpha_v + \beta_v = a_v \in \mathbb{Z}$, and a_v is not divisible by p. Both α_v, β_v must therefore be in $\mathbb{Q}_p$. If we further assume that $\alpha_v \in \mathbb{Z}_p^\times$, then an equivalent definition of a prime being anomalous is that $a_v \equiv 1 \pmod{p}$. Let c_v be the Tamagawa number and denote the highest power of p dividing it by $c_v^{(p)}$.

In this section, we prove the following theorem. This is a joint result with R. Sujatha.

Theorem 5.1.1. *Let F be a number field and E be an elliptic curve of rank 0 over F. Assume that the Shafarevich-Tate group of E/F is finite. Varying over primes of good ordinary reduction,* $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ *is trivial for all primes outside a set of density 0. In particular, Conjecture A holds for $\mathfrak{Y}(E/F_{\mathrm{cyc}})$.*

In [67], Mazur and Rubin show that given F, there exist 'many' rank 0 elliptic curves over F. This guarantees that the statement has content.

Proof. We divide this proof into two steps. In Step 1, we show that under the hypothesis of the theorem, $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ is finite. This implies that $R(E/F_{\mathrm{cyc}})$ is also finite, hence Conjecture A holds. In Step 2, we prove that in fact $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ is trivial.

Step 1: With the setting as in the theorem, it is known [17, Section 4]

$$f_E(0) \sim \left(\prod_{v\ bad} c_v^{(p)}\right)\left(\prod_{v|p}\left|\widetilde{E}_v(f_v)(p)\right|^2\right)\left|\mathrm{Sel}(E/F)\right| \Big/ \left|E(F)(p)\right|^2 \tag{5.1}$$

where $a \sim b$ for $a, b \in \mathbb{Q}_p^\times$ means that a, b have the same p-adic valuation.

It follows from Equation 5.1 that if E is an elliptic curve defined over F satisfying the following conditions, $f_E(0)$ is a unit.

(i) E is a rank 0 elliptic curve defined over F, with $E(F)[p]$ is trivial.

(ii) E has good ordinary non-anomalous reduction at primes above p

(iii) $\text{Ш}(E/F)(p)$ is trivial

(iv) p does not divide the Tamagawa number c_v, where v is a bad prime.

Note that for rank 0 elliptic curves with $E(F)[p] = 0$, $\mathrm{Sel}(E/F) = \text{Ш}(E/F)(p)$. When $f_E(0)$ is a unit, $\mathfrak{X}(E/F_{\mathrm{cyc}})$ (and hence $\mathfrak{Y}(E/F_{\mathrm{cyc}})$) is finite. Equivalently, both $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ and $R(E/F_{\mathrm{cyc}})$ are finite.

We have to check that given such a rank 0 elliptic curve, $f_E(0)$ is a unit for density 1 primes of good ordinary reduction. This follows from the following observations,

(i) it is a result of Merel that given an elliptic curve E, over a fixed number field F, for all but finitely many primes $E(F)[p]$ is trivial.

(ii) given an elliptic curve E/F, it has good reduction at primes above p for all but finitely many p. Using a Chebotarev density argument, for density 1 ordinary primes, it is known E has non-anomalous reduction at p [74].

(iii) since we assume finiteness of the Shafarevich-Tate group, given an elliptic curve E, condition (iii) holds away from a finite set of primes.

(iv) at bad places, the Tamagawa number is finite and bounded. Given an elliptic curve E, condition (iv) holds away from a finite set of primes.

Step 2: To prove that $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ is in fact trivial we need the following lemma proved by Greenberg [17]. This is also proven by Hachimori and Matsuno [40].

Lemma 5.1.2. *Let E be an elliptic curve defined over F with good, ordinary reduction at all primes of F lying over p. Suppose $\mathrm{Sel}(E/F)$ is finite and that $E(F)[p]$ is trivial. Then $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ has no proper $\Lambda(\Gamma)$-submodules of finite index.*

Proof. There is the following canonical surjective map coming from the Cassels pairing

$$E(F)(p) \to \mathrm{Sel}(E/F_{\mathrm{cyc}})_{\Gamma}.$$

By hypothesis, $E(F)(p) = \mathrm{Sel}(E/F_{\mathrm{cyc}})_{\Gamma}$ is trivial. Suppose $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ has a finite, non-zero $\Lambda(\Gamma)$ quotient M; this must be a non-zero, finite, Abelian p-group with Γ-action. M_{Γ} is non-zero but it is a homomorphic image of $\mathrm{Sel}(E/F_{cyc})_{\Gamma}$. This gives the desired contradiction. ☕

We note that the following stronger statement is true [17, Proposition 4.14]. However, we avoid giving a proof as we do not need the full force of the statement.

Lemma 5.1.3. *Let E be an elliptic curve defined over F and that $\mathfrak{X}(E/F_{\mathrm{cyc}})$ be $\Lambda(\Gamma)$-torsion. If $E(F)[p]$ is trivial, then $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ has no proper $\Lambda(\Gamma)$-submodules of finite index.*

If $E(F)[p]$ is trivial, by Lemma 5.1.2 if $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ is non-zero it must be infinite. Therefore, in our setting $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ (and hence $R(E/F_{\mathrm{cyc}})$) must be trivial. The proof is now complete. ☕

Remark 5.1.4. (i) Theorem 5.1.1 strengthens a result of Greenberg, where the same statement is proved for $F = \mathbb{Q}$ [17, Proposition 5.1].

(ii) It is important to emphasize that for a fixed elliptic curve over F, it is possible that $f_E(0) = 1$ when $E(F)[p]$ is non-trivial; for example if there is anomalous reduction at the prime p. It is also possible that such elliptic curves have trivial $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ [20, Theorem 3.11 and Remark 3.12(v)]. Elliptic curves with these properties exist [20, Chapter 5]. However, these are some elliptic curves that are excluded by our theorem. This raises the following natural question.

Question. Let E be a rank 0 elliptic curve defined over F. Is $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ trivial for all but finitely many primes?

In this direction, for $F = \mathbb{Q}$, we have the following proposition of Greenberg [17, Proposition 5.1]. This approach however can not be extended to the case of general number fields.

Proposition 5.1.5. *Let E be an elliptic curve of rank 0 over $\mathbb{Q}$ such that $\mathrm{Ш}(E/\mathbb{Q})$ is finite. If $E(\mathbb{Q})$ has a point of order 2 or if E is $\mathbb{Q}$-isogenous to an elliptic curve E' such that $\left|E'(\mathbb{Q})\right| > 1$, then $\mathrm{Sel}(E/\mathbb{Q}_{\mathrm{cyc}})$ is trivial for all but finitely many primes.*

Proof. Note $\mathbb{Q}$-isogenous elliptic curves have the same set of primes of bad reduction. If p is a prime of good reduction for E, the prime-to-p-part of $E'(\mathbb{Q})_{\mathrm{tors}}$ injects into $\widetilde{E'}(\mathbb{F}_p)$; both $\widetilde{E'}(\mathbb{F}_p)$ and $\widetilde{E}(\mathbb{F}_p)$ have the same order.
Claim: If $E(\mathbb{Q})$ has a point of order 2 and $p \geq 7$, then p is non-anomalous.
Justification: If $a_p \equiv 1 \pmod{p}$, then $2p$ must divide $\left|\widetilde{E}(\mathbb{F}_p)\right|$. But then

$$2p < 1 + p + 2\sqrt{p}.$$

This can not happen if $p \geq 7$.
Claim: Let E be isogenous to E' and suppose $E'(\mathbb{Q})_{\text{tors}}$ has a subgroup of order $q > 2$, then p is non-anomalous if $p \nmid q$.
Justification: Suppose p is an anomalous prime and $p \nmid q$, then qp must divide $\left|\widetilde{E}(\mathbb{F}_p)\right|$. But then

$$qp < 1 + p + 2\sqrt{p},$$

which can not happen since $q > 2$.
With this the proof is complete. ☕

5.2 Relating Conjecture A to the Classical μ=0 Conjecture

There is growing evidence that the ideal class groups and the fine Selmer groups are closely related to one another. The goal of this section is to make explicit the relationship between the two conjectures concerning the vanishing of the respective μ-invariants in the cyclotomic $\mathbb{Z}_p$-extension.

5.2.1 Equivalent Formulations of the Conjectures

We remind the reader the precise formulation of the Classical $\mu = 0$ Conjecture.
Classical $\mu = 0$ Conjecture. *Let F be a number field and consider the cyclotomic $\mathbb{Z}_p$-extension F_{cyc}/F. Let A_n denote the p-part of the class group of the n-th layer; set $X = \varprojlim A_n$. Then $\mu(X) = 0$.*

The following proposition is well-known. It gives an equivalent condition for the vanishing of the μ invariant of *any* torsion $\Lambda(\Gamma)$-module.

Proposition 5.2.1. *Let M be a finitely generated torsion $\Lambda(\Gamma)$-module. Then $\mu(M) = 0$ if and only if M is finitely generated as a $\mathbb{Z}_p$-module.*

Proof. Suppose $\mu(M) = 0$. By the Structure Theorem, we have the following pseudo-isomorphism

$$M \sim \bigoplus_{j=1}^{t} {}^{\Lambda(\Gamma)}\!\Big/\!_{\left(f_j(T)\right)}$$

where f_j is a distinguished polynomial and $\sum_j \deg(f_j) = \lambda$. Applying the division algorithm,

$${}^{\Lambda(\Gamma)}\!\Big/\!_{\left(f_j(T)\right)} \simeq \mathbb{Z}_p^{\deg(g_j)}.$$

Hence, it follows that

$$M \simeq \mathbb{Z}_p^{\lambda} \oplus (\text{finite } p\text{-group}).$$

The converse is straight forward. ☕

There are several equivalent ways of formulating the Classical $\mu = 0$ Conjecture. The following equivalent formulation is proven in [100, Proposition 4.10(1)].

Proposition 5.2.2. *The Classical $\mu = 0$ Conjecture holds for F_{cyc}/F if and only if*

$$H^2\left(G_S\left(F_{\text{cyc}}\right),\ \mu_p\right) = 0.$$

The following result is standard and is proven in [105, Proposition 13.23].

Proposition 5.2.3. $\mu(X) = 0$ *if and only if p-rank of A_n is finite and bounded as $n \to \infty$.*

Similar to Proposition 5.2.3, it is possible to express the vanishing of the μ-invariant associated with the dual fine Selmer group $\mathfrak{Y}(A/F_{\text{cyc}})$ in terms of boundedness of p-ranks.

Proposition 5.2.4. *Let A be a d-dimensional Abelian variety defined over F. Conjecture A holds for $\mathfrak{Y}(A/F_{\text{cyc}})$ if and only if p-rank of $R(A/F_n)$ is finite and bounded as $n \to \infty$.*

Proof. Set $\Gamma_n = \operatorname{Gal}(F_{\text{cyc}}/F_n)$. Consider the following commutative diagram with the vertical maps given by restriction

$$\begin{tikzcd}
0 \arrow[r] & R(A/F_n) \arrow[r] \arrow[d, "r_n"] & H^1(G_S(F_n), A[p^\infty]) \arrow[r] \arrow[d, "f_n"] & \bigoplus_{v_n} H^1(F_{n,v_n}, A[p^\infty]) \arrow[d, "\gamma_n"] \\
0 \arrow[r] & R(A/F_{\text{cyc}})^{\Gamma_n} \arrow[r] & H^1(G_S(F_{\text{cyc}}), A[p^\infty])^{\Gamma_n} \arrow[r] & \left(\varinjlim_n \bigoplus_{v_n} H^1(F_{n,v_n}, A[p^\infty])\right)^{\Gamma_n}
\end{tikzcd}$$

From this diagram, one notices that f_n, γ_n are surjective and

$$r_p\left(\ker(f_n)\right) \leq 2d$$
$$r_p\left(\ker(\gamma_n)\right) \leq 2d\big|S(F_n)\big|.$$

Using Lemma 3.1.5 for the map r_n yields

$$\left| r_p\Big(R\left(A/F_n\right)\Big) - r_p\Big(R\left(A/F_{\text{cyc}}\right)^{\Gamma_n}\Big)\right| = O(1). \tag{5.2}$$

Recall that the Pontryagin dual of $R\left(A/F_{\text{cyc}}\right)^{\Gamma_n}[p]$ is equal to $\mathfrak{Y}\left(A/F_{\text{cyc}}\right)/(p, w_n)$. By [105, Lemma 13.20], $\mathfrak{Y}(A/F_{\text{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module if and only if the p-rank of $R(A/F_{\text{cyc}})^{\Gamma_n}$ is bounded independent of n. By Equation 5.2 the proposition follows.

We give a formulation of Conjecture A in terms of the vanishing of Galois cohomology group. This was established independently by Greenberg [36] and Sujatha [101].

Proposition 5.2.5. *Suppose the analogue of the weak Leopoldt conjecture for elliptic curves holds i.e. $H^2\Big(G_S\left(F_{\text{cyc}}\right), E[p^\infty]\Big) = 0$. Then Conjecture A for $\mathfrak{Y}\left(E/F_{\text{cyc}}\right)$ is equivalent to the assertion*

$$H^2\Big(G_S\left(F_{\text{cyc}}\right),\ E[p]\Big) = 0.$$

Sketch of Proof. Consider the $\Lambda(\Gamma)$-modules

$$\mathcal{Z}^2\left(T_p\left(E\right)/F_{\text{cyc}}\right) = \varprojlim_L H^2\left(G_S\left(L\right),\ T_p\left(E\right)\right),$$
$$\mathcal{Z}^2\left(E[p]/F_{\text{cyc}}\right) = \varprojlim_L H^2\left(G_S\left(L\right),\ E[p]\right).$$

By hypothesis, $H^2\Big(G_S\left(F_{\text{cyc}}\right),\ E[p^\infty]\Big) = 0$. By Lemma 2.5.1, $\mathcal{Z}^2\left(T_p\left(E\right)/F_{\text{cyc}}\right)$ is $\Lambda(\Gamma)$-torsion. From the Poitou-Tate sequence, it follows that $\mathcal{Z}^2(T_p(E)/F_{\text{cyc}})$ and $\mathfrak{Y}(E/F_{\text{cyc}})$ differ by finitely generated $\mathbb{Z}_p$-modules. Note that

$$\mathcal{Z}^2\left(T_p\left(E\right)/F_{\text{cyc}}\right)\Big/ p\mathcal{Z}^2\left(T_p\left(E\right)/F_{\text{cyc}}\right) \simeq \mathcal{Z}^2\left(E[p]/F_{\text{cyc}}\right).$$

Therefore, $\mathcal{Z}^2\left(T_p\left(E\right)/F_{\text{cyc}}\right)$ is a finitely generated $\mathbb{Z}_p$-module if and only if $\mathcal{Z}^2(E[p]/F_{\text{cyc}})$ is finite (hence its μ-invariant is 0). But, $\mathcal{Z}^2(E[p]/F_{\text{cyc}})$ and $H^2(G_S(F_{\text{cyc}}), E[p])^\vee$ have the same μ-invariant. Furthermore, $\mathcal{Z}^2(E[p]/F_{\text{cyc}})$ is finite if and only if $H^2(G_S(F_{\text{cyc}}), E[p])$ is trivial. ☕

Finally, we record a theorem of Sujatha and Witte [100, Theorem 4.1].

Theorem 5.2.6. *Let F be a number field and M be a G_F-representation on a finite dimensional vector space over $\mathbb{F}_p$, where G_F is the absolute Galois group* $\text{Gal}\left(\overline{F}/F\right)$*. Assume that S is a finite set of primes of F containing the primes above p and the primes where M is ramified. The following are equivalent*

(i) $H^2\left(G_S\left(F_{\text{cyc}}\right),\ M\right) = 0.$

(ii) $\mathcal{Z}^2\left(M/F_{\text{cyc}}\right)$ *is finite.*

(iii) the fine Selmer group $R\left(M^\vee(1)/F_{\text{cyc}}\right)$ *is finite.*

(iv) the inflation map $H^2\left(G_S\left(F_{\text{cyc}}\right),\ M\right) \to H^2\left(G_T\left(F_{\text{cyc}}\right),\ M\right)$ *is injective for every finite set of primes T containing S.*

Previous Results in this Direction

We mentioned in Theorem 2.3.1 a close relationship between Conjecture A and the Classical $\mu = 0$ Conjecture. Using very different techniques the theorem was proved in [22, Theorem 3.4] and [60, Theorem 5.5]. We restate the theorem for convenience and also provide a proof.

Theorem. *Let $p \neq 2$. Suppose $F(E[p])/F$ is a finite p-extension. Then $\mathfrak{Y}(E/F_{\text{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module if and only if the Classical $\mu = 0$ Conjecture holds for F_{cyc}.*

The following facts are well known and will be used in the proof of the above theorem.

(i) Iwasawa proved that for a finite p-extension L/F, the Classical $\mu = 0$ Conjecture holds for L_{cyc} if it holds for F_{cyc} [49, Theorem 3]. An analogous statement is true for Conjecture A. We provided a proof of this fact earlier in Proposition 4.2.3.

(ii) Let L/F be any finite extension, the Classical $\mu = 0$ Conjecture holds for F_{cyc} if it holds for L_{cyc} [49, Remark on Page 10]. The analogue is true for Conjecture A; we prove it below.

Lemma 5.2.7. *Let L/F be any finite extension. If Conjecture A holds for $\mathfrak{Y}\left(E/L_{\text{cyc}}\right)$, then it holds for $\mathfrak{Y}\left(E/F_{\text{cyc}}\right)$ as well.*

Proof. Choose a set S large enough so that L/F is unramified outside S. The p-cohomological dimension of $G_S(F_{\text{cyc}})$ is at most 2, hence the following co-restriction map is surjective

$$H^2\left(G_S\left(L_{\text{cyc}}\right),\ A[p]\right) \to H^2\left(G_S\left(F_{\text{cyc}}\right),\ A[p]\right).$$

By Proposition 5.2.5, the hypothesis says $H^2\left(G_S\left(L_{\text{cyc}}\right),\ A[p]\right) = 0$; the lemma follows. ☕

We will now prove the theorem. The proof we present is due to Lim and Murty.

Proof of the Theorem. In view of Lemma 5.2.7 and the hypothesis of the theorem, WLOG we replace F by $F(E[p])$ and assume $E[p] \subseteq E(F)$. This is the setting of Remark 3.1.9. In this case, we know

$$\left| r_p\left(R_p\left(E/F_n\right)\right) - 2r_p\left(\mathrm{Cl}_S\left(F_n\right)\right)\right| = O(1).$$

Since in the cyclotomic extension, the primes in S are finitely decomposed, Equations 3.12 and 3.13 hold. Therefore one concludes

$$\left| r_p\left(R\left(E/F_n\right)\right) - 2r_p\left(\mathrm{Cl}\left(F_n\right)\right)\right| = O(1).$$

Notice $r_p\left(R\left(E/F_n\right)\right)$ is finite and bounded independent of n if and only if the same holds for $r_p\left(\mathrm{Cl}\left(F_n\right)\right)$. The theorem follows from Proposition 5.2.3 and Proposition 5.2.4. ☕

The only property of the cyclotomic extension used in the proof is that in this $\mathbb{Z}_p$-extension, primes are finitely decomposed. Therefore using the same technique, the following general statement is true.

Theorem 5.2.8. *Let $p \neq 2$ and F_∞/F be any $\mathbb{Z}_p$-extension such that all primes are finitely decomposed in this tower. Further assume $F(E[p])/F$ is a finite p-extension. Then $\mathfrak{Y}(E/F_\infty)$ is a finitely generated $\mathbb{Z}_p$-module if and only if the classical μ-invariant associated to F_∞/F is zero.*

The following result of Bloom and Gerth III [6] combined with the above theorem yields an interesting corollary for the vanishing of μ-invariants of dual fine Selmer groups.

Theorem 5.2.9. *Let F be a number field such that it has at least two $\mathbb{Z}_p$-extensions. Assume that for at least one $\mathbb{Z}_p$-extension F_∞/F, the associated classical μ-invariant is 0. There are at most finitely many $\mathbb{Z}_p$-extensions of F which potentially have a positive μ-invariant.*

We will consider the case of CM elliptic curves. Let $p \neq 2,\ 3$ and K be an imaginary quadratic field such that p splits in K as $\mathfrak{p}\overline{\mathfrak{p}}$. Let E/K be an elliptic curve with CM by the ring of integers $\mathcal{O}_K$ and consider the finite field extension $F = K(E[p])/K$. The trivializing extension $K(E[p^\infty])/F$ is an Abelian pro-p extension which is the compositum of the two disjoint split prime $\mathbb{Z}_p$ extensions over F; one is unramified outside primes above $\mathfrak{p}$ (call it N/F) and the other is unramified outside primes above $\overline{\mathfrak{p}}$ (call it N^*/F). Primes are finitely decomposed in the $\mathbb{Z}_p$-extensions, N and N^* [28, Page 45]. Therefore, the same is true for the compositum. By the independent work of Gillard [32] and Schneps [90], we know that the classical μ-invariant associated to N/F (and by symmetry also for N^*/F) is 0. We may now apply Theorem 5.2.9. Thus, there are only finitely many $\mathbb{Z}_p$-extensions of F contained in the trvializing extension where the classical μ-invariant *might* be positive. All $\mathbb{Z}_p$-extensions of F contained in the trivializing extension have the property that primes are finitely decomposed; applying Theorem 5.2.8 the next result is immediate.

Theorem 5.2.10. *Let $p \neq 2,\ 3$. Let K be an imaginary quadratic field such that p splits completely in K. Consider an elliptic curve E/K with CM by $\mathcal{O}_K$. Set $F = K(E[p])$. There are at most finitely many $\mathbb{Z}_p$-extensions F_∞/F over which the μ-invariant associated with $\mathfrak{Y}(E/F_\infty)$ might potentially be positive.*

Remark 5.2.11. The bound on the number of $\mathbb{Z}_p$-extensions which might have a positive μ-invariant is explicitly computable.

The ideas in the above proof of Lim and Murty can be pushed to prove stronger results in either direction. This will be the main focus of the next few sections.

5.2.2 Conjecture A implies the Classical $\mu = 0$ Conjecture

In simple words, the first theorem we prove in this section says the following: given a number field F, to prove the Classical $\mu = 0$ Conjecture for F_{cyc}/F, it suffices to find *one* elliptic curve E/F such that it has non-trivial torsion points over F *and* Conjecture A holds for $\mathfrak{Y}(E/F_{\text{cyc}})$.

Theorem 5.2.12. *Let E be an elliptic curve defined over the number field F. Let p be any odd prime. Further assume that $E(F)[p] \neq 0$. If Conjecture A holds for $\mathfrak{Y}(E/F_{\text{cyc}})$, then the Classical $\mu = 0$ Conjecture holds for F_{cyc}/F.*

The above theorem follows from the following lemma when A is an elliptic curve. The idea of the proof is similar to some of the technical lemmas proved in Chapter 3 and can be obtained from Theorem 3.3.15 by making necessary modifications. For the sake of completeness, we include a detailed proof.

Lemma 5.2.13. *Let F_{cyc}/F be the cyclotomic $\mathbb{Z}_p$-extension and F_n be the subfield of F_{cyc} such that $[F_n : F] = p^n$. Let A be a d-dimensional Abelian variety over F and S be as defined before. Assume $A(F)[p]$ is non-trivial. Then for some positive constant k_1 that depends on $A(F)[p]$,*

$$k_1 r_p\left(\mathrm{Cl}_S(F_n)\right) \leq r_p\left(R(A/F_n)\right) + O(1) \tag{5.3}$$

Proof. For the ease of notation, set $H_n = H_S(F_n)$ and $H_{n,w} = H_S(F_n)_w$. Consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & R(A/F_n) \arrow[r] \arrow[d, "r_n"] & H^1(G_S(F_n), A[p^\infty]) \arrow[r] \arrow[d, "f_n"] & \bigoplus_{v_n} H^1(F_{n,v_n}, A[p^\infty]) \arrow[d, "\gamma_n"] \\
0 \arrow[r] & R(A/H_n) \arrow[r] & H^1(G_S(H_n), A[p^\infty]) \arrow[r] & \bigoplus_{v_n} \bigoplus_{w|v_n} H^1(H_{n,w}, A[p^\infty])
\end{tikzcd}$$

Here v_n runs over all primes in $S(F_n)$, the finite set of primes in F_n that lie above the primes in S. Observe

$$\ker \gamma_n = \bigoplus_{v_n} \ker \gamma_{n,v_n}.$$

Each $\ker \gamma_{n,v_n} = H^1\left(G_{n,v_n}, A\left(H_{n,v_n}\right)[p^\infty]\right)$ where G_{n,v_n} is the decomposition group of $G_n := \mathrm{Gal}(H_n/F_n)$. By definition of p-Hilbert S-class field, $G_{n,v_n} = 1$. So, $\ker \gamma_n = \operatorname{coker} \gamma_n = 0$.

By a standard inflation-restriction argument, $\ker(f_n) = H^1(G_n, A(H_n)[p^\infty])$. By a diagram chase one obtains

$$\ker(f_n) \hookrightarrow R(A/F_n).$$

Therefore we obtain the following inequality

$$r_p\left(H^1\left(G_n,\ A\left(H_n\right)[p^\infty]\right)\right) \leq r_p\left(R\left(A/F_n\right)\right).$$

Combining this with Lemma 3.1.6 gives

$$h_1(G_n) r_p \left(A(F_n)[p^\infty]\right) - 2d \leq r_p \left(R(A/F_n)\right). \tag{5.4}$$

By definition of S-class group, $\mathrm{Gal}(H_n/F_n) = \mathrm{Cl}_S(F_n)$. So

$$\begin{aligned} h_1(G_n) &= h_1 \left(\mathrm{Gal}(H_n/F_n)\right) \\ &= r_p \left(\mathrm{Cl}_S(F_n)/p\right) \\ &= r_p \left(\mathrm{Cl}_S(F_n)\right) \end{aligned}$$

where the last equality follows from the finiteness of the S-class group. Also,

$$\begin{aligned} r_p \left(A(F_n)[p^\infty]\right) &\geq r_p \left(A(F)[p^\infty]\right) \\ &= r_p \left(A(F)[p]\right). \end{aligned}$$

From Inequality 5.4 and the above discussion it follows,

$$r_p \left(A(F)[p]\right) r_p \left(\mathrm{Cl}_S(F_n)\right) \leq r_p \left(R(A/F_n)\right) + O(1). \tag{5.5}$$

This proves the lemma as the hypothesis forces $r_p \left(A(F)[p]\right) \neq 0$. ☕

We now provide a proof of Theorem 5.2.12.

Proof. By Proposition 5.2.4, Conjecture A holds for $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ if and only if $r_p \left(R(E/F_n)\right) = O(1)$. In other words, Conjecture A holds if and only if the p-rank remains bounded in the cyclotomic tower.

We have assumed Conjecture A holds for $\mathfrak{Y}(E/F_{\mathrm{cyc}})$, thus $r_p \left(R(E/F_n)\right) = O(1)$. By hypothesis, $E(F)[p] \neq 0$. Inequality 5.5 implies $r_p \left(\mathrm{Cl}_S(F_n)\right)$ is bounded independent of n. In the cyclotomic tower the primes in S are finitely decomposed, so Equation 3.12 holds; i.e.

$$\left| r_p \left(\mathrm{Cl}(F_n)\right) - r_p \left(\mathrm{Cl}_S(F_n)\right) \right| = O(1).$$

Thus, $r_p \left(\mathrm{Cl}(F_n)\right)$ is bounded independent of n. It follows from Proposition 5.2.3 that the Classical $\mu = 0$ Conjecture holds. ☕

Brief Remarks

Proving Conjecture A *independent* of the Classical $\mu = 0$ Conjecture appears to be a difficult task. By a result of Merel, given a number field F our theorem can at best prove the Classical Iwasawa $\mu = 0$ conjecture for finitely many primes. However, it improves upon a result of Česnavičius [11].

Theorem 5.2.14. *For a prime p and a number field F, to prove the classical Iwasawa $\mu = 0$ conjecture, it suffices to find an Abelian F-variety, A such that*

(i) A has good ordinary reduction at all places above p,

(ii) A has $\mathbb{Z}/p\mathbb{Z}$ as an F-subgroup,

(iii) $\mathfrak{X}(A/F_{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion and has μ-invariant 0.

Our theorem is an improvement over previous results because

(i) there is no condition on the reduction type at primes above p, unlike when one is working with the Selmer group. This is because the dual Selmer group is expected to be $\Lambda(\Gamma)$-torsion only at primes of good ordinary reduction.

(ii) there are no known examples where $\mu(\mathfrak{Y}(E/F_{\text{cyc}})) > 0$ but there are several examples where $\mu(\mathfrak{X}(E/F_{\text{cyc}})) > 0$ even when the base field is $\mathbb{Q}$ and p is a prime of good ordinary reduction.

(iii) in our theorem, we do not need the requirement that $F(E[p])/F$ be a p-extension as in [60]. This appears to be a relatively strict condition to impose when giving concrete examples.

5.2.3 The Classical $\mu = 0$ Conjecture Implies Conjecture A

We now prove the converse of Theorem 5.2.12. It generalizes the following result of Coates and Sujatha.

Theorem 5.2.15. *[22, Corollary 3.6] Assume F is an Abelian extension of $\mathbb{Q}$, p is an odd prime, and $E(F)[p] \neq 0$. Then Conjecture A holds for $\mathfrak{Y}(E/F_{\text{cyc}})$.*

We will prove the following theorem.

Theorem 5.2.16. *Let F be a number field and suppose the Classical $\mu = 0$ Conjecture holds for F_{cyc}. Let E be an elliptic curve over F with $E(F)[p] \neq 0$, then Conjecture A holds for $\mathfrak{Y}(E/F_{\text{cyc}})$.*

Proof. We break the proof into two parts.
Case (i) Suppose $F \supset \mu_p$.
Since $E(F)[p] \neq 0$, it follows from the Weil pairing that $F(E[p])/F$ is either trivial or cyclic of order p. This is precisely the situation of Theorem 2.3.1. There is nothing left to prove.
Case (ii) Suppose $F \not\supset \mu_p$.
First, note that it suffices to prove the following inequality where k_2 is a positive constant,

$$r_p\left(R(E/F_n)\right) \leq k_2 r_p\left(\mathrm{Cl}(F_n)\right) + O(1). \tag{5.6}$$

By Proposition 5.2.3, the Classical $\mu = 0$ Conjecture is equivalent to $r_p\left(\mathrm{Cl}(F_n)\right)$ being bounded independent of n. If the Classical $\mu = 0$ Conjecture holds, it follows from Equation 5.6 that for an elliptic curve E, $r_p\left(R(E/F_n)\right)$ is bounded independent of n. Therefore Conjecture A holds by Proposition 5.2.4.

In the cyclotomic tower, the primes are finitely decomposed. Thus the following estimates hold.

$$\left| r_p\left(\mathrm{Cl}(F_n)\right) - r_p\left(\mathrm{Cl}_S(F_n)\right) \right| = O(1)$$
$$\left| r_p\left(R(E/F_n)\right) - r_p\left(R_p(E/F_n)\right) \right| = O(1).$$

It follows that to prove the theorem, it is enough to show the following variant of Inequality 5.6,

$$r_p\left(R_p(E/F_n)\right) \leq k_2 r_p\left(\mathrm{Cl}_S(F_n)\right) + O(1). \tag{5.7}$$

Define $R_S(E(F_n)[p]/F_n)$ by replacing $E[p]$ with $E(F_n)[p]$ in Exact Sequence 2.5. The Galois action of $G_S(F_n)$ on $E(F_n)[p]$ is trivial; it is possible to relate $R_S\left(E\left(F_n\right)[p]/F_n\right)$ with $\mathrm{Cl}_S(F_n)$ and similarly their p-ranks. Since the Galois action is trivial,

$$H^1\left(G_S\left(F_n\right),\ E\left(F_n\right)[p]\right) = \mathrm{Hom}\left(G_S\left(F_n\right),\ E\left(F_n\right)[p]\right)$$

and there are similar identifications for the local cohomology groups. It follows

$$R_S\left(E\left(F_n\right)[p]/F_n\right) = \mathrm{Hom}\left(\mathrm{Cl}_S\left(F_n\right),\ E\left(F_n\right)[p]\right) \simeq \mathrm{Cl}_S(F_n)[p]^{r_p\left(E(F_n)[p]\right)}$$

where the isomorphism is as Abelian groups. This gives the following inequality of p-ranks

$$r_p\left(R_S\left(E\left(F_n\right)[p]/F_n\right)\right) = r_p\left(E(F_n)[p]\right)\cdot r_p\left(\mathrm{Cl}_S(F_n)\right) \leq 2r_p\left(\mathrm{Cl}_S(F_n)\right).$$

Now Inequality 5.7 follows from the above inequality if we can show that p-ranks of $R_p(E/F_n)$ and $R_S(E(F_n)[p]/F_n)$ have the same order of growth in the cyclotomic tower. This is the content of the next lemma. With this, the proof of the theorem is complete. ☕

Lemma 5.2.17. *Let F be a number field and E/F be an elliptic curve with $E(F)[p] \neq 0$. Let F_{cyc}/F be the cyclotomic $\mathbb{Z}_p$-extension and suppose the Classical $\mu = 0$ Conjecture holds for F_{cyc}. Let S be as defined before. Then*

$$\left| r_p\left(R_S(E(F_n)[p]/F_n)\right) - r_p\left(R_p(E/F_n)\right)\right| = O(1). \tag{5.8}$$

Proof. If $E(F)[p] = E[p]$, then the Lemma is trivial. We focus on the case $E(F)[p] \neq 0,\ E[p]$. Set $B_n = E(F_n)[p]$. Consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & R_S(B_n/F_n) \arrow[r] \arrow[d, "s_n"] & H^1(G_S(F_n),\ B_n) \arrow[r] \arrow[d, "f_n"] & \bigoplus_{v_n} H^1(F_{n,v_n},\ B_n) \arrow[d, "g_n"] \\
0 \arrow[r] & R_p(E/F_n) \arrow[r] & H^1(G_S(F_n),\ E[p]) \arrow[r] & \bigoplus_{v_n} H^1(F_{n,v_n},\ E[p])
\end{tikzcd}$$

where v_n runs over all the primes in the finite set $S(F_n)$.

By hypothesis, E has an F_n-rational p-torsion point. This gives the short exact sequence

$$0 \to B_n \to E[p] \to \mu_p \to 0. \tag{5.9}$$

This is because, if E has an F_n-rational p-torsion point, this point gives an injection $\mathbb{Z}/p\mathbb{Z} \hookrightarrow E[p]$. Therefore,

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to M \to 0.$$

By Cartier duality and the Weil pairing, the above short exact sequence turns into

$$0 \to M^\vee \to E[p] \to \mu_p \to 0,$$

where μ_p is viewed as a quotient of $E[p]$. Since the Weil pairing is alternating, the orthogonal complement of $\mathbb{Z}/p\mathbb{Z}$ is $\mathbb{Z}/p\mathbb{Z}$, thus $M^\vee = \mathbb{Z}/p\mathbb{Z}$ as a subgroup of $E[p]$.

Taking the $G_S(F_n)$-cohomology of Exact Sequence 5.9, $\ker(f_n) \subseteq H^0(G_S(F_n),\ \mu_p)$. Since μ_p is finite, therefore $r_p\left(\ker(f_n)\right) = O(1)$ and hence $r_p\left(\ker(s_n)\right) = O(1)$. A similar argument for the local cohomology gives $r_p\left(\ker(g_n)\right) = O(1)$.

By Lemma 3.1.5 applied to the map s_n,

$$\begin{aligned}\Big| r_p\left(R_S(B_n/F_n)\right) - r_p\left(R_p(E/F_n)\right)\Big| &\leq 2r_p\left(\ker(s_n)\right) + r_p\left(\operatorname{coker}(s_n)\right)\\ &= r_p(\operatorname{coker}(s_n)) + O(1).\end{aligned}$$

If $r_p\left(\operatorname{coker}(s_n)\right) = O(1)$, the proof is complete.

Observe, $\operatorname{coker}(f_n) \subseteq H^1\left(G_S\left(F_n\right),\ \mu_p\right)$ and $\operatorname{coker}(g_n) \subseteq \bigoplus_{v_n} H^1(F_{n,v_n},\ \mu_p)$. Further, note that

$$r_p\left(\ker\left(H^1\left(G_S\left(F_n\right),\ \mu_p\right) \to \bigoplus_{v_n} H^1\left(F_{n,v_n},\ \mu_p\right)\right)\right) = O(1) \Rightarrow r_p\left(\operatorname{coker}(s_n)\right) = O(1).$$

For ease of notation, refer to the kernel as a *fine Selmer group*, $R_S(\mu_p/F_n)$.

By hypothesis, the Classical $\mu = 0$ Conjecture holds for F_{cyc}/F. By Proposition 5.2.2, it is equivalent to $H^2\left(G_S\left(F_{\text{cyc}}\right),\ \mu_p\right) = 0$. This latter statement is often referred to as *Conjecture A for* μ_p. Using equivalent reformulations recorded in Theorem 5.2.6,

$$\begin{aligned}H^2\left(G_S\left(F_{\text{cyc}}\right),\ \mu_p\right) = 0 &\Leftrightarrow \varprojlim_n \left(H^2\left(G_S\left(F_n\right),\ \mu_p\right)\right) \text{ is finite}\\ &\Leftrightarrow R_S\left(\mu_p/F_{\text{cyc}}\right) \text{ is finite}\\ &\Leftrightarrow \varinjlim_n R_S\left(\mu_p/F_n\right) \text{ is finite}\\ &\Leftrightarrow R_S\left(\mu_p/F_n\right) \text{ is finite and bounded.}\end{aligned}$$

This implies $r_p\left(\operatorname{coker}(s_n)\right) = O(1)$ and the proof is now complete. ☕

5.2.4 Isogeny Invariance

In [22], the authors claimed that Conjecture A *should be* invariant under isogeny. However, proving this isogeny invariance appears to be just as hard. Theorems 5.2.12 and 5.2.16 prove isogeny invariance of Conjecture A in some previously unknown cases (see [100]).

Corollary 5.2.18. *Let F be a number field and E, E' be isogenous elliptic curves such that both have non-trivial p-torsion points over F. Then, Conjecture A holds for $\mathfrak{Y}(E/F_{\text{cyc}})$ if and only if Conjecture A holds for $\mathfrak{Y}(E'/F_{\text{cyc}})$.*

Proof. Let E be an elliptic curve isogenous to E' over F with the additional property that both $E(F)[p],\ E'(F)[p]$ are non-trivial. WLOG if Conjecture A holds for $\mathfrak{Y}(E/F_{\text{cyc}})$, then by Theorem 5.2.12 the Classical $\mu = 0$ Conjecture holds for F_{cyc}/F. Now, by Theorem 5.2.16 Conjecture A holds for $\mathfrak{Y}(E'/F_{\text{cyc}})$. This proves the corollary. ☕

Remark 5.2.19. All statements made in this section hold for Abelian varieties of dimension d, with the only caveat that the factor 2 gets replaced by $2d$ in some of the statements. Further, the only property of the cyclotomic $\mathbb{Z}_p$-extension we require in all our proofs is that primes in a certain (finite) set are finitely decomposed. The theorems are stated for elliptic curves over the cyclotomic $\mathbb{Z}_p$-extension as the original Conjecture A was made in this setting.

5.3 p-Rational Fields

The notion of p-rational number fields was introduced by Movaheddi and Nguyen Quang Do [29].

Definition 5.3.1. *Let F be a number field, p be an odd prime, and S_p be the set of primes above p. The maximal p-ramified extension of F is denoted F_{S_p}; set $F_{S_p}(p)$ to be its maximal pro-p quotient. Let $\mathcal{G}_{S_p}(F)$ denote the Galois group* $\mathrm{Gal}(F_{S_p}(p)/F)$.
F is called a ***p-rational number field*** *if and only if $\mathcal{G}_{S_p}(F)$ is pro-p-free.*

Here are some examples of p-rational fields [29, Page 163],

(i) the field of rational numbers, $\mathbb{Q}$.

(ii) an imaginary quadratic field K, such that p does not divide its class number.

(iii) the Abelian field $\mathbb{Q}(\mu_{p^n})$, where p is a regular prime and $n \geq 1$.

More recently, p-rational number fields have been studied by Greenberg [37], wherein he explains heuristic reasons to believe that given a number field F, it *should be* p-rational for all primes outside a set of density 0. In [3], Barbulescu and Ray provide examples of *non-Abelian* p-rational number fields.

5.3.1 The Classical $\mu = 0$ Conjecture for p-Rational Fields

In this section, we show that the Classical $\mu = 0$ Conjecture holds for p-rational number fields. The results in this section might be known to experts but as per the knowledge of the author they have not been written down in the literature.

Let F be a number field. Let S be a finite set of primes of F *containing* the primes above p and the Archimedean primes. The weak Leopoldt conjecture in the classical setting is the assertion

$$H^2\Big(\mathrm{Gal}\left(F_S/F_{\mathrm{cyc}}\right),\ \mathbb{Q}_p/\mathbb{Z}_p\Big) = 0. \tag{5.10}$$

It holds for the cyclotomic extension of a number field [76, Theorem 10.3.25]. If Equation 5.10 holds for a finite set S as mentioned above, it also holds for the set $S = \Sigma = S_p \cup S_\infty$ [76, Theorem 11.3.2]. Therefore, the weak Leopoldt Conjecture is independent of the choice of S. From here on, fix $S = \Sigma$.

The following theorem is well-known.

Theorem 5.3.2. *[76, Theorem 11.3.7] The Classical $\mu = 0$ Conjecture holds for F_{cyc} if and only if $\mathcal{G}_\Sigma(F_{\mathrm{cyc}}) = \mathrm{Gal}(F_\Sigma(p)/F_{\mathrm{cyc}})$ is a free pro-p group.*

Proposition 5.3.3. *[94, Page 23] A pro-p group G is free if and only if its p-cohomological dimension* $\mathrm{cd}_p(G) \leq 1$.

By a standard fact in Galois cohomology of pro-p groups [94, Chapter I, Section 4, Proposition 21], an equivalent formulation of Theorem 5.3.2 is the following: the Classical $\mu = 0$ Conjecture holds for F_{cyc} if and only if

$$H^2(\mathcal{G}_\Sigma(F_{\mathrm{cyc}}),\ \mathbb{Z}/p\mathbb{Z}) = 0. \tag{5.11}$$

Corollary 5.3.4. *Let F be a p-rational number field. The Classical $\mu = 0$ Conjecture holds for F_{cyc}.*

Proof. Note $p \neq 2$, we can replace S_p by Σ in the definition of p-rational fields. By definition, for p-rational number fields, $\mathcal{G}_\Sigma(F) = \mathrm{Gal}(F_\Sigma(p)/F)$ has p-cohomological dimension at most 1, i.e.

$$H^2(\mathcal{G}_\Sigma(F),\ \mathbb{Z}/p\mathbb{Z}) = 0.$$

Since $\mathcal{G}_\Sigma(F_{\mathrm{cyc}}) = \mathrm{Gal}(F_\Sigma(p)/F_{\mathrm{cyc}})$ is a closed normal subgroup of $\mathcal{G}_\Sigma(F)$, we know by Proposition A.3.4,

$$\mathrm{cd}_p\left(\mathcal{G}_\Sigma(F_{\mathrm{cyc}})\right) \leq \mathrm{cd}_p\left(\mathcal{G}_\Sigma(F)\right) \leq 1.$$

Thus,

$$H^2(\mathcal{G}_\Sigma(F_{\mathrm{cyc}}),\ \mathbb{Z}/p\mathbb{Z}) = 0.$$

By Equation 5.11, the result follows. ☕

This allows us to provide new evidence for Conjecture A.

Corollary 5.3.5. *Let F be a p-rational number field and E/F be an elliptic curve with $E(F)[p] \neq 0$. Then Conjecture A holds for $\mathfrak{Y}(E/F_{\mathrm{cyc}})$.*

Proof. This follows from Theorem 5.2.16 and Corollary 5.3.4. ☕

In some cases, Conjecture A can be shown to hold *independent* of the Classical $\mu = 0$ Conjecture.

Proposition 5.3.6. *Let F be a p-rational field and E be an elliptic curve with good reduction everywhere over F (or bad reduction at primes above p) such that $E[p] \subset E(F)$. Then Conjecture A holds for $\mathfrak{Y}(E/F_{\mathrm{cyc}})$.*

Proof. By hypothesis, we may choose $S = \Sigma = S_p \cup S_\infty$. By p-rationality of F and the isomorphism of the inflation map [76, Corollary 10.4.8], it follows

$$H^2\left(\mathcal{G}_\Sigma\left(F\right),\ E[p]\right) = H^2\left(G_\Sigma\left(F\right),\ E[p]\right) = 0. \tag{5.12}$$

By Hochschild-Serre spectral sequence, we have the following exact sequence [76, Page 119]

$$H^2\left(\mathcal{G}_\Sigma\left(F\right),\ E[p]\right) \to H^0\Big(\Gamma,\ H^2\Big(\mathcal{G}_\Sigma\left(F_{\mathrm{cyc}}\right),\ E[p]\Big)\Big) \to 0,$$

where $\Gamma = \mathrm{Gal}(F_{\mathrm{cyc}}/F)$. The first term is 0, thus $H^0\Big(\Gamma,\ H^2\Big(\mathcal{G}_\Sigma\left(F_{\mathrm{cyc}}\right),\ E[p]\Big)\Big)$ is trivial. Furthermore, $H^2\Big(\mathcal{G}_\Sigma\left(F_{\mathrm{cyc}}\right),\ E[p]\Big)$ is a discrete module, so it must be 0. Once again by the isomorphism of the inflation map,

$$0 = H^2\Big(\mathcal{G}_\Sigma\left(F_{\mathrm{cyc}}\right),\ E[p]\Big) = H^2\Big(G_\Sigma\left(F_{\mathrm{cyc}}\right),\ E[p]\Big).$$

By Proposition 5.2.5, Conjecture A holds for $\mathfrak{Y}(E/F_{cyc})$. ☕

Remark 5.3.7. We seem to crucially need that $E[p] \subset E(F)$, so as to ensure $E[p]$ is a $\mathcal{G}_\Sigma(F_{\mathrm{cyc}})$-module.

Chapter 6

Conjecture B and its Relation with Greenberg's Conjecture on Pseudo-nullity

Recently, there has been a renewed interest in studying pseudo-null modules over Iwasawa algebras [5]. It is natural to investigate Conjecture B, whose validity has been established by few concrete examples.

We remind the reader of both the pseudo-nullity conjectures. In the classical setting we have the conjecture of Greenberg over a $\mathbb{Z}_p^d$-extension.

Generalized Greenberg's Conjecture. *Let F be a number field. Let $\widetilde{F}$ be the compositum of all $\mathbb{Z}_p$-extensions of F with $\mathrm{Gal}\left(\widetilde{F}/F\right) \simeq \mathbb{Z}_p^d$ and let $\widetilde{L}$ denote its pro-p Hilbert class field. Then $X_d = \mathrm{Gal}(\widetilde{L}/\widetilde{F})$ is a pseudo-null $\Lambda(\Gamma_d)$-module.*

For elliptic curves, we have the conjecture of Coates and Sujatha over admissible p-adic Lie extensions.

Conjecture B. *Let E be an elliptic curve defined over a number field F, such that Conjecture A holds for $\mathfrak{Y}(E/F_{\mathrm{cyc}})$. Let $\mathcal{L}/F$ be an admissible p-adic Lie extension, and $G_{\mathcal{L}} = \mathrm{Gal}(\mathcal{L}/F)$ be a pro-p p-adic Lie group of dimension strictly greater than 1. Then $\mathfrak{Y}(E/\mathcal{L})$ is a pseudo-null $\Lambda(G_{\mathcal{L}})$-module.*

We prove that Conjecture B holds for special classes of admissible p-adic Lie extensions whenever the dual fine Selmer group over the cyclotomic extension is finite for a CM elliptic curve. For elliptic curves over $\mathbb{Q}$ and a regular prime p, we show that Conjecture B holds over the pro-p trivializing extension $\mathbb{Q}(E_{p^\infty})/\mathbb{Q}(\mu_p)$. This is also proven for a large class of imaginary Galois extensions.

Concrete examples for the validity of Conjecture B have been rather sparse. Our result settles the case of some numerical examples that were considered in [22, Examples 4.7 and 4.8] but were not fully settled there. Example 4.8 was shown to satisfy Conjecture B provided the elliptic curve had no point of infinite order over the trivialising extension associated to the corresponding Galois representation. This latter condition could not be verified despite advances in computational methods.

Conjecture B is in the spirit of generalising Greenberg's pseudo-nullity conjecture to elliptic curves [35]. We clarify this relationship by proving that for CM elliptic curves over an imaginary quadratic field K, the Generalized Greenberg's Conjecture (GGC) is equivalent to Conjecture B for certain pro-p p-adic Lie extensions. Furthermore, Conjecture B over a trivializing extension of K implies GGC for K.

6.1 Powerful Diagram

We begin this chapter by recalling the Powerful Diagram [77, Section 4]. The proof of our main results will depend heavily on analysing this diagram.

Fox-Lyndon Resolution

Let $\mathcal{G}$ be a finitely generated pro-p group of p-cohomological dimension ≤ 2. Suppose the set of generators of $\mathcal{G}$ has d elements, then it has a *free representation*,

$$0 \to \mathcal{N} \to \mathcal{F}(d) \xrightarrow{s} \mathcal{G} \to 0$$

where $\mathcal{F}(d)$ a free pro-p group of rank d and $\mathcal{N}$ is the kernel of the surjective map s. To this representation one can associate the **Fox-Lyndon resolution**,

$$0 \to \mathcal{N}^{ab}(p) \to \Lambda(\mathcal{G})^d \to \Lambda(\mathcal{G}) \to \mathbb{Z}_p \to 0.$$

Since $\mathrm{cd}_p(\mathcal{G}) \leq 2$, the $\Lambda(\mathcal{G})$-module $\mathcal{N}^{ab}(p)$ is projective. It is called the *p-relation module of $\mathcal{G}$.*

Twists

Let A be a fixed p-divisible, p-primary Abelian group of finite $\mathbb{Z}_p$ co-rank r, with a continuous $\mathcal{G}$-action. For a finitely generated $\Lambda(\mathcal{G})$-module M, define the *twist*,

$$M^{\#} := \mathrm{Hom}_{\mathbb{Z}_p,\mathrm{cont}}\left(M,\ A\right)^{\vee} = M \otimes_{\mathbb{Z}_p} A^{\vee}.$$

Note that $\mathcal{G}$ acts diagonally on the tensor product.

The Diagram

In [77], Ochi and Venjakob developed a general theory. However, we will restrict ourselves to the following specific case: let p be a fixed odd prime, E be an elliptic curve defined over a number field F such that F_∞/F is a pro-p extension, and $S \supseteq S_p \cup S_{bad} \cup S_\infty$. The p-divisible, p-primary module A is E_{p^∞}. Fix the following Galois groups

$$\begin{aligned}
\mathcal{G} &= \text{maximal pro} - p \text{ part of } \mathrm{Gal}(F_S/F)\\
\mathcal{H} &= \text{maximal pro} - p \text{ part of } \mathrm{Gal}(F_S/F_\infty)\\
G &= \mathrm{Gal}(F_\infty/F) \quad (\text{this is a pro} - p \text{ group by assumption})
\end{aligned}$$

There is a composition of maps, $\mathcal{F}(d) \to \mathcal{G} \to G$. Set $\mathcal{R}$ to be the kernel of this composition.

Define the **augmentation ideal** $I(\mathcal{G})$ as $\ker\left(\Lambda\left(\mathcal{G}\right) \to \mathbb{Z}_p\right)$. It is a free $\Lambda(\mathcal{G})$-module of rank d. Consider the following short exact sequence

$$0 \to I(\mathcal{G})^{\#} \to \Lambda(\mathcal{G})^{\#} \to A^{\vee} \to 0,$$

where it is known that $\Lambda(\mathcal{G})^{\#}$ is a projective $\Lambda(\mathcal{G})$-module. Taking the $\mathcal{H}$-homology yields

$$0 \to H_1(\mathcal{H}, A^{\vee}) \to \left(I(\mathcal{G})^{\#}\right)_{\mathcal{H}} \to \left(\Lambda(\mathcal{G})^{\#}\right)_{\mathcal{H}} \to (A^{\vee})_{\mathcal{H}} \to 0.$$

For ease, we introduce the following notation

$$\begin{aligned} Y_{A,F_\infty} &= (I(\mathcal{G})^{\#})_{\mathcal{H}} \\ J_{A,F_\infty} &= \ker\left(\left(\Lambda(\mathcal{G})^{\#})\right)_{\mathcal{H}} \to (A^{\vee})_{\mathcal{H}}\right). \end{aligned}$$

The following commutative diagram is a generalization of the work of Jannsen. It is referred to as the **Powerful Diagram** [77, Lemma 4.5].

$$\begin{tikzcd}
 & & & 0 & 0 & \\
 & & & J_{A,F_\infty} \arrow[u] \arrow[r, equal] & J_{A,F_\infty} \arrow[u] & \\
0 \arrow[r] & H^2\left(G_S\left(F_\infty\right),\ A\right)^{\vee} \arrow[r] & \left(\mathcal{N}^{ab}\left(p\right)^{\#}\right)_{\mathcal{H}} \arrow[r] & \Lambda(G)^{2d} \arrow[r] \arrow[u] & Y_{A,\ F_\infty} \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & H^2\left(G_S\left(F_\infty\right),\ A\right)^{\vee} \arrow[r] \arrow[u, equal] & \left(H^1\left(\mathcal{N}^{ab}\left(p\right),\ A\right)^{\mathcal{H}}\right)^{\vee} \arrow[r] \arrow[u, "\simeq"] & H^1\left(\mathcal{R},\ A\right) \arrow[r] \arrow[u] & H^1\left(G_S\left(F_\infty\right),\ A\right)^{\vee} \arrow[r] \arrow[u] & 0 \\
 & & & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd}$$

Figure 6.1: Powerful Diagram

$\left(\mathcal{N}^{ab}(p)^{\#}\right)_{\mathcal{H}}$ is a projective module. It is known that if $H^2(G_S(F_\infty),\ A) = 0$, Y_{A,F_∞} has projective dimension ≤ 1. Further, J_{A,F_∞} has no non-zero torsion submodules. If $\mathcal{H}$-action on A is trivial,

$$\left(\mathcal{N}^{ab}(p)^{\#}\right)_{\mathcal{H}} \simeq \left(\mathcal{N}^{ab}(p)_{\mathcal{H}}\right)^{\#}.$$

6.2 pseudo-nullity Conjecture for Elliptic Curves

In this section, the goal is to provide new evidence for Conjecture B when $\mathcal{L} = F_\infty$, i.e. when it is the trivializing extension as defined in Equation 2.4. We study it in two separate cases. First, for CM elliptic curves we prove that Conjecture B holds provided the fine Selmer group is *finite* over the cyclotomic extension. Second, we prove Conjecture B over a large class of imaginary Galois extensions for regular primes. This proof works for all elliptic curves.

6.2.1 Finite Fine Selmer Group at the Cyclotomic Level

Recall the set up introduced in Section 2.2.3. Let K be an imaginary quadratic number field and E be a CM elliptic curve defined over a a finite extension F/K. Let $p \neq 2,\ 3$ be an unramified prime in F at which E has good ordinary reduction. In this case, $\mathrm{Gal}(F_\infty/F)$ contains an open subgroup which is Abelian and isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. Assume $G = \mathrm{Gal}(F_\infty/F)$ is pro-p, and set $H = \mathrm{Gal}(F_\infty/F_{\mathrm{cyc}})$.

Let G be any p-adic Lie group. Recall that for a finitely generated $\Lambda(G)$-module M, the co-invariance $M_G := H_0(G, M) = M/IM$ is a finitely generated $\Lambda(G)$-module.

Lemma 6.2.1. *With the setting as above, the following natural map is a pseudo-isomorphism, i.e. it has a finite kernel and cokernel,*

$$\mathfrak{Y}(E/F_\infty)_H \to \mathfrak{Y}(E/F_{\text{cyc}}).$$

Proof. Consider the following diagram

$$\begin{tikzcd}
0 \arrow[r] & R(E/F_{\text{cyc}}) \arrow[r] \arrow[d, "\alpha"] & \text{Sel}(E/F_{\text{cyc}}) \arrow[r] \arrow[d, "\beta"] & C(F_{\text{cyc}})(p) \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & R(E/F_\infty)^H \arrow[r] & \text{Sel}(E/F_\infty)^H \arrow[r] & C(F_\infty)(p)^H &
\end{tikzcd}$$

By a result of Perrin-Riou, β is an isomorphism [79, Lemma 1.1(i) and Lemma 1.3]. Therefore, $\ker(\beta) = \text{coker}(\beta) = 0$; hence $\ker(\alpha) = 0$. Also, $\ker(\gamma) = \bigoplus_{v|p} H^1(H_v,\ E(F_{\infty,v})[p^\infty])$ is finite [23]. Now, by an application of the snake lemma, $\text{coker}(\alpha)$ must be finite. ☕

Note that E is an elliptic curve with CM, therefore $\Lambda(H) \simeq \mathbb{Z}_p[[T]]$.

Lemma 6.2.2. *Let M be a finitely generated $\Lambda(H)$-module. If M_H is a finite module, then M is a pseudo-null $\Lambda(G)$-module.*

Proof. If M_H is finite, the higher homology groups $H_i(H, M)$ are trivial for all $i > 0$ [93, Chapter IV, Appendix II]. Since $\Lambda(H)$ is a regular local ring, we know from Equation 2.7 that the rank of a module is equal to its homological rank. By hypothesis, $\Lambda(H)$-rank of M is 0, equivalently M is $\Lambda(H)$-torsion. The lemma follows from the equivalent definition of pseudo-nullity for p-adic Lie extensions "arising from geometry" (see Section 2.4.2). ☕

Theorem 6.2.3. *With the set up as above, if $\mathfrak{Y}(E/F_{\text{cyc}})$ is finite, $\mathfrak{Y}(E/F_\infty)$ is a pseudo-null $\Lambda(G)$-module, i.e. Conjecture B holds for $\mathfrak{Y}(E/F_\infty)$.*

Proof. By Lemma 6.2.1, it follows that $\mathfrak{Y}(E/F_\infty)_H$ is finite when $\mathfrak{Y}(E/F_{\text{cyc}})$ is finite. By Lemma 6.2.2, finiteness of $\mathfrak{Y}(E/F_\infty)_H$ implies that $\mathfrak{Y}(E/F_\infty)$ is pseudo-null. ☕

Note this proof can not be extended to the non-CM case. The primary reason for that is β is no longer an isomorphism. In fact, by the work of Coates and Howson, it is known that $\ker(\beta)$ and $\text{coker}(\beta)$ are finitely generated as $\mathbb{Z}_p$-modules with $\mathbb{Z}_p$-rank equal to the number of primes at which E has split multiplicative reduction over F_{cyc} [18]. Also, in the non-commutative setting an analogue of Lemma 6.2.2 is not well understood.

6.2.2 Conjecture B for Regular Primes

In this section we prove Conjecture B over the trivializing extension when p does not divide the class number of the base field. The main theorem is the following statement.

Theorem 6.2.4. *Consider a Galois extension $F/\mathbb{Q}$ containing μ_p such that $p \nmid |\text{Cl}(F)|$ and p is totally ramified in F. Suppose F_∞/F is a pro-p extension. For E an elliptic curve defined over F, Conjecture B holds for $\mathfrak{Y}(E/F_\infty)$.*

Lemma 6.2.5. *Let $\mathcal{L}$ be an S-admissible p-adic Lie extension of F with $\text{Gal}(\mathcal{L}/F) = G$. Suppose $G_S(\mathcal{L})$ acts trivially on $E[p^\infty]$. Then $H^2\left(G_S\left(\mathcal{L}\right),\ E[p^\infty]\right) = 0$ and $\mathcal{Z}^2\left(E/\mathcal{L}\right)$ is a $\Lambda(G)$-torsion module.*

Proof. As a $G_S(\mathcal{L})$-module, $E[p^\infty]$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^2$ and the Galois action is trivial. In [50], Iwasawa proved that for the cyclotomic $\mathbb{Z}_p$-extension L_{cyc}/L,

$$H^2\left(G_S(L_{\text{cyc}}),\ \mathbb{Q}_p/\mathbb{Z}_p\right) = 0$$

for every finite extension L/F. Taking the inductive limit one obtains

$$H^2\left(G_S(\mathcal{L}),\ \mathbb{Q}_p/\mathbb{Z}_p\right) = 0.$$

The last assertion follows from Lemma 2.5.1. ☕

Proposition 6.2.6. *With the setting as in the statement of Theorem 6.2.4,*

$$E^1\left(\mathcal{Z}^2\left(E/F_\infty\right)\right) := \operatorname{Ext}^1_{\Lambda(G)}\left(\mathcal{Z}^2\left(E/F_\infty\right),\ \Lambda(G)\right) = 0.$$

Proof. The rightmost column of the Powerful Diagram is the short exact sequence

$$0 \to H^1\left(G_S\left(F_\infty\right),\ E_{p^\infty}\right)^\vee \to Y_\infty \to J_\infty \to 0. \tag{6.1}$$

The following isomorphism is known by a result of Ochi and Venjakob [78, Proposition 3.5]

$$E^1\left(\mathcal{Z}^2\left(E/F_\infty\right)\right) \simeq H^1\left(G_S\left(F_\infty\right),\ E_{p^\infty}\right)^\vee_{\text{tors}}. \tag{6.2}$$

To prove the proposition it is enough to show $H^1(G_S(F_\infty), E_{p^\infty})^\vee_{\text{tors}} = 0$. Since J_∞ has no non-zero torsion submodules, the proposition follows if Y_∞ has no Λ-torsion submodules. This is done by a thorough analysis of the Powerful Diagram.

Since F_∞ is the trivializing extension, the top row of the Powerful Diagram is the following short exact sequence,

$$0 \to \left(\mathcal{N}^{ab}(p) \otimes_{\mathbb{Z}_p} E^\vee_{p^\infty}\right)_{\mathcal{H}} \to \Lambda(G)^{2d} \to Y_\infty \to 0 \tag{6.3}$$

where $d := \dim_{\mathbb{F}_p} H^1(\mathcal{G},\ \mathbb{F}_p)$. We now analyse the first term of the exact sequence. It is known [78, Proof of Theorem 3.2]

$$\left(\mathcal{N}^{ab}(p) \otimes_{\mathbb{Z}_p} E^\vee_{p^\infty}\right)_{\mathcal{H}} = \Lambda(G)^{2s}$$

where $s = d - r_2 - 1$ when $p \neq 2$. Therefore Exact Sequences 6.3 becomes

$$0 \to \Lambda(G)^{2s} \to \Lambda(G)^{2d} \to Y_\infty \to 0. \tag{6.4}$$

By [76, Lemma 10.7.3] we know

$$d = 1 + \sum_{\mathfrak{p} \in S} \delta_{\mathfrak{p}} - \delta + \dim_{\mathbb{F}_p}(\mathrm{Cl}_S(F)/p). \tag{6.5}$$

where $\delta_{\mathfrak{p}}$ (resp. δ) is 1 if $\mu_p \subseteq F_{\mathfrak{p}}$ (resp. $\mu_p \subseteq F$) and 0 otherwise. By hypothesis, F contains μ_p, so $\delta = 1$. Also by hypothesis, $p \nmid |\operatorname{Cl}(F)|$. Since the class group of a number field is always finite and the S-class group is a subgroup of the class group, it follows that $\dim_{\mathbb{F}_p}(\mathrm{Cl}_S(F)/p) = 0$. Choose $S = S_p \cup S_{bad} \cup S_\infty$. Since p ramifies totally in F, $|S_p| = 1$. Further, since F is a totally imaginary field,

$|S_\infty| = r_2$. Thus,

$$\begin{aligned}|S| &= |S_p| + |S_\infty| + |S_{bad}| \\ &= 1 + r_2 + |S_{bad}|\end{aligned}$$

Under our hypothesis, the contribution of $\delta_{\mathfrak{q}} = 0$ for $\mathfrak{q} \in S \setminus S_p$. Therefore from Equation 6.5

$$\begin{aligned}d &= r_2 + 1. \\ \Rightarrow s &= d - r_2 - 1 = 0.\end{aligned}$$

Since $s = 0$, from Exact Sequence 6.4 it follows $Y_\infty \simeq \Lambda(G)^{2d}$ and hence it is torsion free. ☕

We restate the main theorem of this section for convenience.

Theorem. *Consider a Galois extension $F/\mathbb{Q}$ containing μ_p such that $p \nmid |\operatorname{Cl}(F)|$ and p is totally ramified in F. Suppose F_∞/F is a pro-p extension. For E/F an elliptic curve, Conjecture B holds for $\mathfrak{Y}(E/F_\infty)$.*

Proof. By definition of pseudo-nullity (see (2.8)), to prove the theorem, we need to prove

$$E^i\left(\mathfrak{Y}\left(E/F_\infty\right)\right) = 0 \quad \text{for } i = 0, 1. \tag{6.6}$$

By Poitou-Tate duality introduced in Exact Sequence 2.9,

$$\mathfrak{Y}\left(E/F_\infty\right) \hookrightarrow \mathcal{Z}^2\left(E/F_\infty\right).$$

Therefore $\mathfrak{Y}\left(E/F_\infty\right)$ is a pseudo-null $\Lambda(G)$-module if $\mathcal{Z}^2(E/F_\infty)$ is pseudo-null, i.e.

$$E^i\left(\mathcal{Z}^2\left(E/F_\infty\right)\right) = 0 \quad \text{for } i = 0, 1.$$

Since F_∞ is the trivializing extension, by Lemma 6.2.5 $H^2\left(G_S(F_\infty),\ E_{p^\infty}\right) = 0$ and $\mathcal{Z}^2(E/F_\infty)$ is a torsion $\Lambda(G)$-module. Thus, $E^0\left(\mathcal{Z}^2\left(E/F_\infty\right)\right) = 0$. By Proposition 6.2.6, $E^1\left(\mathcal{Z}^2\left(E/F_\infty\right)\right) = 0$. With this the proof is complete. ☕

6.2.3 Trivial Fine Selmer Groups over the Trivializing Extension

Under some restrictive conditions, it will be possible to show that the fine Selmer group is in fact trivial over the trivializing extension. This will be proved as a corollary of the following result of Iwasawa.

Theorem 6.2.7. *[46, Theorem II] Let F be a number field and F' be a cyclic extension of p-power degree. Suppose $\mathfrak{p}$ is the unique prime above p in F, it remains totally ramified in F', and there are no ramified primes other that $\mathfrak{p}$ in F'. Then*

$$p \nmid \operatorname{Cl}(F) \Rightarrow p \nmid \operatorname{Cl}(F').$$

An iterative application of the above theorem yields the following corollary.

Corollary 6.2.8. *Let p be a fixed odd prime. Let F be a number field such that $p \nmid \operatorname{Cl}(F)$ and $\mathfrak{p}$ is the unique prime above p in F. Let E/F be an elliptic curve such that it has good reduction everywhere over*

F or has bad reduction at primes above p. Suppose the trivializing extension F_∞/F is a pro-p extension, then $\mathfrak{Y}(E/F_\infty) = 0$.

Proof. Set the notation $M(F_\infty)/F_\infty$ to denote the maximal unramified Abelian p-extension in which every prime above p splits completely. It is well known [22, Lemma 3.8]

$$R\left(E/F_\infty\right) = \mathrm{Hom}\Big(\mathrm{Gal}\left(M\left(F_\infty\right)/F_\infty\right),\ E_{p^\infty}\Big).$$

Since $p \nmid \mathrm{Cl}(F)$, iterative application of Theorem 6.2.7 yields that the p-part of the Iwasawa algebra over the trivializing extension is trivial. Since $\mathrm{Gal}\left(M\left(F_\infty\right)/F_\infty\right)$ is a quotient of the p-part of the Iwasawa algebra, it follows that the fine Selmer group is trivial. ☕

6.3 NUMERICAL EXAMPLES FOR CONJECTURE B

In [22], the authors mentioned two possible examples of elliptic curves where Conjecture B could hold. For the first, they could show that the $\Lambda(H)$-rank of $\mathfrak{Y}(E/F_\infty)$ is even but could not rule out the possibility of the rank being 2; for the other it could not be shown that there is no point of infinite order over F_∞. A special case of Theorem 6.2.4 resolves Conjecture B for both these examples.

Theorem 6.3.1 (Special Case of Theorem 6.2.4)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Set $F = \mathbb{Q}(\mu_p)$ such that p is a regular prime. Then Conjecture B is true for $\mathfrak{Y}\Big(E/\mathbb{Q}\left(E_{p^\infty}\right)\Big)$.*

Proof. Recall, an odd rational prime p, is called **regular** if it does not divide the class number of $\mathbb{Q}(\mu_p)$. It follows that this is a particular case of Theorem 6.2.4. ☕

For historical reasons, elliptic curves of conductor 11 are very special in Iwasawa theory. It is known that there are three elliptic curves up to isomorphism of conductor 11; all three of them are isogenous over $\mathbb{Q}$. Conjecture A is known to be true for all three of these elliptic curves [106].

We note that Conjecture B is isogeny invariant [22, Page 827]. Indeed, if $E \xrightarrow{\varphi} E'$ is an isogeny, the dual isogeny $\varphi^\vee$ induces $\Lambda(G)$-homomorphisms in both directions between the dual fine Selmer groups $\mathfrak{Y}(E/F_\infty)$ and $\mathfrak{Y}(E'/F_\infty)$. The kernels and the cokernels are annihilated by the degree of the isogeny. This proves $\mathfrak{Y}(E/F_\infty)$ is $\Lambda(H)$-torsion if and only if $\mathfrak{Y}(E'/F_\infty)$ is $\Lambda(H)$-torsion.

Example 6.3.2. [20, Chapter 5] Consider the elliptic curve $E/\mathbb{Q}$ defined by

$$E : y^2 + y = x^3 - x^2.$$

This is an elliptic curve of conductor 11 without CM. When $F = \mathbb{Q}(\mu_5)$ and $p = 5$, $\mathrm{Sel}(E/F_{\mathrm{cyc}})_p = 0$ [20, Theorem 5.4]. Theorem 6.3.1 shows that Conjecture B holds for $\mathfrak{Y}(E/F_\infty)$ where $F_\infty = \mathbb{Q}(E_{5^\infty})$.

By the above discussion, Conjecture B holds at the prime $p = 5$ for *all three* elliptic curves (up to isomorphism) of conductor 11.

6.3.1 EXAMPLE 1: CURVE OF CONDUCTOR 294

We need the following theorem for the discussion.

Theorem 6.3.3. *[22, Theorem 4.5] Let $p \geq 5$. Assume F_∞/F is the trivializing extension such that $G = \mathrm{Gal}(F_\infty/F)$ is pro-p and $\mathfrak{X}(E/F_{\mathrm{cyc}})$ has μ-invariant 0. Set $H = \mathrm{Gal}(F_\infty/F_{\mathrm{cyc}})$.*

(i) If $\operatorname{rank}_{\Lambda(H)}(\mathfrak{X}(E/F_\infty))$ *is odd,*

$$\operatorname{rank}_{\Lambda(H)}\left(\mathfrak{Y}\left(E/F_\infty\right)\right) \leq \operatorname{rank}_{\Lambda(H)}\left(\mathfrak{X}\left(E/F_\infty\right)\right) - 1.$$

(ii) If $\operatorname{rank}_{\Lambda(H)}\left(\mathfrak{X}\left(E/F_\infty\right)\right)$ *is even and* $E(F_\infty)$ *has a point of infinite order,*

$$\operatorname{rank}_{\Lambda(H)}\left(\mathfrak{Y}\left(E/F_\infty\right)\right) \leq \operatorname{rank}_{\Lambda(H)}\left(\mathfrak{X}\left(E/F_\infty\right)\right) - 2.$$

Example. [22, Example 4.7] Consider the following elliptic curve $E/\mathbb{Q}$,

$$E : y^2 + xy = x^3 - x - 1.$$

This is a non-CM elliptic curve of conductor 294. Take $p = 7$. Here, $F_\infty = \mathbb{Q}(E_{7^\infty})$ is a pro-7 extension of $F = \mathbb{Q}(\mu_7)$. E has good ordinary reduction at the unique prime above 7, split multiplicative reduction at the primes above 2, and the unique prime above 3. For this elliptic curve, $\operatorname{Sel}(E/F_{\text{cyc}}) = 0$ [20, Theorem 5.32]. Then

$$\operatorname{rank}_{\Lambda(H)}\left(\mathfrak{X}\left(E/F_\infty\right)\right) = \operatorname{rank}_{\mathbb{Z}_p}\left(\mathfrak{X}\left(E/F_{\text{cyc}}\right)\right) + r$$

where r is the number of primes of F_{cyc} at which E has split multiplicative reduction [44, Theorem 2.8]. There are three primes of F_{cyc} where E has split multiplicative reduction, so $\operatorname{rank}_{\Lambda(H)}\left(\mathfrak{X}\left(E/F_\infty\right)\right) = 3$. By Theorem 6.3.3(i),

$$\operatorname{rank}_{\Lambda(H)}\left(\mathfrak{Y}\left(E/F_\infty\right)\right) \leq \operatorname{rank}_{\Lambda(H)}\left(\mathfrak{X}\left(E/F_\infty\right)\right) - 1.$$

Since $\mathfrak{Y}(E/F_\infty)$ must always have even $\Lambda(H)$-rank, $\operatorname{rank}_{\Lambda(H)}(\mathfrak{Y}(E/F_\infty)) = 0$ or 2. It had not been possible to rule out the latter possibility. The conditions of Theorem 6.3.1 are satisfied, so Conjecture B holds for $\mathfrak{Y}\left(E/\mathbb{Q}\left(E_{7^\infty}\right)\right)$.

6.3.2 Example 2: Curve of Conductor 150

Corollary 6.3.4 (Corollary to Theorem 6.3.3)**.** *Let $p \geq 5$. Assume F_∞/F is the trivializing extension such that $G = \operatorname{Gal}(F_\infty/F)$ is pro-p and $\mathfrak{X}(E/F_{\text{cyc}})$ has μ-invariant 0. If $\operatorname{rank}_{\Lambda(H)}\left(\mathfrak{X}\left(E/F_\infty\right)\right) = 2$, then either $E(F_\infty)$ is a torsion Abelian group or $\mathfrak{Y}(E/F_\infty)$ is pseudo-null.*

Example. [22, Example 4.8] Consider the elliptic curve $E/\mathbb{Q}$ defined by

$$E : y^2 + xy = x^3 - 3x - 3.$$

This is an elliptic curve of conductor 150 without CM. With $p = 5$, $F_\infty = \mathbb{Q}(E_{5^\infty})$ is a pro-5 extension of $F = \mathbb{Q}(\mu_5)$. It is known $\operatorname{Sel}(E/F_{\text{cyc}}) = 0$ [20, section 4.3]. At the unique primes of F above 2 and 3, E has split multiplicative reduction. Therefore $r = 2$ and

$$\operatorname{rank}_{\Lambda(H)}\left(\mathfrak{X}\left(E/F_\infty\right)\right) = 2.$$

By Corollary 6.3.4, either $E(F_\infty)$ has no point of infinite order over F_∞ or $\mathfrak{Y}(E/F_\infty)$ is pseudo-null. Computationally, it had not been possible to check that there is no point of infinite order. Our theorem settles this theoretically as the hypotheses are satisfied.

6.3.3 Example 3: Curve of Conductor 256

Consider the elliptic curve $E/\mathbb{Q}$ defined by

$$E : y^2 + y = x^3 + 156.$$

This is an elliptic curve of conductor 256 with CM by $\mathbb{Q}(\sqrt{-3})$. When $F = \mathbb{Q}(\mu_3)$ and $p = 3$, it is known [61, Elliptic Curve 225.d2] that $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/3\mathbb{Z}$. Set $F_\infty = \mathbb{Q}(E_{3^\infty})$. It follows from the Weil pairing that F_∞/F is a pro-3 extension. Theorem 6.3.1 shows that Conjecture B holds for $\mathfrak{Y}(E/F_\infty)$.
We will see in Remark 6.4.6, that this example allows us to recover GGC for $\mathbb{Q}(\mu_3)$.

6.4 Relating Conjecture B to the Generalized Greenberg's Conjecture

In this section, we clarify the relationship between the Generalized Greenberg's Conjecture and Conjecture B for CM elliptic curves. We are in the setting of Section 2.2.3.

Let K be an imaginary quadratic field and $\mathcal{O}_K$ be its ring of integers. Let E be an elliptic curve over K with CM by $\mathcal{O}_K$ and good reduction at the primes above p. Set

$$F = K(E_p), \quad F_\infty = K(E_{p^\infty}), \quad G = G_{F_\infty} = \mathrm{Gal}(F_\infty/F), \quad \mathcal{G}_\infty = \mathrm{Gal}(F_\infty/K).$$

By our choice of F, G is a pro-p group. In fact, $G \simeq \mathbb{Z}_p^2$. Set $\widetilde{K}$ (resp $\widetilde{F}$) to be the compositum of all $\mathbb{Z}_p$-extensions of K (resp F). It is the unique $\mathbb{Z}_p^2$ Galois extension of K; this is because by the work of Ax and Brumer, Leopoldt conjecture is known for quadratic number fields. Whereas, $\widetilde{F}/F$ is a $\mathbb{Z}_p^d$-extension with $r_2(F) + 1 \leq d \leq [F : \mathbb{Q}]$. Throughout this section, we assume the following.

Hypothesis. *$p \geq 5$ is a prime. p is unramified in K.*

Recall that by the theory of CM, $\mathcal{G}_\infty = G \times \Delta$ where $\Delta \simeq \mathrm{Gal}(F/K)$ is a finite Abelian group. Since p does not ramify in K, $p \nmid |\Delta|$.

By the Weil pairing, $K(E_p) \supset K(\mu_p)$. Furthermore, if $E(K)[p] \neq 0$, then $K(E_p)$ is a trivial or a degree p extension of $K(\mu_p)$. But we know $p \nmid |\Delta|$, this forces

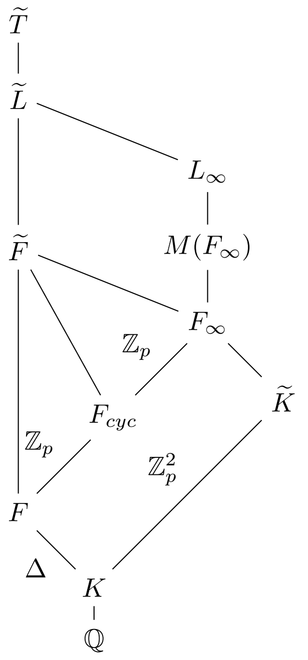
$$F = K(E_p) = K(\mu_p).$$

The theory of CM tells us that $F_\infty = F\widetilde{K}$. By the Weil pairing, the trivializing extension contains the cyclotomic $\mathbb{Z}_p$-extension, hence it is an admissible p-adic Lie extension. Furthermore, $F_\infty \subseteq \widetilde{F}$.

Denote by $\widetilde{L}$ (resp L_∞) the pro-p Hilbert class field tower of $\widetilde{F}$ (resp. F_∞). This is the maximal Abelian unramified pro-p-extension of $\widetilde{F}$ (resp. F_∞). Denote by $\widetilde{T}$ the maximal Abelian extension of $\widetilde{F}$ unramified outside S. Set the notation

$$X_d = X_{nr}^{\widetilde{F}} = \mathrm{Gal}(\widetilde{L}/\widetilde{F}), \quad X_{nr}^{F_\infty} = \mathrm{Gal}(L_\infty/F_\infty), \quad X_S^{\widetilde{F}} = \mathrm{Gal}(\widetilde{T}/\widetilde{F}).$$

For convenience, the field diagram of the set up is drawn below.



In this section, we often vary the p-adic Lie extension, therefore we want to keep track of it in our notation. For any p-adic Lie extension $\mathcal{L}/F$, denote its Galois group $\mathrm{Gal}(\mathcal{L}/F)$ by $G_{\mathcal{L}}$. Denote by $M(\mathcal{L})$ the maximal unramified Abelian p-extension of $\mathcal{L}$ such that primes above p split completely.

Let E be an elliptic curve over F and $\mathcal{L}/F$ be as above. If $G_S(\mathcal{L})$ acts trivially on E_{p^∞}, Conjecture B for $\mathfrak{Y}(E/\mathcal{L})$ can be formulated in terms of pseudo-nullity of a Galois extension of $\mathcal{L}$ [21].

Conjecture B for CM Elliptic Curves. *Let E be an elliptic curve defined over F. Let $\mathcal{L}/F$ be a pro-p, p-adic Lie extension such that $G_S(\mathcal{L})$ acts trivially on E_{p^∞}. Set $\mathfrak{Y}(\mathcal{L}) = \mathrm{Gal}\big(M(\mathcal{L})/\mathcal{L}\big)$. Then $\mathfrak{Y}(\mathcal{L})$ is a pseudo-null $\Lambda(G_{\mathcal{L}})$-module.*

Sketch of equivalence of the two conjectures. Since we assume that $F(E[p^\infty]) \subseteq \mathcal{L}$ and $G_{\mathcal{L}}$ is pro-p, we know that Conjecture A for $\mathfrak{Y}(E/F_{\mathrm{cyc}})$ is equivalent to the Classical $\mu = 0$ Conjecture for F_{cyc}. We will assume these equivalent conjectures hold. Further, since the Galois action is trivial

$$R(E/\mathcal{L}) = \mathrm{Hom}\Big(\mathrm{Gal}\left(M\left(\mathcal{L}\right)/\mathcal{L}\right), E[p^\infty]\Big).$$

It follows that

$$\mathfrak{Y}(E/\mathcal{L}) = \mathrm{Gal}\left(M(\mathcal{L})/\mathcal{L}\right)^{\#}$$

where on the right hand side of the equality the twist is by $E[p^\infty]^\vee$. Set $\mathcal{H} = \mathrm{Gal}(\mathcal{L}/F_{\mathrm{cyc}})$; by comparing $\Lambda(\mathcal{H})$-ranks, $\mathfrak{Y}(E/\mathcal{L})$ is a $\Lambda(\mathcal{H})$-torsion module if and only if the same is true for $\mathrm{Gal}\big(M(\mathcal{L})/\mathcal{L}\big)$. ☕

The first statement we prove in this section says that the Generalized Greenberg's Conjecture and Conjecture B for CM elliptic curves are equivalent over an extension containing the trivializing extension. In proving this, we use several results from [103]. Most of the results we use are in a far more general setting and their proofs are involved; we therefore avoid providing a sketch of these lemmas.

We begin by stating a result from [103]. See also [103, Page 32].

Lemma 6.4.1. *[103, Theorem 4.9] Assume that $\mu_p \subset F$ and let $\mathcal{L} = F_\infty$ or $\widetilde{F}$. $X_{nr}^{\mathcal{L}}$ is pseudo-null if and only if $X_S^{\mathcal{L}}$ is torsion-free.*

Theorem 6.4.2. *With notation as above, let $\mathcal{L} = F_\infty$ or $\widetilde{F}$. Then $X_{nr}^{\mathcal{L}}$ is pseudo-null if and only if Conjecture B holds for $\mathfrak{Y}(E/\mathcal{L})$. Equivalently, $X_{nr}^{\mathcal{L}}$ is pseudo-null if and only if $\mathfrak{Y}(\mathcal{L})$ is pseudo-null.*

Proof. By Lemma 6.4.1, to prove the theorem it is enough to prove

$$X_S^{\mathcal{L}} \text{ is torsion-free} \quad \Leftrightarrow \quad \text{Conjecture B holds for } \mathfrak{Y}(E/\mathcal{L}). \tag{6.7}$$

Simplifying the LHS of Equivalence 6.7: In the classical setting [103, Section 4.1.1],

$$X_S^{\mathcal{L}} = H^1\left(G_S\left(\mathcal{L}\right), \mathbb{Q}_p/\mathbb{Z}_p\right)^\vee \simeq \mathrm{Gal}(F_S/\mathcal{L})^{ab}(p).$$

In this setting, the rightmost column of the Powerful Diagram becomes (cf Figure 6.1)

$$0 \to X_S^{\mathcal{L}} \to Y_S^{\mathcal{L}} \to J^{\mathcal{L}} \to 0.$$

Since it is well-known that $J^{\mathcal{L}}$ has no non-zero torsion submodules, it follows

$$X_S^{\mathcal{L}} \text{ is torsion-free} \quad \Leftrightarrow \quad Y_S^{\mathcal{L}} \text{ is torsion-free.} \tag{6.8}$$

Simplifying the RHS of Equivalence 6.7: From the standard Poitou-Tate sequence (see [22, Equation 45]) we know Conjecture B for $\mathfrak{Y}(E/\mathcal{L})$ is equivalent to the pseudonullity of the Iwasawa cohomology module $\mathcal{Z}^2(E/\mathcal{L})$. It is known [103, Propostion 2.12]

$$\mathcal{Z}^2(E/\mathcal{L}) = \mathcal{Z}^2\left(\mathbb{Z}_p\left(1\right)\right) \otimes T_p(E/\mathcal{L}). \tag{6.9}$$

This gives

$$\begin{aligned} \text{Conjecture B holds for } \mathfrak{Y}(E/\mathcal{L}) &\Leftrightarrow \ \mathcal{Z}^2(E/\mathcal{L}) \text{ is pseudo-null} \\ &\Leftrightarrow \ \mathcal{Z}^2\left(\mathbb{Z}_p\left(1\right)\right) \text{ is pseudonull.} \end{aligned}$$

To prove Equivalence 6.7, it suffices to show $Y_S^{\mathcal{L}}$ is torsion-free if and only if $\mathcal{Z}^2\left(\mathbb{Z}_p\left(1\right)\right)$ is pseudonull. This is precisely [103, Proposition 2.16]. ☕

Theorem 6.4.3. *With the notation above, if there exists one CM elliptic curve E over an imaginary quadratic field K such that $\mathfrak{Y}(E/K(E_{p^\infty}))$ is pseudo-null, then GGC holds for K, $K(\mu_p)$, and $K(E_p)$.*

To prove this theorem, we need to record some lemmas. The following result of Bandini assures pseudo-nullity over a larger tower, once it holds for a non-trivial quotient.

Lemma 6.4.4 (Pseudo-nullity Lifting Lemma)**.** *Let $\mathcal{F}/\mathbb{Q}$ be a finite Galois extension that contains μ_p. As before, $\widetilde{\mathcal{F}}$ is the compositum of all $\mathbb{Z}_p$-extensions of $\mathcal{F}$. Let $\mathrm{Gal}(\widetilde{\mathcal{F}}/\mathcal{F}) \simeq \mathbb{Z}_p^n$ and let $\mathcal{F}' \subset \widetilde{\mathcal{F}}$ such that $\mathrm{Gal}(\mathcal{F}'/\mathcal{F}) \simeq \mathbb{Z}_p^d$ for some $2 \leq d < n$. If $X_{nr}^{\mathcal{F}'}$ is pseudo-null then GGC holds for $\widetilde{\mathcal{F}}/\mathcal{F}$.*

Proof. This lemma is a special case of [2, Theorem 12]. Since it is assumed that $\mathcal{F}$ contains μ_p, the technical conditions in the mentioned theorem are satisfied by [57, Theorem 3.2] or [2, Remark 15]. ☕

The next result of Kleine studies pseudonullity of Galois modules for base change.

Lemma 6.4.5 (Pseudo-nullity Shifting Down Lemma)**.** *Let $\mathcal{F}$ be a number field and $\mathcal{F}'/\mathcal{F}$ be a $\mathbb{Z}_p^d$-extension. Let $\mathcal{F}_1/\mathcal{F}$ be a finite extension such that $\mathbb{F} = \mathcal{F}' \cdot \mathcal{F}_1$. If $X_{nr}^{\mathbb{F}}$ is a pseudo-null module, then $X_{nr}^{\mathcal{F}'}$ is a pseudo-null module.*

Proof. For a proof, see [56, Theorem 3.1(1)].

We now provide a proof of the theorem.

Proof of Theorem 6.4.3. Let E/K be a CM elliptic curve such that Conjecture B holds for $\mathfrak{Y}\left(E/K\left(E_{p^\infty}\right)\right)$. Recall $F = K(E_p) \supset \mu_p$ and by hypothesis, E has good reduction everywhere over F [87, Lemma 2]. Since the definition of the fine Selmer group is independent of the choice of the set S, choose it to be precisely the set of Archimedean primes and primes above p.

(i) We had earlier set the notation $F_\infty = K(E_{p^\infty})$. By Theorem 6.4.2, pseudo-nullity of $\mathfrak{Y}(F_\infty)$ is equivalent to the pseudo-nullity of $X_{nr}^{F_\infty}$. Using Lemma 6.4.4 with $\mathcal{F} = F = K(E_p)$ and $\mathcal{F}' = F_\infty$, Conjecture B for $\mathfrak{Y}\left(E/K\left(E_{p^\infty}\right)\right)$ implies GGC holds for $K(E_p)$.

(ii) Since K is an (imaginary) quadratic field, the Leopoldt conjecture holds, i.e. $\mathrm{Gal}(\widetilde{K}/K) \simeq \mathbb{Z}_p^2$. $\widetilde{K}$ is the unique $\mathbb{Z}_p^2$ extension of K; it is the compositum of all $\mathbb{Z}_p$-extensions of K.
By the theory of CM, $F_\infty = F\widetilde{K}$. Applying Lemma 6.4.5 with $\mathbb{F} = F_\infty = F\widetilde{K}$, pseudo-nullity of $X_{nr}^{F_\infty}$ can be "shift down" to pseudo-nullity of $X_{nr}^{\widetilde{K}}$. This is precisely GGC for the imaginary quadratic field K.

(iii) Now, $K(\mu_p) \subseteq K(E_p)$. So, there is a $\mathbb{Z}_p^2$- extension of $K(\mu_p)$, call it K'_∞, such that

$$K'_\infty = K(\mu_p)\widetilde{K}; \quad F_\infty = FK'_\infty.$$

Applying Lemma 6.4.5 with $\mathbb{F} = F_\infty = FK'_\infty$, pseudo-nullity of $X_{nr}^{F_\infty}$ can be "shift down" to the pseudo-nullity of $X_{nr}^{K'_\infty}$. By Lemma 6.4.4, pseudo-nullity over the $\mathbb{Z}_p^2$-tower can be lifted to the compositum, i.e. GGC holds for $K(\mu_p)$.

Remark 6.4.6. It is possible to imitate the proof of Theorem 6.4.3 to show that if there exists one CM elliptic curve $E/\mathbb{Q}$ such that Conjecture B holds for $\mathfrak{Y}\left(E/\mathbb{Q}\left(E_{p^\infty}\right)\right)$, then GGC holds for $\mathbb{Q}(\mu_p)$. This recovers a result of McCallum [69].

6.5 Conjecture B and its Relation with the Iwasawa Main Conjecture

In this section, we study the implications of Conjecture B to the four term exact sequence studied in proving the Main Conjecture. For simplicity, assume the base field is $\mathbb{Q}$.

Let E be an elliptic curve defined over $\mathbb{Q}$. Since E is modular, there is an associated weight 2 cusp form f_E with Fourier expansion $f_E = \sum_{n\geq 1} a_n q^n$. The coefficients of this Fourier expansion are integral and the L-series associated to this modular form is $L(f_E,\ s) = \sum_{n\geq 1} a_n n^{-s}$.

Given a p^r-th power root of unity $\zeta = \zeta_{p^r}$, we have a homomorphism,

$$\begin{aligned} \phi_\zeta : \Lambda(\Gamma) &\to \mathbb{Z}_p[\zeta] \subset \overline{\mathbb{Q}_p} \\ \gamma &\mapsto \zeta \end{aligned}$$

where γ is the topological generator of Γ. Denote by ψ_ζ the Dirichlet character of $\left(\mathbb{Z}/p^{r+1}\mathbb{Z}\right)^\times$ such that the image of $\gamma \in \Gamma \simeq 1 + p\mathbb{Z}_p$ is sent to ζ.

Suppose E has good ordinary or multiplicative reduction at p. There exists a p-adic L-function $\mathcal{L}(E/\mathbb{Q}_{\mathrm{cyc}})$ such that for any ζ,

$$\phi_\zeta\left(\mathcal{L}\left(E/\mathbb{Q}_{\mathrm{cyc}}\right)\right) = e_p(\zeta)\frac{L\left(f_E,\ \psi_\zeta^{-1},\ 1\right)}{\Omega_{f_E}}.$$

Here, $L\left(f_E,\ \psi_\zeta^{-1},\ 1\right)$ is the twist of the L-series $L(f_E,\ s)$ by the Dirichlet character ψ_ζ^{-1}, Ω_{f_E} is the canonical period of f_E, and

$$e_p(\zeta) = \begin{cases} \alpha_p^{-(r+1)}\frac{p^{r+1}}{G(\psi_\zeta^{-1})} & \zeta \neq 1 \\ \alpha_p^{-1}\left(1 - \frac{1}{\alpha_p}\right)^{m_p}, & \zeta = 1. \end{cases}$$

In the above expression, $G(\psi_\zeta^{-1})$ denotes the Gauss sum. When p is a prime of good ordinary reduction, α_p is the p-adic unit root of $X^2 - a_p(E)X + p$ and $m_p = 1$. If E has multiplicative reduction at p, then $\alpha_p = a_p(E)$ is either 1 or -1, and $m_p = 1$.

We now state the **cyclotomic Main Conjecture** for the p-primary Selmer group $\mathrm{Sel}(E/\mathbb{Q}_{\mathrm{cyc}})$.

Cyclotomic Main Conjecture. *Let E be an elliptic curve defined over $\mathbb{Q}$ with good ordinary or multiplicative reduction at p. The Pontryagin dual $\mathfrak{X}(E/\mathbb{Q}_{\mathrm{cyc}})$ of the Selmer group is a torsion $\Lambda(\Gamma)$-module. Furthermore, its characteristic ideal is generated by a p-adic L-function $\mathcal{L}(E/\mathbb{Q}_{\mathrm{cyc}})$ in $\Lambda(\Gamma) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. If $E[p]$ is an irreducible* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-representation, then $\mathcal{L}(E/\mathbb{Q}_{\mathrm{cyc}})$ is in $\Lambda(\Gamma)$.*

As a consequence of global duality, we have the following short exact sequence of torsion $\Lambda(\Gamma)$-modules

$$0 \to \frac{\mathcal{Z}^1(E/\mathbb{Q}_{\mathrm{cyc}})}{\langle Z \rangle} \to \frac{\mathcal{Z}^1_p(E/\mathbb{Q}_{\mathrm{cyc},p})}{\langle Z_p \rangle} \to \mathfrak{X}(E/\mathbb{Q}_{\mathrm{cyc}}) \to \mathfrak{Y}(E/\mathbb{Q}_{\mathrm{cyc}}) \to 0. \tag{6.10}$$

Here, $\mathcal{Z}^1(E/\mathbb{Q}_{\mathrm{cyc}})$ is the compact Iwasawa cohomology group and $\mathcal{Z}^1_p(E/\mathbb{Q}_{\mathrm{cyc},p})$ is the local Iwasawa cohomology group which can be defined analogously. We denote by $\langle Z \rangle$ the submodule generated by the Euler system Z constructed by Kato. It is a free $\Lambda(\Gamma)$-module inside $\mathcal{Z}^1(E/\mathbb{Q}_{\mathrm{cyc}})$. Under the natural functorial map, the image of $\langle Z \rangle$ generates a submodule of the local Iwasawa cohomology group, denoted by $\langle Z_p \rangle$.

The Coleman isomorphism interpolates the (dual) Bloch-Kato exponential maps. This isomorphism, yields the following identification

$$\mathrm{Col}:\ \mathcal{Z}^1_p\left(E/\mathbb{Q}_{\mathrm{cyc},p}\right) \simeq \Lambda(\Gamma).$$

It was further shown by Kato that the image $\mathrm{Col}(Z_p)$ is precisely the p-adic L-function that appears in the statement of the Main Conjecture.

The philosophy in proving the Main Conjecture is to show that the first and the last term of the

Exact Sequence 6.10 have the same characteristic power series. Since the characteristic power series is multiplicative in exact sequences, this forces the second and the third term to have the same characteristic power series which is precisely the statement of the Main Conjecture.

In a large number of examples considered in the earlier sections, $\mathfrak{X}(E/\mathbb{Q}_{\text{cyc}})$ was trivial. This yields the isomorphism

$$\frac{\mathcal{Z}^1(E/\mathbb{Q}_{\text{cyc}})}{\langle Z\rangle} \simeq \frac{\mathcal{Z}^1_p(E/\mathbb{Q}_{\text{cyc},p})}{\langle Z_p\rangle}.$$

If the Main Conjecture holds, the triviality of the dual fine Selmer group implies that the first term is pseudo-null (equivalently finite in a $\mathbb{Z}_p$-extension). But we know that the second term of the Exact Sequence 6.10 is of projective dimension 1, so it has no non-zero finite submodules. Thus, the first term is trivial. This shows that if the dual Selmer group is trivial over the cyclotomic extension, all terms in the exact sequence 6.10 are trivial. In particular, the Euler system generates $\mathcal{Z}^1(E/\mathbb{Q}_{\text{cyc}})$.

More generally, consider a p-adic Lie extension $\mathcal{L}/\mathbb{Q}$ of dimension at least 2. We obtain a short exact sequence similar to the one above

$$0 \to \frac{\mathcal{Z}^1(E/\mathcal{L})}{\langle Z\rangle} \to \frac{\mathcal{Z}^1_p(E/\mathcal{L}_p)}{\langle Z_p\rangle} \to \mathfrak{X}(E/\mathcal{L}) \to \mathfrak{Y}(E/\mathcal{L}) \to 0, \tag{6.11}$$

where $\mathcal{L}_p$ is the localization of $\mathcal{L}$ at p and the other terms are defined as before. We note that in this full generality, existence of the Euler system Z is still conjectural. However, they have been constructed in some special cases and the validity of the Main Conjecture has been verified, see [81], [88], [99].

Let $E/\mathbb{Q}$ be an elliptic curve. If the Main Conjecture is valid over $\mathbb{Q}(E_{p^\infty})$ and Conjecture B holds for $\mathfrak{Y}\left(E/\mathbb{Q}\left(E_{p^\infty}\right)\right)$, then by the same argument as before we have that $\frac{\mathcal{Z}^1\left(E/\mathbb{Q}\left(E_{p^\infty}\right)\right)}{\langle Z\rangle}$ must be pseudo-null and therefore trivial.

Appendix A

Appendix

A.1 Nakayama's's Lemma

Informally, the Nakayama Lemma gives a precise sense in which finitely generated modules over a commutative ring behave like vector spaces over a field. It is important as it allows modules over local rings to be studied point-wise as vector spaces over the residue field of the ring.

A.1.1 Commutative Case

Lemma A.1.1 (Nakayama's Lemma)**.** *Let M be a compact $\Lambda(\Gamma)$-module and $\mathfrak{m}$ be the unique maximal ideal of $\Lambda(\Gamma)$. The following are equivalent*

(i) M is finitely generated over $\Lambda(\Gamma)$.

(ii) M/TM is a finitely generated $\mathbb{Z}_p$-module.

(iii) $M/\mathfrak{m}$ is a finitely generated $\mathbb{F}_p$-vector space.

Proof. (i) ⇒ (ii) ⇒ (iii). We now show (iii) ⇒ (i).
Consider a set of generators $\{x_1, \dots x_n\}$ of $M/\mathfrak{m}M$ as an $\mathbb{F}_p$-vector space. Define
$N = \Lambda(\Gamma)x_1 + \dots + \Lambda(\Gamma)x_n \subseteq M$; it is compact and hence closed. Thus M/N is also compact. By assumption $N + \mathfrak{m}M = M$. Thus

$$\left.{}^{M}\middle/_{N}\right. = \left.{}^{N+\mathfrak{m}M}\middle/_{N}\right. = \mathfrak{m}\left.{}^{M}\middle/_{N}\right..$$

Therefore,

$$\left.{}^{M}\middle/_{N}\right. = \mathfrak{m}^n \left.{}^{M}\middle/_{N}\right. \qquad \text{for all } n > 0.$$

Consider a small neighbourhood U around 0 in M/N. Since $\mathfrak{m}^n \to 0$ in $\Lambda(\Gamma)$, for any $z \in M/N$, there is a neighbourhood U_z around z and some integer n_z such that $\mathfrak{m}^{n_z} U_z \subseteq U$. But by compactness of M/N, $\mathfrak{m}^k M/N \subseteq U$ for all k sufficiently large. Thus

$$\left.{}^{M}\middle/_{N}\right. = \bigcap \mathfrak{m}^k \left.{}^{M}\middle/_{N}\right. = 0.$$

It follows $M = N$ is finitely generated over $\Lambda(\Gamma)$. ☕

The following theorem is a straightforward application of the Nakayama's Lemma.

Theorem A.1.2. *Let M be an Abelian pro-p group on which Γ acts continuously. Regard M as a $\Lambda(\Gamma)$-module. Then*

(i) $M = 0 \Leftrightarrow M/TM = 0 \Leftrightarrow M/\mathfrak{m}M = 0.$

(ii) For a finitely generated $\Lambda(\Gamma)$-module M, the minimal number of generators of M is $\dim_{\mathbb{F}_p}\left(M/\mathfrak{m}M\right)$

(iii) If M/TM is finite, then M is $\Lambda(\Gamma)$-torsion.

Proof. The first two statements are rephrasing of the Nakayama's Lemma. However, we give a different proof of (i) which can be imitated as is in the non-commutative case.

(i) By hypothesis, $M = \mathrm{Hom}\left(A,\ \mathbb{Q}_p/\mathbb{Z}_p\right)$ where A is a discrete p-primary Abelian group. M/TM is dual to A^Γ. We need to show $A^\Gamma = 0$ if and only if $A = 0$. When $A = 0$, there is nothing to show. Suppose $A^\Gamma = 0$ but $A \neq 0$. Since A is a discrete Γ-module, there exists an open normal subgroup U of Γ such that $A^U \neq 0$. Therefore, there exists a non-zero finite Γ-module B of A^U. On the other hand, $A^\Gamma = 0$ so $B^{\Gamma/U} = 0$; Γ/U is a finite p-group so $B = 0$. This gives the desired contradiction.

(ii) Rephrasing of the Nakayama's Lemma.

(iii) Assume M/TM is finite; the same is true for $M/\mathfrak{m}M$. Thus, M is a finitely generated $\Lambda(\Gamma)$-module with generators $\{x_1 \ldots, x_n\}$. If M/TM has exponent p^k, $p^k x_i \in TM$ for $1 \leq i \leq n$. Write

$$p^k x_i = \sum_{i=1}^{n} T\alpha_{ij}(T)x_j \qquad 1 \leq i \leq n,$$

with $\alpha_{ij}(T) \in \Lambda(\Gamma)$. For each i, this can be rewritten as

$$\sum_{j=1}^{n}\left(p^k\delta_{ij} - T\alpha_{ij}(T)\right)x_j = 0 \tag{A.1}$$

Consider the $n \times n$ matrix $[p^k\delta_{ij} - T\alpha_{ij}(T)]$ and A^* be its adjoint matrix. $A^*A = \det(A)I_n$. Set $f(T) = \det(A)$; $f(T)$ is a non zero element of $\Lambda(\Gamma)$ as $f(0) = p^{nk}$. From Equation A.1, we see that for each i, $f(T)x_i = 0$; hence it annihilates M.

☕

A.1.2 Non-Commutative Case

There are unexpected subtleties in the question of giving a sufficient condition for a compact left $\Lambda(G)$-module M to be finitely generated when G is any arbitrary profinite group [1]. These difficulties can be avoided when M is itself profinite; fortunately this is the case we care about.

Define the augmentation ideal $I(G)$ of $\Lambda(G)$ by

$$I(G) = \ker\left(\Lambda(G) \to \mathbb{Z}_p\right).$$

Theorem A.1.3 (Nakayama's Lemma)**.** *Assume G is a pro-p group and M is a pro-p Abelian group which is a left $\Lambda(G)$-module.*

1. *$M = 0$ if and only if $M/I(G)M = 0$.*

2. *If $M/I(G)M$ is a finitely generated $\mathbb{Z}_p$-module, then M is a finitely generated $\Lambda(G)$-module.*

Remark A.1.4. In [1], Balister and Howson show that the analogue of Theorem A.1.2(iii) breaks down when G is any pro-p open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$.

A.2 Fundamental Diagram

Let A be an Abelian variety defined over the number field F. Consider an infinite Galois extension $\mathcal{L}/F$ such that $G = \mathrm{Gal}(\mathcal{L}/F)$ is a p-adic Lie group with $\dim(G) \geq 1$. The following **Fundamental Diagram** plays a key role in studying the $\Lambda(G)$-module $\mathfrak{X}(A/\mathcal{L})$ (i.e. the Pontryagin dual of $\mathrm{Sel}(A/\mathcal{L})$).

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}(A/\mathcal{L})^G \arrow[r] & H^1(G_S(\mathcal{L}), A[p^\infty])^G \arrow[r] & \bigoplus_{v\in S} \varprojlim \left(\oplus_{w|v} H^1(L_w, A)(p)\right)^G \\
0 \arrow[r] & \mathrm{Sel}(A/F) \arrow[r] \arrow[u, "\alpha"] & H^1(G_S(F), A[p^\infty]) \arrow[r] \arrow[u, "\beta"] & \bigoplus_{v\in S} H^1(F_v, E)(p) \arrow[u, "\gamma"]
\end{tikzcd}$$

A.3 Facts About p-Cohomological Dimension

Definition A.3.1. *[94] Let p be any prime and G be a profinite group. The p-**cohomological dimension** $\mathrm{cd}_p(G)$, is the lower bound of the integers n satisfying the following condition:*

For every discrete torsion G-module A, and for every $q > n$, the p-primary component of $H^q(G, A)$ is null.

Proposition A.3.2. *[94, Section 3.1, Proposition 11]. Let G be a profinite group, p be a prime and let n be an integer. The following properties are equivalent*

(i) $\mathrm{cd}_p(G) \leq n$.

(ii) $H^q(G, A) = 0$ for all $q > n$ and every discrete G-module A which is a p-primary torsion group.

(iii) $H^{n+1}(G, A) = 0$ when A is a simple discrete G-module killed by p.

Proof. Let A be a torsion G-module. Write $A = \bigoplus A(p)$. It is known that

$$H^q\left(G,\ A(p)\right) = H^q\left(G,\ A\right)(p).$$

The equivalence of the first two statements follows from the above equality. Statement (ii) implies (iii).

Recall the following well-known fact. For a discrete G-module A,

$$H^q(G, A) = \varinjlim H^q(G, B) \qquad \text{for all } q \geq 0$$

where B runs over the set of finitely generated sub-G-modules of A.

Suppose (iii) holds. By a *dévissage* argument, $H^{n+1}(G, A) = 0$ if A is finite and annihilated by a power of p. The same result is now extended to every discrete G-module A which is a p-primary torsion group, by taking the inductive limit. To obtain (ii), use induction on q: imbed A in the induced module $M_G(A)$; apply induction hypothesis to the p-primary torsion module ${M_G(A)}\big/{A}$. ☕

Corollary A.3.3. *Let G be a pro-p group and n be any integer. For $\mathrm{cd}_p(G) \leq n$ it is necessary and sufficient that $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$.*

Proof. This follows from the above proposition upon observing that every simple discrete G-module killed by p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. ☕

Proposition A.3.4. *[94, Section 3.3, Proposition 14] Let H be a closed subgroup of the profinite group G. Then*

$$\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G) = n.$$

Equality holds in each of the following cases,

(i) $[G : H]$ is of index prime to p.

(ii) H is open in G and $\mathrm{cd}_p(G)$ is finite.

Notation: Let G be a profinite group with a closed subgroup H. Let A be an Abelian group on which H acts continuously. The **induced module** $A^* = M_G^H(A)$ is the group of continuous maps a^* from G to A such that

$$a^*(hx) = h \cdot a^*(x) \qquad \text{for } h \in H,\ x \in G.$$

Sketch of Proof. Suppose A is a discrete torsion H-module, then the induced module is a discrete torsion G-module. By Shapiro's Lemma

$$H^q\left(G,\ M_G^H(A)\right) \simeq H^q(H,\ A).$$

The first inequality follows. For the reverse inequalities we use,

(i) the restriction map

$$H^q(G,\ A)(p) \xrightarrow{res} H^q(H,\ A)(p)$$

is injective on p-primary components.

(ii) the corestriction map

$$H^n(H,\ A)(p) \xrightarrow{cor} H^n(G,\ A)(p)$$

is surjective on the p-primary components.

☕

Proposition A.3.5. *Let H be a closed normal subgroup of the profinite group G. Then*

$$\mathrm{cd}_p(G) \leq \mathrm{cd}_p(H) + \mathrm{cd}_p(G/H).$$

Proof. Suppose $\mathrm{cd}_p(G/H) = m$ and $\mathrm{cd}_p(H) = n$. Let M be a p-primary torsion G-module. Consider the Hochschild-Serre spectral sequence

$$E_2^{i,j} + H^i\left(G/H,\ H^j(H,\ M)\right) \Rightarrow H^{i+j}(G,\ M).$$

If $i + j = q > m + n$, then either $i > m$ or $j > n$. Thus $E_2^{i,j} = 0$. $H^q(G, M)$ has a filtration whose quotients are subquotients of $E_2^{i,j}$. So $H^q(G, M) = 0$. This finishes the proof. ☕

Index

Bibliography

[1] PN Balister and Susan Howson. Note on Nakayama's lemma for compact Λ-modules. *Asian J. Math.*, 1(2):224–229, 1997.

[2] Andrea Bandini. Greenberg's conjecture and capitulation in $\mathbb{Z}_p^d$-extensions. *J. Number Theory*, 122(1):121–134, 2007.

[3] Razvan Barbulescu and Jishnu Ray. Some remarks and experiments on Greenberg's p-rationality conjecture. *arXiv preprint arXiv:1706.04847*, 2017.

[4] Massimo Bertolini. Iwasawa theory for elliptic curves over imaginary quadratic fields. *J. Théor. Nombres Bordeaux*, 13(1):1–25, 2001.

[5] FM Bleher, T Chinburg, R Greenberg, M Kakde, G Pappas, R Sharifi, and MJ Taylor. Higher Chern classes in Iwasawa theory. *arXiv preprint arXiv:1512.00273*, 2015.

[6] John R Bloom and Frank Gerth III. The Iwasawa invariant μ in the composite of two $\mathbb{Z}_\ell$-extensions. *J. Number Theory*, 13(2):262–267, 1981.

[7] Armand Borel, Sarvadaman Chowla, Carl S Herz, Kenkichi Iwasawa, and Jean Pierre Serre. *Seminar on Complex Multiplication: Seminar Held at the Institute for Advanced Study, Princeton, NY, 1957-58*, volume 21. Springer, 1966.

[8] Nigel Boston. Some cases of the Fontaine-Mazur conjecture. *J. Number Theory*, 42(3):285–291, 1992.

[9] Winfried Bruns and Jürgen Herzog. Cohen–Macaulay rings. *Adv. Math*, 39, 1993.

[10] David Burns. On main conjectures in non-commutative Iwasawa theory and related conjectures. *J. Reine Angew. Math.*, 2015(698):105–159, 2015.

[11] Kęstutis Česnavičius. Selmer groups and class groups. *Comp. Math.*, 151(3):416–434, 2015.

[12] Kęstutis Česnavičius. p–Selmer growth in extensions of degree p. *J. London Math. Soc.*, 95(3):833–852, 2017.

[13] Claude Chevalley. Sur la théorie du corps de classes dans les corps finis et les corps locaux. 1934.

[14] Pete L Clark and Shahed Sharif. Period, index and potential Sha. *Algebra & Number Theory*, 4(2):151–174, 2010.

[15] John Coates. Infinite descent on elliptic curves with complex multiplication. In *Arithmetic and geometry*, pages 107–137. Springer, 1983.

[16] John Coates, Takako Fukaya, Kazuya Kato, Ramdorai Sujatha, and Otmar Venjakob. The GL_2 main conjecture for elliptic curves without complex multiplication. *Publications mathématiques de l'IHÉS*, 101(1):163–208, 2005.

[17] John Coates, Ralph Greenberg, Kenneth A Ribet, and Karl Rubin. *Arithmetic Theory of Elliptic Curves: Lectures given at the 3rd Session of the Centro Internazionale Matematico Estivo (CIME) held in Cetaro, Italy, July 12-19, 1997.* Springer, 1999.

[18] John Coates and Susan Howson. Euler characteristics and elliptic curves II. *J. Math. Soc. Japan*, 53(1):175–235, 2001.

[19] John Coates, Peter Schneider, and Ramdorai Sujatha. Modules over Iwasawa algebras. *Journal of the Institute of Mathematics of Jussieu*, 2(1):73–108, 2003.

[20] John Coates and Ramdorai Sujatha. *Galois cohomology of elliptic curves.* Narosa, 2000.

[21] John Coates and Ramdorai Sujatha. Fine Selmer groups for elliptic curves with complex multiplication. In *Algebra and Number Theory*, pages 327–337. Springer, 2005.

[22] John Coates and Ramdorai Sujatha. Fine Selmer groups of elliptic curves over p-adic Lie extensions. *Math. Annalen*, 331(4):809–839, 2005.

[23] John Coates, Ramdorai Sujatha, and Jean-Pierre Wintenberger. On the Euler-Poincaré characteristics of finite dimensional p-adic Galois representations. *Publications mathematiques de l'IHES*, 93:107–143, 2001.

[24] John Coates and Andrew Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[25] John Coates and Andrew Wiles. On p-adic L-functions and elliptic units. *J. Austral. Math. Soc.*, 26(1):1–25, 1978.

[26] Brendan Creutz. Potential Sha for abelian varieties. *J. Number Theory*, 131(11):2162–2174, 2011.

[27] Albert A Cuoco and Paul Monsky. Class numbers in $\mathbb{Z}_p^d$-extensions. *Math. Annalen*, 255(2):235–258, 1981.

[28] Ehud De Shalit. *Iwasawa theory of elliptic curves with complex multiplication.* Orlando, 1987.

[29] T Nguyen Quang Do and A Movahhedi. Sur l'arithmétique des corps de nombres p-rationnels. In *Séminaire de Théorie des Nombres, Paris 1987–88*, pages 155–200. Springer, 1990.

[30] Bruce Ferrero and Lawrence C Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. Math.*, pages 377–395, 1979.

[31] JM Fontaine and B Mazur. Geometric galois representations, in elliptic curves, modular forms and Fermat's last theorem, 1993.

[32] Roland Gillard. Fonctions L p-adiques des des corps quadratiques imaginaires et de leurs extensions abeli'ennes. *J. Reine Angew. Math.*, 358:76–91, 1985.

[33] Evgeniy Solomonovich Golod and Igor Rostislavovich Shafarevich. On the class field tower. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 28(2):261–272, 1964.

[34] Ralph Greenberg. The Iwasawa invariants of Γ-extensions of a fixed number field. *American Journal of Mathematics*, 95(1):204–214, 1973.

[35] Ralph Greenberg. Iwasawa theory—past and present. *Adv. Studies in Pure Math*, 30:335–385, 2001.

[36] Ralph Greenberg. *Iwasawa theory, projective modules, and modular representations.* American Math. Soc., 2010.

[37] Ralph Greenberg. Galois representations with open image. *Annales mathématiques du Québec*, 40(1):83–119, 2016.

[38] Ralph Greenberg et al. Iwasawa theory for p-adic representations. In *Algebraic Number Theory—in Honor of K. Iwasawa*, pages 97–137. Mathematical Society of Japan, 1989.

[39] Yoshitaka Hachimori and Kazuo Matsuno. An analogue of Kida's formula for the Selmer groups of elliptic curves. *J. Alg. Geom.*, 8:581–601, 1999.

[40] Yoshitaka Hachimori and Kazuo Matsuno. On finite Λ-submodules of Selmer groups of elliptic curves. *Proc. American Math Society*, pages 2539–2541, 2000.

[41] Farshid Hajir. On the growth of p-class groups in p-class field towers. *J. Algebra*, 188(1):256–271, 1997.

[42] Farshid Hajir and Christian Maire. Prime decomposition and the Iwasawa μ-invariant. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 166, pages 599–617. Cambridge University Press, 2019.

[43] Michael Harris. p-adic representations arising from descent on abelian varieties. *Comp. Math.*, 39(2):177–245, 1979.

[44] Susan Howson. Euler characteristics as invariants of Iwasawa modules. *Proc. London Math. Soc.*, 85(3):634–658, 2002.

[45] Hideo Imai. A remark on the rational points of Abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions. *Proc. Jap. Academy*, 51(1):12–16, 1975.

[46] Kenkichi Iwasawa. A note on class numbers of algebraic number fields. *Abh. Math. Sem. Univ. Hamburg*, 20:257–258, 1956.

[47] Kenkichi Iwasawa. On Γ-extensions of algebraic number fields. *Bull. Am. Math. Soc.*, 65(4):183–226, 1959.

[48] Kenkichi Iwasawa. On p-adic l-functions. *Ann. Math.*, pages 198–205, 1969.

[49] Kenkichi Iwasawa. On the μ-invariants of $\mathbb{Z}_\ell$-extensions, number theory. *Algebraic Geometry and Commutative Algebra*, pages 1–11, 1973.

[50] Kenkichi Iwasawa. On the μ-invariants of $\mathbb{Z}_\ell$-extensions, number theory. *Algebraic Geometry and Commutative Algebra*, pages 1–11, 1973.

[51] Kenkichi Iwasawa. Riemann-Hurwitz formula and p-adic Galois representations for number fields. *Tohoku Math. Journal, Second Series*, 33(2):263–288, 1981.

[52] Somnath Jha and Ramdorai Sujatha. On the Hida deformations of fine Selmer groups. *J. Algebra*, 338(1):180–196, 2011.

[53] Mahesh Kakde. Proof of the main conjecture of noncommutative Iwasawa theory for totally real number fields in certain cases. *J. Alg. Geometry*, 20(4):631–683, 2011.

[54] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.

[55] Yûji Kida. ℓ-extensions of CM-fields and cyclotomic invariants. *J. Number Theory*, 12:519–528, 1980.

[56] Sören Kleine. Relative extensions of number fields and Greenberg's generalised conjecture. *Acta Arithmetica*, 174:367–392, 2016.

[57] Arthur Lannuzel and Thong Nguyen Quan Do. Greenberg conjectures and pro-p-free extensions of a number field. *Manuscripta Mathematica*, 102(2):187–209, 2000.

[58] Franz Lemmermeyer. The ambiguous class number formula revisited. *J. Ramanujan Math. Soc*, 28:415–421, 2013.

[59] Meng Fai Lim and V Kumar Murty. Growth of Selmer groups of CM abelian varieties. *Canadian J. Math.*, 67(3):654–666, 2015.

[60] Meng Fai Lim and V Kumar Murty. The growth of fine Selmer groups. *J. Ramanujan Math. Society*, 31(1):79–94, 2016.

[61] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2013. [Online; accessed 29 September 2019].

[62] Alexander Lubotzky and Avinoam Mann. Powerful p-groups II p-adic analytic groups. *J. Algebra*, 105(2):506–515, 1987.

[63] Ahmed Matar. Selmer groups and generalized class field towers. *Int. J. Number Theory*, 8(04):881–909, 2012.

[64] Ahmed Matar. On the Λ-cotorsion subgroup of the Selmer group. *Asian J. Math.*, to appear.

[65] Kazuo Matsuno. An analogue of Kida's formula for the p-adic L-functions of modular elliptic curves. *J. Number Theory*, 84(1):80–92, 2000.

[66] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18(3-4):183–266, 1972.

[67] Barry Mazur and Karl Rubin. Ranks of twists of elliptic curves and Hilbert's tenth problem. *Invent. Math.*, 181(3):541–575, 2010.

[68] Barry Mazur and Andrew Wiles. Class fields of abelian extensions of $\mathbb{Q}$. *Invent. Math.*, 76(2):179–330, 1984.

[69] William G McCallum. Greenberg's conjecture and units in multiple p-extensions. *American Journal of Mathematics*, 123(5):909–930, 2001.

[70] Gary McConnell. On the iwasawa theory of cm elliptic curves at supersingular primes. *Comp. Math*, 101(1):1–19, 1996.

[71] P Monsky. Fine estimates for the growth of e_n in $\mathbb{Z}_p^d$-extensions. In *Algebraic Number Theory—in honor of K. Iwasawa*, pages 309–330. Mathematical Society of Japan, 1989.

[72] Paul Monsky. The Hilbert-Kunz function. *Math. Annalen*, 263(1):43–49, 1983.

[73] Paul Monsky. p-ranks of class groups in $\mathbb{Z}_p^d$-extensions. *Math. Annalen*, 263(4):509–514, 1983.

[74] V Kumar Murty. Modular forms and the Chebotarev density theorem II. *London Mathematical Society Lecture Note Series*, pages 287–308, 1997.

[75] V Kumar Murty and Yi Ouyang. The growth of selmer ranks of an abelian variety with complex multiplication. *Pure and Applied Mathematics Quarterly*, 2(2):539–555, 2006.

[76] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323. Springer, 2013.

[77] Yoshihiro Ochi and Otmar Venjakob. On the structure of Selmer groups over p-adic Lie extensions. *J. Alg. Geom.*, 11(3):547–580, 2002.

[78] Yoshihiro Ochi and Otmar Venjakob. On the ranks of Iwasawa modules over p-adic Lie extensions. In *Math. Proc. Camb. Philos. Soc*, volume 135, pages 25–43. Cambridge University Press, 2003.

[79] Bernadette Perrin-Riou. Groupe de Selmer d'une courbe elliptique à multiplication complexe. *Comp. Math.*, 43(3):387–417, 1981.

[80] Bernadette Perrin-Riou. Arithmétique des courbes elliptiques et théorie d'Iwasawa. *Mémoires de la société mathématique de France*, 17:1–130, 1984.

[81] Robert Pollack and Karl Rubin. The main conjecture for CM elliptic curves at supersingular primes. *Ann. Math.*, pages 447–464, 2004.

[82] Robert Pollack and Tom Weston. Kida's formula and congruences. *Documenta Mathematica, Special*, 2006:615–630, 2006.

[83] Ken Ribet. Torsion points of abelian varieties in cyclotomic extensions (appendix to an article of Nicholas Katz and Serge Lang). *Enseign. Math*, 27(3-4):285–319, 1981.

[84] Jürgen Ritter and Alfred Weiss. On the "main conjecture" of equivariant Iwasawa theory. *Journal of the American Mathematical Society*, 24(4):1015–1050, 2011.

[85] Karl Rubin. Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. *Inventiones mathematicae*, 64(3):455–470, 1981.

[86] Karl Rubin. On the main conjecture of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 93(3):701–713, 1988.

[87] Karl Rubin. Tate–Shafarevich groups of elliptic curves with complex multiplication. In *Algebraic Number Theory—in honor of K. Iwasawa*, pages 409–419. Mathematical Society of Japan, 1989.

[88] Karl Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.

[89] Karl Rubin. *Euler Systems.(AM-147)*, volume 147. Princeton University Press, 2014.

[90] Leila Schneps. On the μ-invariant of p-adic l-functions attached to elliptic curves with complex multiplication. *J. Number Theory*, 25(1):20–33, 1987.

[91] René Schoof. Infinite class field towers of quadratic fields. *Journal für die reine und angewandte Mathematik*, 372, 1986.

[92] Jean-Pierre Serre. *Local fields*, volume 67. Springer, 1979.

[93] Jean-Pierre Serre. *Local algebra.* Springer, 2012.

[94] Jean-Pierre Serre. *Galois cohomology.* Springer, 2013.

[95] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math.(2)*, 88(492-517):2, 1968.

[96] Sudhanshu Shekhar. Comparing the corank of fine Selmer group and Selmer group of elliptic curves. *Journal of the Ramanujan Mathematical Society*, 33(2):205–217, 2018.

[97] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[98] Warren Sinnott. On the μ-invariant of the Γ-transform of a rational function. *Invent. math.*, 75(2):273–282, 1984.

[99] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[100] R Sujatha and M Witte. Fine Selmer groups and isogeny invariance. In *Conference on Geometry, Algebra, Number Theory, and their Information Technology Applications*, pages 419–444. Springer, 2016.

[101] Ramdorai Sujatha. Elliptic curves and Iwasawa's μ= 0 conjecture. In *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, pages 125–135. Springer, 2010.

[102] Otmar Venjakob. On the structure theory of the Iwasawa algebra of a p-adic Lie group. *Journal of the European Mathematical Society*, 4(3):271–311, 2002.

[103] Otmar Venjakob. On the Iwasawa theory of p-adic Lie extensions. *Compositio Mathematica*, 138(1):1–54, 2003.

[104] Otmar Venjakob and Denis Vogel. A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory. *J. Reine Angew. Math.*, pages 153–192, 2003.

[105] Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer, 1997.

[106] Christian Wuthrich. *The fine Selmer group and height pairings.* PhD thesis, University of Cambridge, 2004.

[107] Christian Wuthrich. The fine Tate–Shafarevich group. In *Math. Proc. Camb. Philos. Soc.*, volume 142, pages 1–12. Cambridge University Press, 2007.