ABSTRACT

Title of dissertation: ON THE CYCLOTOMIC IWASAWA INVARIANTS OF ELLIPTIC CURVES

Foivos Chnaras, Doctor of Philosophy, 2026

Dissertation directed by: Professor Niranjan Ramachandran
University of Maryland

Iwasawa theory began with investigations into the Galois module structure of ideal class groups, originally developed by Kenkichi Iwasawa within the framework of cyclotomic fields. In the early 1970s, Barry Mazur broadened this perspective by applying Iwasawa theory to the Selmer groups of elliptic curves—and more generally, abelian varieties—at good ordinary primes. Later, Perrin-Riou, along with Pollack and Kobayashi, extended these ideas to the realm of supersingular primes. The resulting Iwasawa invariants offer deep insights into the arithmetic properties of these structures.

This thesis is dedicated to examining these invariants. In particular, it seeks to establish arithmetic criteria that guarantee the minimal possible values of the Iwasawa invariants. While Gold's criterion addresses this issue in the classical context of Iwasawa theory, our goal is to develop an analogous criterion for elliptic curves of rank one.

Furthermore, numerical evidence indicates that for a set of primes of density one, the Iwasawa invariants for rank-one elliptic curves achieve their smallest conceivable values. This work provides additional support for that conjecture.

ON THE CYCLOTOMIC IWASAWA INVARIANTS OF ELLIPTIC CURVES

by

Foivos Chnaras

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2026

Advisory Committee:
Professor Niranjan Ramachandran, Chair/Advisor
Professor Lawrence Washington, Co-Advisor
Professor Thomas Haines
Professor Dori Bejleri

Acknowledgments

I would like to thank my parents for their continued love, support, and belief in me. It is only through their sacrifices that I was even able to pursue my education.

Thank you to my advisors, Dr. Niranjan Ramachandran and Dr. Lawrence Washington, for their guidance and support throughout my time at the University of Maryland. I am grateful for their patience and encouragement, and for the many hours they spent helping me develop my ideas and refine my work.

Thank you to all of my students who made teaching such an enjoyable experience.

Most importantly, I would like to thank my sister for being the person I look up to the most.

Table of Contents

Chapter 1: Introduction

1.1 Fermat

Diophantus' Arithmetica is one of the great classics of Greek mathematics. Rediscovered and translated into Latin in the early 1600s, a copy eventually reached the hands of Samuel Fermat. The book had belonged to his father, Pierre Fermat, a jurist whose marginal notes would change the course of number theory. Next to Problem 8 of Book II—"Given a square number, write it as the sum of two other squares"—Pierre Fermat scribbled:

> On the other hand, it is impossible to write a cube as the sum of two cubes, or a fourth power as the sum of two fourth powers, or in general any power beyond the second as the sum of two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.

This was the beginning of *Fermat's Last Theorem*.

1.2 Kummer

Over the centuries many eminent mathematicians—Gauss, Lamé, Cauchy, Wantzel, and others—announced proofs of Fermat's assertion. Lamé's 1847 argument, in particular, relied on the then-novel idea of working in the ring $\mathbb{Z}[\zeta]$, where

$$x^n + y^n = (x+y)(x+\zeta y)\cdots(x+\zeta^{n-1}y), \qquad \zeta := e^{2\pi i/n}.$$

Since the factors on the right are pairwise coprime, Lamé claimed, then any solution $x^n + y^n = z^n$ would force each factor to be an n-th power, leading to a clever impossible infinite descent.

Three years earlier, however, Ernst Kummer had already noticed the flaw: unique factorisation can fail in $\mathbb{Z}[\zeta]$. For $p = 37$ he produced explicit counter-examples. To repair the argument he introduced "ideal complex numbers"—what we now call *ideals*—and showed that unique factorisation holds in $\mathbb{Z}[\zeta_p]$ precisely when the p-part of the ideal class group is trivial.

This was the beginning of algebraic number theory.

1.3 Iwasawa

In the 1950s Kenkichi Iwasawa pushed Kummer's ideas further. Instead of studying a single cyclotomic field, he considered the entire cyclotomic $\mathbb{Z}_p$-extension of a number field

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots, \qquad [K_n : K] = p^n$$

and analysed how the p-part of the class group grows with n. He proved the striking formula

$$\#\mathrm{Cl}(K_n)(p) = p^{\mu p^n + \lambda n + \nu},$$

where the *Iwasawa invariants* μ, λ, ν depend only on the base field K and the prime p. Even more remarkably, he observed that the characteristic polynomial governing this growth appears to coincide with the p-adic L-function of Kubota and Leopoldt—a prediction now known as the **Iwasawa Main Conjecture**.

For the cyclotomic extension of an abelian field, Ferrero–Washington proved that $\mu = 0$. Greenberg conjectured that $\lambda = 0$ for totally real fields. Consequently, the first place one

expects *non-trivial* Iwasawa invariants is an imaginary quadratic field. Iwasawa showed that if p does *not* split in K and $p \nmid h_K$, then $\mu_p(K) = \lambda_p(K) = 0$, whereas if p splits, one always has $\mu_p(K) + \lambda_p(K) \geq 1$. Gold [Gol74] supplied an explicit numerical criterion that decides when equality holds.

In recent decades Iwasawa theory has been extended far beyond class groups—to Selmer groups of elliptic curves and even to general motives. Understanding the similarities and contrasts among these settings is an active area of research. One natural such question is whether Gold-type criteria exist for Selmer groups of elliptic curves.
This was the beginning of this thesis.

The main goal of this thesis is to develop an analog of Gold's criterion for elliptic curves over $\mathbb{Q}$, at primes of both ordinary and supersingular reduction. In particular, we establish a numerical criterion that determines when the Iwasawa invariants attain their minimal possible values. This requires a detailed study of the theory of p-adic heights. In the supersingular case, the analysis becomes more intricate, as the p-adic Birch and Swinnerton-Dyer conjecture is formulated in terms of Dieudonné modules. This discussion culminates in the main results of the thesis: Theorem 4.4 and Theorem 5.1. Finally, the thesis is complemented by computations carried out in SageMath, which provide evidence supporting the heuristic models developed throughout.

1.4 Overview of the Thesis

Chapter 2 Background. We review the basic definitions of Iwasawa theory, cyclotomic $\mathbb{Z}_p$-extensions, the structure of Λ-modules, and Selmer groups of elliptic curves.

Chapter 3 Gold's Criterion. We present several equivalent formulations of Gold's criterion for imaginary quadratic fields, its proofs via genus theory, Federer–Gross, and modern cohomological approaches, and we survey computational evidence.

Chapter 4 Ordinary Primes. We develop the p-adic height, regulator, and Iwasawa invariants for elliptic curves with good ordinary reduction, culminating in an analogue of Gold's criterion (our Theorem 4.4).

Chapter 5 Supersingular Primes. After reviewing Dieudonné modules, signed Selmer groups, and Pollack's signed p-adic L-functions, we prove a supersingular analogue of Gold's criterion (Theorem 5.1) and relate it to generalized Wieferich primes.

Chapter 6 Local Index for Non-Minimal Models. We analyse how the local index $[E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$ changes under different Weierstrass models, derive a global constant C_E such that $C_E P \in E^0(\mathbb{Q})$ for all $P \in E(\mathbb{Q})$, and give an algorithm for finding smaller, point-specific multiples.

Chapter 7 We discuss possible directions for future research.

Chapter 2: Background

In this chapter, we give a brief overview of the main definitions and results in Iwasawa theory. We focus on the cyclotomic $\mathbb{Z}_p$-extension over a number field K and discuss the Iwasawa theory of class groups and elliptic curves. For the class group case, a good reference is [Was82] and for the elliptic curve case [Gre99].

2.1 Iwasawa modules

Fix a prime p and consider the cyclotomic extension $\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}$. By Galois theory, we have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \oplus \mathbb{Z}/p^n\mathbb{Z}.$$

There is a unique subfield $\mathbb{Q} \subset \mathbb{Q}_n \subset \mathbb{Q}(\zeta_{p^{n+1}})$ such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Repeating this process for every n yields an infinite tower

$$\mathbb{Q} = \mathbb{Q}_0 \subset \mathbb{Q}_1 \subset \cdots \subset \mathbb{Q}_n \subset \cdots \subset \mathbb{Q}_\infty = \bigcup_n \mathbb{Q}_n,$$

called the **cyclotomic** $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Notice that $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$ and $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. For a number field K, the compositum $K_\infty := K\mathbb{Q}_\infty$ defines the cyclotomic $\mathbb{Z}_p$-extension of K.

A $\mathbb{Z}_p$-extension of a number field K in general refers to a tower

$$K \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \bigcup K_n$$

such that $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$. We denote $\Gamma = \mathrm{Gal}(K_\infty/K)$ and $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$. Note that $K_n = K_\infty^{\Gamma_n}$.

Conjecture 2.1 (Leopoldt)**.** *Let K be a number field and p a prime number. Then the number of independent $\mathbb{Z}_p$-extensions of K is exactly $1 + r_2$, where r_2 is the number of pairs of complex embeddings of K.*

Leopoldt's conjecture is known to hold for abelian number fields. In particular, for $K = \mathbb{Q}$, the cyclotomic $\mathbb{Z}_p$-extension is the unique one.

Definition 2.1. *Let G be a profinite group. The Iwasawa algebra is defined as*

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

where the inverse limit is taken over all open normal subgroups H of G, with respect to the natural projection maps.

When $G := \Gamma = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, the Iwasawa algebra has a particularly nice structure:

Theorem 2.1. *Let K be a number field and K_∞/K a $\mathbb{Z}_p$-extension with $\Gamma = \mathrm{Gal}(K_\infty/K)$. Fix a topological generator γ of Γ. Then there is an isomorphism*

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

In particular, we list some useful properties of this Iwasawa algebra:

1. It is Noetherian.

2. It is a local ring with maximal ideal $\mathfrak{m} = (p, T)$. If $f(T) = \sum_i a_i T^i \in \Lambda(\Gamma)$, then $f(T)$ is invertible if and only if $a_0 \in \mathbb{Z}_p^\times$.

In Iwasawa theory, we are interested in finitely generated modules over the Iwasawa algebra. It turns out that their structure resembles that of finitely generated modules over a PID. We begin with the following definition:

Definition 2.2. *Two Λ-modules M and N are said to be **pseudo-isomorphic**, written*

$$M \sim N,$$

if there is a homomorphism $M \to N$ with finite kernel and cokernel.

We remark that this is not an equivalence relation in general. In particular, if $M \sim N$, it does not necessarily imply $N \sim M$ (it does when M, N are finitely generated).

Theorem 2.2 (Structure theorem for finitely generated Λ-modules)**.** *Let M be a finitely generated $\Lambda(\Gamma)$-module. Then*

$$M \sim \Lambda(\Gamma)^r \oplus \left(\bigoplus_{i=1}^{t} \Lambda(\Gamma)/p^{n_i} \right) \oplus \left(\bigoplus_{j=1}^{s} \Lambda(\Gamma)/f_j^{m_j} \right),$$

where the f_j are irreducible distinguished polynomials in $\mathbb{Z}_p[[T]]$.

Based on the above theorem, we make the following definitions:

Definition 2.3. *The constant r is called the **rank** of M.*
*If $r = 0$, we say that M is a **torsion** Λ-module. In that case, we define:*

1. $\mu(M) := \sum_{i=1}^{t} n_i$

2. $\lambda(M) := \sum_{j=1}^{s} m_j \deg(f_j)$

3. *Write* $f_M(T) = p^{\mu} \prod f_j^{m_j}(T)$ *for the* ***characteristic polynomial*** *of* M. *The ideal* $(f_M(T))$ *is called the* ***characteristic ideal*** *of* M.

Remark 2.1. *In practice, the characteristic polynomial of a finitely generated torsion* Λ*-module is given in the form of a power series* $f(T) \in \mathbb{Z}_p[[T]]$. *In theory, one can decompose* $f(T)$ *in its distinguished polynomials using the Weierstrass preparation theorem, but for computing the Iwasawa invariants, there's no need for it; we can directly compute them from the power series as follows:*

$$\mu_p(f) = \max\{n : p^n | f(T)\}$$

Write $\frac{1}{p^{\mu_p(f)}} f(T) = \sum_{i=0}^{\infty} c_i T_i \in \mathbb{Z}_p[[T]]$. *Then*

$$\lambda_p(f) = \min\{n : c_n \in \mathbb{Z}_p^{\times}\}$$

It's easy to check using the Weierstrass Preparation Theorem that this is equivalent to the Definition 2.3.

Example 2.1. *Before we move on, it's worthwhile to see an example in practice.*

$$\begin{aligned} f(T) = 5 + 4\cdot 5^2 + 4\cdot 5^3 + O(5^5) + \left(4\cdot 5 + O(5^2)\right) T \\ + \left(5 + O(5^2)\right) T^2 + \left(4\cdot 5 + O(5^2)\right) T^3 \\ + \left(3\cdot 5 + O(5^2)\right) T^4 + O(T^5). \end{aligned}$$

$$\frac{1}{5}f(T) = 1 + 4\cdot 5 + 4\cdot 5^2 + O(5^4) + (4+O(5))\,T + (1+O(5))\,T^2 + (4+O(5))\,T^3 + (3+O(5))\,T^4 + O(T^5).$$

This means that $\mu_p(f) = 1$ *and* $\lambda_p(f) = 0$

The following remark is going to be used extensively in this thesis

Remark 2.2. *If* $f(T) = T^r g(T)$ *then* $g(0) \in \mathbb{Z}_p^\times \iff \mu_p(f) = 0$ *and* $\lambda_p(f) = r$

We finish with a collection of important results that are direct consequences of Nakayama's Lemma:

Theorem 2.3 (Nakayama's Lemma)**.** *Let* X *be a finitely generated* Λ*-module. Then:*

1. $X = 0 \iff X/TX = 0 \iff X/\mathfrak{m}X = 0$
2. *If* X *is finitely generated, then* $X/\mathfrak{m}X$ *is a finite-dimensional* $\mathbb{F}_p$*-vector space. In that case,* $\dim_{\mathbb{F}_p} X/\mathfrak{m}X$ *equals the minimum number of* Λ*-generators of* X*, which we denote by* $g_p(X)$*.*
3. *If* X/TX *is finite, then* X *is a torsion* Λ*-module.*

2.2 Iwasawa theory of class groups

In this section, we discuss the Iwasawa theory of class groups, focusing on the cyclotomic $\mathbb{Z}_p$-extension of a number field K. We also introduce the Iwasawa invariants and their relation to the growth of the class group in the cyclotomic $\mathbb{Z}_p$-extension.

Fix a number field K and a prime number p. Let $A := A_K := \mathrm{Cl}(K)_p$, the p-part of the class group. Consider a $\mathbb{Z}_p$-extension

$$K \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \bigcup K_n,$$

and write $A_n = \mathrm{Cl}(K_n)_p$ and

$$A_\infty := \varinjlim A_n.$$

This is a discrete Λ- module. We also denote

$$\mathfrak{X} := A_\infty^\vee = \mathrm{Hom}_{\mathrm{cont}}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$$

the pontryagin dual. Through a simple application of Nakayama's lemma, one can see that this is a finitely generated Λ-module. In fact, Iwasawa proved that $\mathfrak{X}$ is a torsion Λ-module. Therefore, it has associated Iwasawa invariants, which we denote by $\mu = \mu_p(K)$ and $\lambda = \lambda_p(K)$, along with a characteristic polynomial $f_K(T)$. He proved the following celebrated theorem:

Theorem 2.4 (Iwasawa)**.** *Let K_∞/K be any $\mathbb{Z}_p$-extension. Write $\#A_n = p^{e_n}$. Then there exists an integer ν such that*

$$e_n = \mu p^n + \lambda n + \nu$$

for all sufficiently large n. Here μ, λ are the Iwasawa invariants of $\mathfrak{X}$ defined above.

Thus, to understand the growth of the p-part of the class group, it suffices to study the Iwasawa invariants μ and λ. In general, very little is known, but when we restrict to the cyclotomic $\mathbb{Z}_p$-extension, we have a much better understanding.

Conjecture 2.2 (Iwasawa)**.** *Let K be a number field and consider K_∞/K the cyclotomic $\mathbb{Z}_p$-extension. Then $\mu_p(K) = 0$.*

This conjecture was proven for abelian number fields by Ferrero and Washington [FW79].

Conjecture 2.3 (Greenberg)**.** *Let K be a totally real number field and K_∞/K the cyclotomic $\mathbb{Z}_p$-extension. Then $\lambda_p(K) = 0$.*

In particular, for a totally real number field K, it is expected that $\mu_p(K) = \lambda_p(K) = 0$. This is known when $K = \mathbb{Q}$.

Although we will not go into detail, it is worth mentioning that this is only one side of the picture in Iwasawa theory. The other side concerns the analytic aspect. Kubota and Leopoldt constructed p-adic L-functions, which are p-adic analogues of classical L-functions. The **Iwasawa main conjecture** asserts that these p-adic L-functions coincide with the characteristic polynomials $f_K(T)$ that we constructed earlier.

2.3 Iwasawa theory of elliptic curves

We now move to the Iwasawa theory of elliptic curves. This was pioneered by Mazur, and later developed by Greenberg and many others. A good reference is [Gre99] for an overview of the theory.

2.3.1 Selmer groups

Let E be an elliptic curve over a number field K and p a prime number. Let S be a finite set of primes containing the Archimedean primes, the primes above p, and the primes of bad reduction. We denote by K_S the maximal extension of K unramified outside S and write $G_S := G_{K,S} := \mathrm{Gal}(K_S/K)$ and $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$. Finally, we write $E[n]$ for the n-torsion of the elliptic curve, and $E(p) = E[p^\infty]$ for the p^∞-torsion.

Definition 2.4. *With the above notation, define the p^k-Selmer group as*

$$\mathrm{Sel}_{p^k}(E/K) := \ker\left(H^1(K_S/K, E[p^k]) \to \bigoplus_{v\in S} H^1(K_v, E)[p^k]\right).$$

Taking direct limits with respect to the inclusions $E[p^k] \hookrightarrow E[p^{k+1}]$, define

$$\mathrm{Sel}_{p^\infty}(E/K) := \varinjlim \mathrm{Sel}_{p^k}(E/K).$$

If K_∞/K is a $\mathbb{Z}_p$-extension, define

$$\mathrm{Sel}_{p^\infty}(E/K_\infty) := \varinjlim \mathrm{Sel}_{p^\infty}(E/K_n),$$

where K_n are the intermediate fields in the $\mathbb{Z}_p$-tower.

The Kummer sequence gives the following important exact sequence:

$$0 \to E(K)\otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/K) \to Ш(E/K)(p) \to 0 \tag{2.1}$$

A few remarks are in order:

1. $E(K)\otimes \mathbb{Q}_p/\mathbb{Z}_p \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r$, where $r = \mathrm{rank}\, E(K)$.
2. The Tate–Shafarevich group $Ш(E/K)$ is conjecturally always finite. This means that the infinite part of the Selmer group is fully captured by the rank of the elliptic curve.
3. There is an equivalent definition of the Selmer group:

$$\mathrm{Sel}_{p^k}(E/K) := \ker\left(H^1(K, E[p^k]) \to \prod_{v} H^1(K_v, E)[p^k]\right),$$

where the product runs over all primes. Understanding the equivalence of these two

definitions is an important exercise. In fact, this is a crucial step in proving the weak Mordell–Weil theorem.

2.3.2 Fundamental diagram and applications

From now on, and for the rest of the chapters, we assume K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension. In this section, we fix an elliptic curve E/K with good ordinary reduction at every prime above p.

For an algebraic extension M/K with $M \subset K_S$ and a prime η of M, we write

$$\mathcal{G}_E^S(M) := \mathrm{Im}\left(H^1(M, E[p^\infty]) \to \bigoplus_{v \in S} H^1(M_\eta, E)[p^\infty] \right).$$

Consider the following commutative diagram:

$$\begin{array}{ccccccccc}
 & & \ker(s_n) & \longrightarrow & H^1(\Gamma_n, E(K_\infty)[p^\infty]) & \longrightarrow & \ker(g_n) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Sel}_{p^\infty}(E/K_n) & \longrightarrow & H^1(K_S/K_n, E[p^\infty]) & \longrightarrow & \mathcal{G}_E^S(F_n) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle s_n} & & \downarrow{\scriptstyle h_n} & & \downarrow{\scriptstyle g_n} & & \\
0 & \longrightarrow & \mathrm{Sel}_{p^\infty}(E/K_\infty)^{\Gamma_n} & \longrightarrow & H^1(K_S/K_\infty, E[p^\infty])^{\Gamma_n} & \longrightarrow & \mathcal{G}_E^S(F_\infty)^{\Gamma_n} & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \mathrm{coker}(s_n) & \longrightarrow & H^2(\Gamma_n, E[p^\infty]) = 0 & & & &
\end{array} \tag{2.2}$$

We list a few facts:

Remark 2.3. *1. It is not hard to see that $E(K_\infty)[p^\infty]$ is finite. This implies that $H^1(\Gamma_n, E(K_\infty)[p^\infty])$ is finite and bounded as $n \to \infty$. This conclusion can also be reached without assuming the finiteness of $E(K_\infty)[p^\infty]$, but we omit that discussion here.*

2. The middle column follows from the inflation-restriction sequence.

3. $\Gamma_n \cong \mathbb{Z}_p$ *is a free pro-p group, and hence has p-cohomological dimension 1. Therefore,* $\operatorname{coker}(h_n) = 0$.

4. $\ker(g_n) \leq \bigoplus_{v \in S} H^1((K_\infty)_\eta / K_n, E(K_\infty)_\eta[p^\infty])$. *The size of this group is finite and bounded as* $n \to \infty$*, and is equal to*

$$\prod_{v \text{ bad}} c_v^{(p)} \cdot \prod_{v|p} N_v^2,$$

where $N_v := \#\tilde{E}(k_v)(p)$ *and* k_v *is the residue field of* K *at* v*, and* $c_v^{(p)}$ *is the p-part of the Tamagawa number at* v*. Its Pontryagin dual is a quotient of* $\bigoplus_{v \in S} \varprojlim E(K_v)/p^n$*, which is a finitely generated* $\mathbb{Z}_p$*-module.*

Iwasawa theory for elliptic curves begins with the following result of Mazur:

Theorem 2.5 (Mazur)**.** *Let* E/K *be an elliptic curve and p any prime. The Pontryagin dual of the Selmer group,*

$$\mathfrak{X}(E/K_\infty) := \operatorname{Hom}(\operatorname{Sel}_{p^\infty}(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p),$$

is a finitely generated $\Lambda(\Gamma)$*-module.*

Proof. By Nakayama's Lemma (Theorem 2.3), it suffices to show that $\operatorname{Sel}_{p^\infty}(E/K_\infty)^\Gamma$ is a cofinitely generated $\mathbb{Z}_p$-module. This follows from the diagram above and Remark 2.3. □

In fact, Mazur conjectured the following:

Conjecture 2.4. *Suppose the elliptic curve has good ordinary reduction at every prime of* K *above* p *(we will simply say that* p *is a good ordinary prime in that case). Then* $\mathfrak{X}(E/K_\infty)$ *is a torsion* Λ*-module.*

When $K/\mathbb{Q}$ is an abelian extension, this conjecture is known by the results of Kato and Rohrlich. It is also easy to prove when $\mathrm{Sel}_{p^\infty}(E/K)$ is finite, via a quick application of the Control Theorem. It is important to remark, as we see in Chapter 5, that the module $\mathfrak{X}$ is not torsion when the elliptic curve has supersingular reduction.

Definition 2.5. *When $\mathfrak{X}(E/K_\infty)$ is a torsion Λ-module, we denote its Iwasawa invariants by $\mu_p(E)$ and $\lambda_p(E)$.*

A key result in the theory is the following:

Theorem 2.6 (Mazur's Control Theorem)**.** *Suppose E/K has good ordinary reduction at all primes above p, and K_∞/K is any $\mathbb{Z}_p$-extension. Then the kernel and cokernel of the natural maps*

$$\mathrm{Sel}_{p^\infty}(E/K_n) \to \mathrm{Sel}_{p^\infty}(E/K_\infty)^{\Gamma_n}$$

are finite and bounded as $n \to \infty$.

Proof. As in Theorem 2.5, this follows from the fundamental diagram 2.2 and Remark 2.3. □

A key difference between the Iwasawa theory of class groups and that of Selmer groups is the behavior of the μ-invariant. Although conjecturally $\mu_p = 0$ for class groups, the same is not true for elliptic curves. For an elliptic curve $E/\mathbb{Q}$, there are (rare) examples with $\mu_p(E) > 0$. However, we have the following conjecture:

Conjecture 2.5 (Greenberg)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at p. If $E[p]$ is irreducible (which is true for all but finitely many primes), then $\mu_p(E) = 0$.*

The best result toward this conjecture was proven recently using modular symbols [Cha24]:

Theorem 2.7. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $\mu_p(E) \leq 1$ for all but finitely many ordinary primes.*

The λ-invariant provides an upper bound for the rank:

Theorem 2.8. *Assume E/K has good ordinary or multiplicative reduction at all primes v of K above p, and that $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is Λ-cotorsion. Then*

$$\operatorname{rank} E(K_n) \leq \lambda_p(E)$$

for all $n \geq 0$.

Proof. By definition, $\lambda_p(E) = \operatorname{rank}_{\mathbb{Z}_p} \mathfrak{X}(E/K_\infty) = \operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/K_\infty)$. The map $\mathrm{Sel}_{p^\infty}(E/K_n) \to \mathrm{Sel}_{p^\infty}(E/K_\infty)$ has finite kernel by the Control Theorem 2.6 (we do not need the cokernel to be finite).

Hence,

$$\operatorname{rank}(E/K_n) \leq \operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/K_n) \leq \operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/K_\infty),$$

as desired. (The first inequality follows from the Kummer sequence 2.1). The multiplicative case works very similarly and details can be found in [Gre99]. □

Remark 2.4. *If $\lambda_p(E) = \operatorname{rank} E(K)$, then the above theorem implies that the rank of the elliptic curve remains stable throughout the $\mathbb{Z}_p$-extension. Heuristic evidence suggests that this in fact happens for density one of the primes. One of the goals of this thesis is to provide theoretical and computational evidence of this fact.*

We continue with an important property of the Selmer group:

Theorem 2.9. *Suppose $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is Λ-cotorsion and $E(K)[p] = 0$ (which is true for all but finitely many primes). Then $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ has no proper Λ-submodules of finite index.*

Proof. See [Gre99, Prop. 4.15]. □

We close this section by stating the **weak Leopoldt conjecture for elliptic curves**:

Conjecture 2.6. *Let E/K be an elliptic curve and p any prime. Then*

$$H^2(K_S/K_\infty, E[p^\infty]) = 0.$$

Remark 2.5.

1. *When $K/\mathbb{Q}$ is an abelian extension, this is known by Kato [Kat04].*
2. *When E/K is a CM elliptic curve, this is known by Rubin [Rub99] in the ordinary case, and by McConnell in the supersingular case [McC96].*

2.4 Fermat Quotient

In this section, we introduce some notation and basic properties that are used throughout the thesis concerning the Fermat quotient.

Definition 2.6. *Let p be a prime and let $a \in \mathbb{Z}$ with $(a,p) = 1$. Define the Fermat quotient $q_p(a) \in \mathbb{Z}/p\mathbb{Z}$ by*

$$q_p(a) \equiv \frac{a^{p-1} - 1}{p} \pmod{p}.$$

We record some basic properties:

Lemma 2.1. *Let p be a prime. The following hold:*

1. $q_p(1) = 0$.
2. $q_p(-a) = q_p(a)$ *for all a coprime to p.*

If $a, b \in \mathbb{Z}$ are coprime to p, then:

(a) $q_p(ab) = q_p(a) + q_p(b)$.

(b) $q_p(a/b) = q_p(a) - q_p(b)$.

(c) $q_p(a+np^2) = q_p(a)$ *for all* $n \in \mathbb{Z}$.

(d) $q_p(a+np) = q_p(a) - \frac{n}{a}$ *for all* $n \in \mathbb{Z}$, *where* $\frac{1}{a}$ *denotes the inverse of* a *in* $\mathbb{Z}/p\mathbb{Z}$.

If an elliptic curve $E/\mathbb{Q}$ has Weierstrass model

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and $Q = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \in E^1(\mathbb{Q}_p)$, then substituting the coordinates of the point into the equation and clearing denominators transforms the equation into:

$$b^2 + a_1abd + a_3bd^3 = a^3 + a_2a^2d^2 + a_4ad^4 + a_6d^6. \tag{2.3}$$

Since $p^2 \mid d^2$, all terms involving d^2 (and higher powers) vanish when applying Lemma 2.1(c). Hence:

$$q_p\left(b^2 + a_1abd\right) = q_p(a^3). \tag{2.4}$$

Chapter 3: Gold's Criterion

As mentioned in Conjecture 2.3, for the cyclotomic Iwasawa invariants of class groups, it is expected that $\mu_p(K) = \lambda_p(K) = 0$ whenever K is totally real. This is already known in the case $K = \mathbb{Q}$. Therefore, to find examples with non-trivial λ-invariants, the first place one should look is among imaginary quadratic fields. Gold [Gol74] developed an important criterion in this setting that determines when the Iwasawa invariants attain their minimal values.

In this chapter, we discuss various formulations, approaches, and applications of Gold's criterion. We will assume the notation from Section 2.2.

3.1 Preliminaries

We begin with two important results that set the groundwork for what follows.

Proposition 3.1. *Let K be any number field and p a prime number. Assume that there is a unique prime $\mathfrak{p}$ above p and that it is totally ramified in K_∞. Then $(\mathfrak{X})_{\Gamma_n} \simeq A_n$. In particular,*

$$p \nmid h_0 \iff p \nmid h_n \quad \text{for all } n \geq 0,$$

where $h_n := \#\mathrm{Cl}(K_n)$.

Proof. For the proof, see [Was82, Proposition 13.22]. □

As a consequence, we immediately obtain the following corollary:

Corollary 3.1. *Assume K is an imaginary quadratic field and that K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension. If $p \nmid h_K$ and does not split in K, then $\lambda_p = 0$.*

When p divides h_K, the λ-invariant can be positive, but such cases are very sporadic.

Theorem 3.1 (Iwasawa)**.** *Let K be an imaginary quadratic field, let p be a rational prime which splits in K, and let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension. Let*

$$\mathfrak{X} := A_\infty^\vee \simeq \mathrm{Gal}(L_\infty/K_\infty),$$

where $A_\infty = \varinjlim_n A_n$ and L_∞ is the maximal abelian pro-p extension of K_∞ unramified everywhere. Then $\mathfrak{X}$ has a quotient isomorphic to $\Lambda/(T)$, where $\Lambda = \mathbb{Z}_p[[T]]$. Consequently,

$$T \mid \mathrm{char}_\Lambda(\mathfrak{X}), \qquad \textit{hence} \qquad \lambda_p(K) \geq 1.$$

Proof. Write

$$p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}, \qquad \Gamma := \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p,$$

and let $\widetilde{K}$ be the compositum of all $\mathbb{Z}_p$-extensions of K. Since Leopoldt's conjecture is known for the abelian field K, we have

$$G := \mathrm{Gal}(\widetilde{K}/K) \simeq \mathbb{Z}_p^2.$$

We claim that $\tilde{K}/K_\infty$ is unramified at the primes above p. Let $I_\mathfrak{p}$ and $I_{\bar{\mathfrak{p}}}$ be the inertia subgroups of G at $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. We claim that

$$I_\mathfrak{p} \simeq I_{\bar{\mathfrak{p}}} \simeq \mathbb{Z}_p.$$

Indeed, by ray class field theory there exists a $\mathbb{Z}_p$-extension of K ramified only at $\mathfrak{p}$, and

likewise one ramified only at $\bar{\mathfrak{p}}$. (For example, the p-primary parts of the ray class groups of conductors $\mathfrak{p}^m$ are unbounded, since $(\mathscr{O}_K/\mathfrak{p}^m)^\times \simeq (\mathbb{Z}/p^m\mathbb{Z})^\times$ has p-part of unbounded order, while $\mathscr{O}_K^\times$ is finite.) Thus $I_{\mathfrak{p}} \neq 0$ and $I_{\bar{\mathfrak{p}}} \neq 0$. On the other hand, $I_{\mathfrak{p}} \neq G$, because the $\mathbb{Z}_p$-extension ramified only at $\bar{\mathfrak{p}}$ is unramified at $\mathfrak{p}$; similarly $I_{\bar{\mathfrak{p}}} \neq G$. Since $G \simeq \mathbb{Z}_p^2$, it follows that each of $I_{\mathfrak{p}}$ and $I_{\bar{\mathfrak{p}}}$ is a rank-one closed subgroup, hence isomorphic to $\mathbb{Z}_p$.

Now let

$$\pi : G \twoheadrightarrow \Gamma$$

be the quotient map corresponding to the subextension $K_\infty \subset \widetilde{K}$, and put

$$H := \ker(\pi) = \mathrm{Gal}(\widetilde{K}/K_\infty).$$

Because the cyclotomic $\mathbb{Z}_p$-extension K_∞/K ramifies at both primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ above p, the restrictions

$$\pi|_{I_{\mathfrak{p}}} : I_{\mathfrak{p}} \to \Gamma, \qquad \pi|_{I_{\bar{\mathfrak{p}}}} : I_{\bar{\mathfrak{p}}} \to \Gamma$$

are nonzero. Since $I_{\mathfrak{p}} \simeq I_{\bar{\mathfrak{p}}} \simeq \mathbb{Z}_p$, these maps are injective. Therefore

$$H \cap I_{\mathfrak{p}} = H \cap I_{\bar{\mathfrak{p}}} = 0.$$

So $\widetilde{K}/K_\infty$ is unramified at the primes above p.

On the other hand, every $\mathbb{Z}_p$-extension of K is unramified outside p, hence so is $\widetilde{K}/K$. Therefore $\widetilde{K}/K_\infty$ is everywhere unramified. It follows that

$$\widetilde{K} \subseteq L_\infty,$$

and restriction gives a surjection

$$\mathfrak{X} \simeq \mathrm{Gal}(L_\infty/K_\infty) \twoheadrightarrow \mathrm{Gal}(\widetilde{K}/K_\infty) = H.$$

Finally, since $G \simeq \mathbb{Z}_p^2$ and $\Gamma \simeq \mathbb{Z}_p$, we have

$$H \simeq \mathbb{Z}_p.$$

Moreover, the action of Γ on H is trivial, because $\widetilde{K}/K$ is abelian. Hence, as a Λ-module,

$$H \simeq \Lambda/(T).$$

Since $\mathfrak{X}$ is a torsion Λ-module and admits a quotient isomorphic to $\Lambda/(T)$, its characteristic ideal is divisible by T:

$$T \mid \mathrm{char}_\Lambda(\mathfrak{X}).$$

Therefore $\lambda_p(K) \geq 1$. □

In fact, one can prove that in this case $T \mid f_K(T)$ but $T^2 \nmid f_K(T)$, where f_K is the characteristic polynomial of $\mathfrak{X}$. We examine this more carefully in Section 3.3.

3.2 Original Gold's Criterion and Applications

Using genus theory, Gold developed the following criterion [Gol74].

Theorem 3.2 (Gold's Criterion)**.** *Let K be an imaginary quadratic field and p a prime that splits in K. Write $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Assume $p \nmid h_K$. Let $r \geq 1$ be such that $\mathfrak{p}^r = (\alpha)$ is a principal*

ideal and $(r,p)=1$ *(such an* r *always exists; for example, one can take* $r=h_K$*). Then*

$$\lambda_p > 1 \iff \alpha^{p-1} \equiv 1 \mod \bar{\mathfrak{p}}^2.$$

Furthermore, if $p \mid h_K$ *but* $p \nmid r$*, then* $\lambda_p(K) > 1$.

The original formulation of Gold omits the final comment, which follows from the approach of Federer and Gross, discussed in the next section.

Corollary 3.2. *Assume the notation of the theorem. One can reformulate the above criterion as follows:*

1. *If* $r > 1$*, then*

$$\alpha^{p-1} \equiv 1 \mod \bar{\mathfrak{p}}^2 \iff \mathrm{Tr}(\alpha)^{p-1} \equiv 1 \mod p^2.$$

2. *If* $r = 1$*, then*

$$a^{p-1} \equiv 1 \mod \bar{\mathfrak{p}}^2 \iff \mathrm{Tr}(a^2)^{\frac{p-1}{2}} \equiv 1 \mod p^2 \iff \mathrm{Tr}(a)^{p-1} + p \cdot \mathrm{Tr}(a)^{p-3} \equiv 1 \mod p^2.$$

Proof. 1. This can be found in [San93]. Assume $r > 1$ and $\mathfrak{p}^r = (\alpha)$. Then $\bar{\alpha} \equiv 0 \mod \bar{\mathfrak{p}}^2$, so

$$\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha} \equiv \alpha \mod \bar{\mathfrak{p}}^2,$$

and hence

$$\mathrm{Tr}(\alpha)^{p-1} \equiv \alpha^{p-1} \mod \bar{\mathfrak{p}}^2.$$

But $\mathrm{Tr}(\alpha) \in \mathbb{Z}$, so we conclude

$$\alpha^{p-1} \equiv 1 \mod \bar{\mathfrak{p}}^2 \iff \mathrm{Tr}(\alpha)^{p-1} \equiv 1 \mod p^2.$$

2. Assume $\mathfrak{p} = (\alpha)$. Then $\bar{\alpha}^2 \equiv 0 \mod \bar{\mathfrak{p}}^2$, so $\mathrm{Tr}(\alpha^2) \equiv \alpha^2 \mod \bar{\mathfrak{p}}^2$. In particular,

$$\mathrm{Tr}(\alpha^2)^{\frac{p-1}{2}} \equiv \alpha^{p-1} \mod p^2.$$

Now, since $\mathrm{Tr}(\alpha)^2 = \mathrm{Tr}(\alpha)^2 - 2 \cdot \mathrm{Nm}(\alpha) = \mathrm{Tr}(\alpha)^2 - 2p$, we have

$$(\mathrm{Tr}(\alpha)^2 - 2p)^{\frac{p-1}{2}} \equiv \mathrm{Tr}(\alpha)^{p-1} + p\,\mathrm{Tr}(\alpha)^{p-3} \mod p^2.$$

□

At first glance, the criterion may not seem very strong—after all, it only checks whether $\lambda > 1$. However, it has a number of useful applications:

1. **Heuristic density argument:** Heuristically, if α behaves "randomly enough," then the probability that
$$\mathrm{Tr}(\alpha)^{p-1} \equiv 1 \mod p^2$$
is roughly $\frac{1}{p}$. This suggests that the set of primes p for which $\lambda_p > 1$ has density 0.

2. **Computation and data gathering:** The criterion is easily computable, allowing us to gather a large amount of data. Below is a table computed using Sage [Tea24]. The heuristic mentioned above—that the probability $\lambda_p > 1$ is approximately $\frac{1}{p}$—seems to hold. The code and its output can be found at [Foi25].

Table 3.1: Summary of Imaginary Quadratic Field Results

p	Total # of Fields Tested	$\lambda_p = 1$	$\lambda_p > 1$
3	1609	1062	547
5	1971	1591	380
7	2277	1945	332
11	2574	2350	224
13	2647	2434	213
17	2771	2606	165
19	2814	2654	160

3. **Constructing infinite families:** For a fixed prime p, one can construct infinite families of imaginary quadratic fields $\{K_i\}$ such that $\lambda_p(K_i) > 1$. For example, consider

$$K = \mathbb{Q}(\sqrt{1-4p^n}).$$

Then it is easy to see that p splits and

$$\mathfrak{p}^n = \left(\frac{1+\sqrt{1-4p^n}}{2}\right) = (\alpha).$$

But $\mathrm{Tr}(\alpha) = 1$, so for all n such that $(n,p) = 1$, we have $\lambda_p > 1$.

4. **Fields with $\lambda_p = 1$:** On the other hand, constructing infinite families of fields with $\lambda_p = 1$ is more difficult, as one must check whether $p \mid h_K$. However, the following remarkable theorem offers a workaround:

Theorem 3.3 (Jochnowitz)**.** *Fix an odd prime p. Suppose there exists one imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ with $\lambda_p(K) = 1$ and such that p splits in K. Then there*

exist infinitely many such imaginary quadratic fields.

Proof. See [Joc94]. The proof is non-constructive and relies on properties of p-adic L-functions and modular forms. □

The remaining question is whether one can find at least one imaginary quadratic field with $\lambda_p = 1$. This can be achieved with the following result:

Theorem 3.4. *Assume $p > 3$ and $p \neq 7$. If $\lambda_p(\mathbb{Q}(\sqrt{1-p})) > 1$, then $\lambda_p(\mathbb{Q}(\sqrt{4-p})) = 1$.*

Proof. We present a much simplified version of the proof from [Ito15], using the notation and properties of Fermat quotients introduced in Section 2.4.

First, recall an analytic number theory result stating that $h_K < \frac{|d_K|}{4}$, where d_K is the discriminant of K. This implies $h_K < p$ for both number fields under consideration.

Let $K = \mathbb{Q}(\sqrt{1-p})$. Then p splits since $\left(\frac{1-p}{p}\right) = 1$, and $\mathfrak{p} = (1+\sqrt{1-p}) = (\alpha)$ is a principal ideal with $\mathrm{Tr}(\alpha^2) = 4-2p$. By Corollary 3.2,

$$\lambda_p(K) > 1 \iff q_p(4-2p) \equiv 0 \mod p \iff q_p(4) + \frac{1}{2} \equiv 0 \mod p \iff q_p(4) \equiv -\frac{1}{2} \mod p.$$

Let $L = \mathbb{Q}(\sqrt{4-p})$. Again, p splits and $\mathfrak{p} = (2+\sqrt{4-p}) = (\beta)$ is principal with $\mathrm{Tr}(\beta^2) = 16-2p$. Then:

$$\lambda_p(L) > 1 \iff q_p(16-2p) = 0 \iff q_p(16) + \frac{1}{8} \equiv 0 \mod p \iff q_p(4) \equiv -\frac{1}{16} \mod p.$$

This completes the proof. □

3.3 Federer–Gross

A deeper approach to Gold's criterion, which applies to CM fields in general, was developed by Federer and Gross in [FG81]. We provide a brief overview here.

We begin by introducing some notation. Let K be a CM field with totally real subfield k. Fix an odd prime number p and define:

1. $S := \{\mathfrak{p} \trianglelefteq K : \mathfrak{p} \mid p \text{ or } \infty\}$.
2. I is the set of primes in k that split in K.
3. $r := r(K) := \#I$.
4. $V := V(K)$ is the group of units of K.
5. $V_S := V_S(K)$ is the group of S-units of K.
6. M is the free abelian group on the set S (i.e., the group of divisors supported on S).
7. For any $\mathrm{Gal}(K/k)$-module N, define the *minus part* $N^- := \{n \in N : \mathfrak{c}(n) = -n\}$, where $\mathfrak{c}$ denotes complex conjugation.
8. $h_K^- := \#A_K^-$, the order of the minus part of the class group.
9. f_v is the residue field degree of a prime v.
10. w_K is the number of roots of unity in K.

Note that both $V_S(K)^-$ and M^- are finitely generated abelian groups of rank $r(K)$.

Define the maps:

$$\phi : V_S^- \to M^-, \qquad \varepsilon \mapsto \sum_{v \mid p} \mathrm{ord}_p(N_{K_v/\mathbb{Q}_p}\varepsilon) \cdot v,$$

$$\lambda : V_S^- \to \mathbb{Q}_p \otimes M^-, \qquad \varepsilon \mapsto \sum_{v|p} \log_p(N_{K_v/\mathbb{Q}_p}\varepsilon) \cdot v.$$

We remark that:

- The map $\phi : \mathbb{Q} \otimes V_S^- \to \mathbb{Q} \otimes M^-$ is an isomorphism.
- The map $\lambda : \mathbb{Q} \otimes V_S^- \to \mathbb{Q}_p \otimes M^-$ is conjectured to be an isomorphism. This is known when $K/\mathbb{Q}$ is abelian or when $r(K) = 1$.

Define the p-adic regulator as

$$\mathrm{Reg}_p := \det(\lambda \circ \phi^{-1} \mid \mathbb{Q}_p \otimes M^-).$$

Now consider the cyclotomic $\mathbb{Z}_p$-extension K_∞/K. Write $A_\infty^- = \varinjlim A_n^-$ and $\mathfrak{X}^- := (A_\infty^-)^\vee$ is a finitely generated torsion Λ-module, and we write $f(T)$ for its characteristic polynomial.

Theorem 3.5 (Federer–Gross)**.** *In the above setting, $f(T)$ factors as $f(T) = T^r g(T)$, and*

$$g(0) \sim \frac{h_K^- \cdot \prod_{\mathfrak{p} \in I} f_\mathfrak{p}}{w_{K(\mu_p)}^{r(K)}} \cdot \frac{\mathrm{Reg}_p}{p^{r(K)}}.$$

This is a powerful result. Let us specialize to the case where K is an imaginary quadratic field, $k = \mathbb{Q}$, and p is a prime that splits in K.

1. $A = A^-$ and $h_K = h_K^-$.
2. $S = \{\mathfrak{p}, \bar{\mathfrak{p}}, \infty\}$, $I = \{p\}$, and hence $r = 1$.
3. Up to 2-torsion, $V_S = \langle \pi \rangle \oplus \langle \bar{\pi} \rangle$, and $V_S^- = \left\langle \frac{\pi}{\bar{\pi}} \right\rangle$, where π is a uniformizer with $\mathrm{ord}_p(\pi) = 1$.
4. $M = \langle \mathfrak{p}, \bar{\mathfrak{p}}, \infty \rangle$, and $M^- = \langle \mathfrak{p} - \bar{\mathfrak{p}} \rangle$.

5. The map $\phi : V_S^- \to M^-$ sends $\varepsilon = \frac{\pi}{\bar{\pi}} \mapsto 2(\mathfrak{p} - \bar{\mathfrak{p}})$.

   The map $\lambda : \mathbb{Q} \otimes V_S^- \to \mathbb{Q}_p \otimes M^-$ sends $\varepsilon = \frac{\pi}{\bar{\pi}} \mapsto 2\log_p(\pi)$.

6. $w_K = 2$, except when $K = \mathbb{Q}(i)$ (where $w_K = 4$) or $K = \mathbb{Q}(\sqrt{-3})$ (where $w_K = 6$). In general, $w_{K(\mu_p)} = \mathrm{lcm}(w_K, p-1) \sim 1$ for any odd prime p (except $p = 3$ and $K = \mathbb{Q}(\sqrt{-3})$).

7. $\mathrm{Reg}_p = \log_p(\pi)$.

Now suppose $\mathfrak{p}^r = (\alpha)$ for some r coprime to p. Then $\alpha = \pi^r u$ for some unit $u \in V_S$, and hence

$$\log_p(\pi) = \frac{1}{r}\log_p(\alpha).$$

Applying the theorem, we get that $f(T) = Tg(T)$ with $g(0) \neq 0$ and

$$g(0) \sim h_K \cdot \frac{\mathrm{Reg}_p}{p} \sim h_K \cdot \frac{\log_p(\alpha)}{pr}.$$

The observation that

$$\mathrm{ord}_p(\log_p(\alpha)) > 1 \iff \alpha^{p-1} \equiv 1 \mod \bar{\mathfrak{p}}^2$$

leads us directly to the original formulation of Gold's criterion! It is precisely this approach that we will attempt to generalize in the setting of elliptic curves.

3.4 Two Other Approaches

We close this chapter by briefly discussing two other interesting approaches to Gold's criterion.

In the original paper by Gross, his criterion is reformulated as follows. Let H be the p-ray class field of K modulo $\bar{\mathfrak{p}}^2$, and let $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(H/K)$ be the image of $\mathfrak{p}$ under the Artin map. Then

$$\lambda_p(K) > 1 \iff \sigma_{\mathfrak{p}} = 1.$$

Ray class fields of imaginary quadratic fields are closely related to CM elliptic curves. By exploring this relationship and using Deuring's criterion, Stokes [Sto24] arrived at the following theorem:

Theorem 3.6 (Stokes)**.** *Let K be an imaginary quadratic field and p a prime that splits, $(p) = \mathfrak{p}\bar{\mathfrak{p}}$. Let H_K be the Hilbert class field of K, and let E/H_K be an elliptic curve with complex multiplication by K. Let $\mathfrak{P} \trianglelefteq H_K$ be a prime above $\mathfrak{p}$, and let $\tilde{E}$ be the reduction of $E \mod \mathfrak{P}$. Then*

$$\lambda_p(K) > 1 \iff \#\tilde{E}(\mathbb{F}_{p^{p-1}}) \equiv 0 \mod p^2.$$

Proof. See [Sto24]. □

Finally, building on work of Sharifi et al. [LLS+23], Peikai [Qi24] offered a new proof of Gold's criterion using Iwasawa cohomology and cup products. The idea can be outlined as follows:

Define:

1. $G = \mathrm{Gal}(K_S/K)$ and $N \trianglelefteq G$ a closed normal subgroup (either $\mathrm{Gal}(K_S/K_\infty)$ or $\mathrm{Gal}(K_S/K_n)$).
2. $\Omega = \mathbb{F}_p[[G/N]]$ and $I = I_\Omega$ its augmentation ideal.
3. The Iwasawa cohomology groups:

$$H^i_{\mathrm{Iw}}(N, \mu_p) := \varprojlim H^i(U, \mu_p),$$

where the inverse limit is taken over open normal subgroups $U \subset G$ containing N, with respect to corestriction maps. In particular:

$$H^i_{\mathrm{Iw}}(N,\mu_p) = \begin{cases} \varprojlim H^i(K_S/K_n,\mu_p) & \text{if } N = \mathrm{Gal}(K_S/K_\infty), \\ H^i(K_S/K_n,\mu_p) & \text{if } N = \mathrm{Gal}(K_S/K_n). \end{cases}$$

Consider the short exact sequence:

$$0 \to I^n/I^{n+1} \otimes_{\mathbb{F}_p} \mu_p \to \Omega/I^{n+1} \otimes_{\mathbb{F}_p} \mu_p \to \Omega/I^n \otimes_{\mathbb{F}_p} \mu_p \to 0,$$

for $0 \leq n < |G/N|$. Since $\mathrm{cd}_p(G) = 2$, this induces a map

$$\Psi^{(n)} : H^1(G, \Omega/I^n \otimes \mu_p) \to H^2(G,\mu_p) \otimes I^n/I^{n+1},$$

called the **Bockstein map**.

Sharifi et al. [LLS+23] proved the following fundamental result:

Theorem 3.7.

$$\frac{I^n H^2_{\mathrm{Iw}}(N,\mu_p)}{I^{n+1}} \simeq \frac{H^2(G,\mu_p) \otimes I^n/I^{n+1}}{\mathrm{Im}(\Psi^{(n)})}, \qquad 0 \leq n < |G/N|.$$

An immediate corollary is the following:

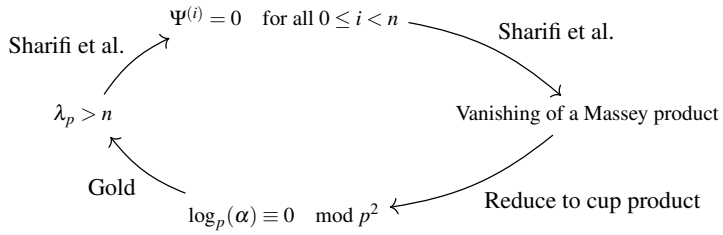
Corollary 3.3. *Assume* $\Psi^{(k)} \neq 0$ *for some* $0 < k < |G/N|$. *Then*

$$|H^2_{\mathrm{Iw}}(N,\mu_p)| = p^n, \qquad \textit{where } n = \min\{n : \Psi^{(n)} \neq 0\}.$$

The value of the λ-invariant determines the size of $H^2_{\mathrm{Iw}}(N,\mu_p)$, which in turn governs the vanishing of the Bockstein maps. Through techniques introduced in [LLS+23], the

vanishing of Bockstein maps corresponds to the vanishing of certain **Massey products**, which generalize cup products in Galois cohomology. Finally, the vanishing of the Massey product recovers the original numerical formulation of Gold's criterion.

The following diagram summarizes the logic of the proof:



Let $\chi : \mathrm{Gal}(K_S/K) \to \mathrm{Gal}(K_\infty/K)$ be the canonical character. In the usual setting where $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ and $\mathfrak{p}^r = (\alpha)$ with $p \nmid h_K$, the element α corresponds (via Kummer theory) to a cohomology class $\chi_\alpha \in H^1(K, \mu_p)$ under the identification $K^\times/(K^\times)^p \simeq H^1(K, \mu_p)$.

The approach outlined above yields the following result:

Theorem 3.8 (Peikai)**.** *Under the above notation,*

$$\lambda_p > 1 \iff \chi \cup \chi_\alpha = 0 \iff \alpha \in \mathrm{Nm}(K_1/K).$$

See [Qi24] for more details.

It would be interesting to explore whether this strategy could be adapted to other settings, such as the fine Selmer group of elliptic curves.

Chapter 4: Iwasawa Theory of Elliptic Curves at Ordinary Primes

In this chapter, we study the ordinary case; the supersingular case is treated in the next chapter. Our ultimate objective is to establish an analog of Gold's criterion in this setting.

Throughout this section, we fix an elliptic curve $E/\mathbb{Q}$ and an odd prime $p \geq 5$ at which E has good ordinary reduction. In this situation, the dual of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ is a torsion Λ-module, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ and $\Lambda = \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$ denotes the Iwasawa algebra. We denote by $f_E(T)$ the characteristic polynomial of

$$\mathfrak{X}(E/\mathbb{Q}_\infty) = \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\vee.$$

Here, $(-)^\vee$ denotes the Pontryagin dual $\mathrm{Hom}_{\mathrm{cont}}(-, \mathbb{Q}_p/\mathbb{Z}_p)$.

4.1 Notation

Throughout the remaining chapters, we adopt the following notation.

We fix an elliptic curve $E/\mathbb{Q}$ and a prime $p \geq 5$ of good reduction. We denote by $\tilde{E}/\mathbb{F}_p$ the reduction of E modulo p.

- $E^0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : P \text{ has non-singular reduction at } p\}$.
- $E^0(\mathbb{Q}) = \{P \in E(\mathbb{Q}) : P \text{ has non-singular reduction at every prime } \ell\}$.
- $E^k(\mathbb{Q}_p)$ denotes the k-th step in the formal group filtration.

- If A is a finite group, we write $A[p]$ for its p-torsion subgroup, and $A(p)$ for its p-primary part.
- $N_p(E) = \#\tilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ where $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ denotes the set of non-singular points of $\tilde{E}$ over $\mathbb{F}_p$. When the elliptic curve is clear from context, we simply write N_p.
- $C_E = \min\{n \geq 1 : nP \in E^0(\mathbb{Q}) \text{ for all } P \in E(\mathbb{Q})\}$.
- c_ℓ denotes the local Tamagawa number of E at ℓ.
- $\mathrm{Tam}(E)$ denotes the least common multiple of the Tamagawa numbers.
- If
$$P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \in E(\mathbb{Q}),$$
we always assume that $a, b, d \in \mathbb{Z}$ with $d > 0$ and $\gcd(a,d) = \gcd(b,d) = 1$. We define
$$a(P) = a, \quad b(P) = b, \quad d(P) = d,$$
and write
$$nP = \left(\frac{a_n}{d_n^2}, \frac{b_n}{d_n^3}\right).$$
When we need to be more explicit, we write $a_n(P), b_n(P), d_n(P)$ instead of a_n, b_n, d_n.

4.2 The p-adic σ-function

We begin by describing the construction of the p-adic regulator. To this end, we first briefly recall the p-adic σ-function. In this subsection, we follow [MT91] and [MST06].

Theorem 4.1 (Mazur–Tate)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at*

a prime p, given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then the p-adic σ-function is the unique function

$$\sigma_p : E^1(\mathbb{Q}_p) \cong \hat{E}(\mathfrak{p}) \longrightarrow \mathbb{Q}_p$$

satisfying the following properties:

1. *For all $m \in \mathbb{Z}$ and $Q \in \hat{E}(\bar{\mathbb{Z}}_p)$,*

$$\sigma_p(mQ) = \sigma_p(Q)^{m^2} f_m(Q),$$

   where f_m denotes the m-th division polynomial with respect to the invariant differential ω.

2. *The function σ_p is odd, satisfies $\sigma_p(t) \in t\mathbb{Z}_p[[t]]$, and there exists a constant $c \in \mathbb{Z}_p$ such that*

$$x(t) + c = -\frac{d}{\omega}\left(\frac{1}{\sigma_p}\frac{d\sigma_p}{\omega}\right).$$

   The constant c can be computed explicitly as

$$c = \frac{a_1^2 + 4a_2}{12} - \frac{1}{12}\mathbb{E}_2(E, \omega),$$

   where $\mathbb{E}_2(E, \omega)$ denotes the Katz weight 2 p-adic Eisenstein series evaluated at (E, ω).

We shall see later that property (1) is also satisfied by the denominator of a point P.

The differential equation in property (2) of Theorem 4.1 provides an explicit method

for computing the p-adic σ-function. See, for example, Algorithm 3.1 in [MST06]. Implementing that algorithm in Sage [Tea24], one obtains the expansion

$$\sigma_p(t) = t + \frac{1}{2}a_1 t^2 + \left(\frac{3}{8}a_1^2 + \frac{1}{2}a_2 - \frac{1}{2}c\right)t^3 + \left(\frac{5}{16}a_1^3 + \frac{3}{4}a_1a_2 - \frac{3}{4}a_1c + \frac{1}{2}a_3\right)t^4 + \dots. \tag{4.1}$$

We record the following observations.

1. Since σ_p is odd, one expects $\sigma_p(-P) = -\sigma_p(P)$ for suitable $P \in E(\mathbb{Q})$. To interpret this via the formal group, consider the isomorphism

$$\begin{aligned} E^1(\mathbb{Q}_p) &\xrightarrow{\sim} \hat{E}(\mathfrak{p}) \cong p\mathbb{Z}_p \\ P = (x,y) = \left(\tfrac{a}{d^2}, \tfrac{b}{d^3}\right) &\longmapsto t = -\tfrac{x}{y} = -\tfrac{a}{b}d \end{aligned} \tag{4.2}$$

which sends P to $t = -x/y$. Since

$$-P = (x, -y + a_1x + a_3),$$

it does not follow in general that $-P$ is sent to $-t$. Consequently, the expansion (4.1) may contain even powers of t.

However, if $a_1 = a_3 = 0$ (for example, when E is in short Weierstrass form), then $\sigma_p(t) \in t\mathbb{Z}_p[[t]]$ is an odd power series.

2. In order to compute σ_p, one must first determine the constant c, and hence compute the Katz weight 2 p-adic Eisenstein series. This can be achieved using Kedlaya's algorithm. The original version required $p \geq 5$ and a minimal Weierstrass model. By modifying the model, Balakrishnan [Bal16] extended the method to the case $p = 3$.

3. If E is a CM elliptic curve of rank 1, then the value of $\mathbb{E}_2(E,\omega)$ is independent of p and lies in the field of complex multiplication of E; see [Kat76, Lemma 8.0.13].

4.3 The p-adic Height

We now describe the construction of the p-adic height, focusing on its computational aspects. Throughout this subsection, we follow [MST06].

Definition 4.1. *Let E be an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at an odd prime p, and let $P \in E^1(\mathbb{Q}_p) \cap E^0(\mathbb{Q})$. The (cyclotomic) p-adic height of P is defined by*

$$h_p(P) = \log_p\left(\frac{\sigma_p(P)}{d(P)}\right), \tag{4.3}$$

where $\log_p$ denotes the p-adic logarithm.

If $P \in E(\mathbb{Q})$, choose a positive integer m such that

$$Q := mP \in E^1(\mathbb{Q}_p) \cap E^0(\mathbb{Q}),$$

and define

$$h_p(P) := \frac{1}{m^2} h_p(Q).$$

Such an integer m always exists, as explained in Remark 4.1 below. We note that this definition is independent of the choice of Weierstrass model for E.

Remark 4.1. *1. Some references include an additional factor of $\frac{1}{p}$ in (4.3); we adopt the normalization given above.*

2. If E is given by a global minimal Weierstrass model, then one may take

$$m = \operatorname{lcm}\big(\operatorname{Tam}(E), N_p\big),$$

where $\mathrm{Tam}(E)$ *denotes the least common multiple of the Tamagawa numbers, and*

$$N_p = [E^0(\mathbb{Q}_p) : E^1(\mathbb{Q}_p)] = [E(\mathbb{Q}_p) : E^1(\mathbb{Q}_p)] = \#\tilde{E}(\mathbb{F}_p),$$

since p is a good prime. Indeed, by definition of the Tamagawa numbers, $\mathrm{Tam}(E) \cdot P \in E^0(\mathbb{Q})$ *for all* $P \in E(\mathbb{Q})$*. Moreover,* $N_p \cdot P \in E^1(\mathbb{Q}_p)$ *for all* $P \in E(\mathbb{Q})$*. Hence* $mP \in E^1(\mathbb{Q}_p) \cap E^0(\mathbb{Q})$ *for all* $P \in E(\mathbb{Q})$*.*

3. *If E is not given by a global minimal Weierstrass model, then* $\mathrm{Tam}(E) \cdot P$ *need not lie in* $E^0(\mathbb{Q})$*.*[1] *In Section 6 we present an algorithm for computing the index* $[E(\mathbb{Q}) : E^0(\mathbb{Q})]$ *in terms of the Tamagawa numbers. This index is independent of P. Alternatively, one may use Proposition 6.2 to determine the smallest scalar multiple m such that* $mP \in E^0(\mathbb{Q})$*. Although this m depends on P, it is computationally more efficient.*

We conclude with some fundamental properties.

Proposition 4.1. *The p-adic height defined above is well-defined and satisfies the following properties:*

1. $h_p(mP) = m^2 h_p(P)$ *for all* $P \in E(\mathbb{Q})$ *and* $m \in \mathbb{Z}$*.*
2. $h_p(P+Q) + h_p(P-Q) = 2h_p(P) + 2h_p(Q)$ *for all* $P, Q \in E(\mathbb{Q})$*.*

These properties imply that the p-adic height induces a symmetric bilinear pairing

$$\langle \cdot, \cdot \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow \mathbb{Q}_p, \quad \langle P, Q \rangle := \frac{1}{2}\big(h_p(P+Q) - h_p(P) - h_p(Q)\big).$$

The p-adic regulator is defined as the discriminant of this pairing on the free part of the Mordell–Weil group $E(\mathbb{Q})$.

[1] In [MST06, Algorithm 3.4], this issue appears to have been overlooked, which led to an incorrect implementation in Sage. This has since been corrected.

In particular, if $E(\mathbb{Q})$ has rank 1 and P generates its free part, then

$$\mathrm{Reg}_p(E/\mathbb{Q}) = \frac{1}{2}\big(h_p(2P) - 2h_p(P)\big) = h_p(P).$$

(Some authors omit the factor $\frac{1}{2}$ in the definition of the regulator. Since we restrict to odd primes, this difference in normalization will not affect our arguments.)

4.4 Algebraic Version of the p-adic BSD Conjecture

In this section, we discuss an algebraic version of the p-adic Birch and Swinnerton-Dyer (BSD) conjecture, which relates the characteristic polynomial $f_E(T)$ to the p-adic regulator. This version is generally more accessible than the analytic formulation, in which $f_E(T)$ is replaced by the p-adic L-function $L_p(E,T)$.

4.5 Rank 0

We begin with the rank 0 case, which is significantly simpler. Throughout this section, we write $A \sim B$ to denote equality up to a p-adic unit.

Theorem 4.2 ([Gre99])**.** *Fix a number field K. Let E/K be an elliptic curve such that $\mathrm{Sel}_{p^\infty}(E/K)$ is finite, and suppose that E has good ordinary reduction at all primes above $p \geq 5$. Then*

$$f_E(0) \sim \frac{\prod_{v \text{ bad}} c_v \cdot \prod_{v|p} N_v^2 \cdot \#Ш(E/K)(p)}{\#E(K)_{\mathrm{tors}}^2}.$$

We record the following observations.

Remark 4.2. *1. By the definition of the characteristic polynomial, we have*

$$f_E(0) \in \mathbb{Z}_p^\times \iff \mu_p(E) = \lambda_p(E) = 0.$$

2. *Assume that* $Ш(E/K)$ *is finite. Then the quantities* $\prod c_v$, $\#Ш(E/K)$, *and* $\#E(K)_{\text{tors}}$ *are finite and independent of* p. *A prime* p *is called* ***anomalous*** *if it divides* N_v *for some* $v \mid p$. *By a standard application of the Chebotarev density theorem, anomalous primes have density zero.*

   It follows that, if $Ш(E/K)$ *is finite, then* $\mu_p = \lambda_p = 0$ *for a set of ordinary primes of density one.*

   More can be said.

   Proposition 4.2 (Greenberg)**.** *Suppose* $E/\mathbb{Q}$ *is* $\mathbb{Q}$*-isogenous to an elliptic curve with non-trivial torsion. Then* $\mu_p = \lambda_p = 0$ *for all but finitely many primes.*

   This is proven in [Gre99, Prop. 5.1], where it is shown that in this situation the set of anomalous primes is finite and can be described explicitly. There are also known examples of elliptic curves for which $\mu_p = \lambda_p = 0$ *for* all *ordinary primes.*

4.6 Positive Rank

We now consider the case where E has positive rank. The following theorem is a natural generalization of Theorem 4.2.

Theorem 4.3 (Perrin-Riou, Schneider)**.** *Let* $E/\mathbb{Q}$ *be an elliptic curve of rank* r_E *with good ordinary reduction at a prime* p. *Suppose:*

1. $Ш(E/\mathbb{Q})(p)$ *is finite;*
2. $\text{Reg}_p(E/\mathbb{Q}) \neq 0$.

Then the characteristic polynomial factors as $f_E(T) = T^{r_E} g(T)$ *with* $g(0) \neq 0$, *and*

$$g(0) \sim \frac{\prod_\ell c_\ell \cdot \#Ш(E/\mathbb{Q})(p) \cdot N_p^2}{\#E(\mathbb{Q})_{\text{tors}}^2} \cdot \frac{\text{Reg}_p(E/\mathbb{Q})}{p^{r_E}}.$$

Note that the right-hand side coincides with that of Theorem 4.2, except for the presence of the (generally non-trivial) p-adic regulator.

Remark 4.3. *1. Since $f_E(T) = T^{r_E} g_E(T)$, we have*

$$g_E(0) \in \mathbb{Z}_p^\times \iff \mu_p(E) = 0 \text{ and } \lambda_p(E) = r_E.$$

If $g_E(0) \notin \mathbb{Z}_p^\times$, then one cannot determine from this alone whether the jump is caused by the μ- or the λ-invariant. However, assuming Greenberg's conjecture, it is expected that the λ-invariant is typically responsible.

2. *When $r_E = 1$, the p-adic regulator is simply the p-adic height $h_p(P)$, where P generates the free part of the Mordell–Weil group. In this case, we will restrict our attention and develop a numerical criterion to determine when*

$$\frac{N_p^2 h_p(P)}{p}$$

is a p-adic unit.

4.7 Main Result

We now state the main result of this section.

Theorem 4.4. *Let $E/\mathbb{Q}$ be an elliptic curve of rank $r = 1$, and let p be a prime of good ordinary reduction. Assume $p \nmid \prod_\ell c_\ell$. Let $P \in E(\mathbb{Q})_{\text{free}}$ be a generator of the free part of the Mordell–Weil group, and take*

$$Q = mP = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \in E^1(\mathbb{Q}_p) \cap E^0(\mathbb{Q}).$$

Then

$$N_p^2 \cdot \frac{\mathrm{Reg}_p}{p} \in \mathbb{Z}_p^\times \iff a^{p-1} \not\equiv 1 \pmod{p^2}.$$

In particular, assume:

1. $p \nmid \prod c_\ell$,
2. $p \nmid \#Ш(E/\mathbb{Q})$,
3. $E(\mathbb{Q})[p] = 0$.

Then

$$\mu_p = 0 \text{ and } \lambda_p = 1 \iff a^{p-1} \not\equiv 1 \pmod{p^2}.$$

Remark 4.4. 1. *The integer m is chosen as in Remark 4.1.*

2. *If p divides $\prod c_\ell$ or $\#Ш(E/\mathbb{Q})$, then Theorem 4.3 implies $\mu_p + \lambda_p > 1$. Conjecturally, such primes occur only finitely often.*

We also need a simple technical lemma.

Lemma 4.1. *Let $z \in \mathbb{Z}_p^\times$ and $N \geq 1$. Then $\log_p z \bmod p^N$ depends only on $z \bmod p^N$. In particular, for $v \in \mathbb{Z}_p^\times$,*

$$v_p(\log_p v) > 1 \iff v^{p-1} \equiv 1 \pmod{p^2}.$$

Proof. See, for example, [Har08, Lemma 8]. □

We now prove the theorem. Throughout, we use the notation and basic properties of Fermat quotients introduced in Section 2.4.

Proof. Let E be given by a Weierstrass model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and let $Q \in E^1(\mathbb{Q}_p) \cap E^0(\mathbb{Q})$. We first claim that

$$z := \frac{\sigma_p(Q)}{d(Q)} \in \mathbb{Z}_p^\times.$$

Indeed, write $Q = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$, and identify Q with $t = -\frac{a}{b}d \in p\mathbb{Z}_p$ via the isomorphism (4.2). Since $Q \in E^1(\mathbb{Q}_p)$, we have $p \mid d := d(Q)$ and $p \nmid a, b$. Using the expansion (4.1), we obtain

$$z = -\frac{a}{b} + \frac{1}{2}a_1 \cdot \frac{a^2}{b^2}d + O(d^2) \in \mathbb{Z}_p^\times. \tag{4.4}$$

Here $O(d^2) \subseteq p^2\mathbb{Z}_p$ since $p \mid d$.

By Lemma 4.1 to determine whether $\frac{h_p(Q)}{p} \in \mathbb{Z}_p^\times$, it suffices to determine whether

$$z^{p-1} \not\equiv 1 \pmod{p^2},$$

or equivalently whether $q_p(z) \neq 0$.

Case 1: $a_1 = 0$**.** From (4.4), we have $z \equiv -\frac{a}{b} \pmod{p^2}$, and hence

$$q_p(z) = q_p\left(\frac{a}{b}\right) = q_p(a) - q_p(b).$$

Since $a_1 = 0$, equation (2.4) gives $q_p(b^2) = q_p(a^3)$, i.e.

$$2q_p(b) = 3q_p(a).$$

Thus

$$q_p(z) = q_p(a) - q_p(b) = q_p(a) - \frac{3}{2}q_p(a) = -\frac{1}{2}q_p(a),$$

so $q_p(z) = 0 \iff q_p(a) = 0$.

Case 2: $a_1 \neq 0$ **and** $Q \in E^2(\mathbb{Q}_p)$**.** Then $p^2 \mid d$, so again $z \equiv -\frac{a}{b} \pmod{p^2}$ and

$$q_p(z) = q_p\left(\frac{a}{b}\right).$$

Moreover, since $p^2 \mid d$, equation (2.4) again reduces to $q_p(b^2) = q_p(a^3)$, hence $2q_p(b) = 3q_p(a)$, and the same computation yields $q_p(z) = -\frac{1}{2}q_p(a)$.

Case 3: $Q \in E^1(\mathbb{Q}_p) \setminus E^2(\mathbb{Q}_p)$**.** That is, $p \mid d$ but $p^2 \nmid d$. Using Lemma 2.1(d) in (4.4) gives

$$q_p(z) = q_p\left(\frac{a}{b}\right) + \frac{1}{2}a_1 \cdot \frac{a}{b} \cdot \frac{d}{p}.$$

On the other hand, rewriting equation (2.4) using Lemma 2.1(d) yields

$$a_1 \cdot \frac{a}{b} \cdot \frac{d}{p} = q_p(b^2) - q_p(a^3).$$

Substituting and using $q_p(b^2) = 2q_p(b)$ and $q_p(a^3) = 3q_p(a)$, we obtain

$$q_p(z) = q_p\left(\frac{a}{b}\right) + \frac{1}{2}\big(2q_p(b) - 3q_p(a)\big) = (q_p(a) - q_p(b)) + q_p(b) - \frac{3}{2}q_p(a) = -\frac{1}{2}q_p(a).$$

Hence $q_p(z) = 0 \iff q_p(a) = 0$.

In all cases, $q_p(z) = 0 \iff q_p(a) = 0$, i.e.

$$z^{p-1} \equiv 1 \pmod{p^2} \iff a^{p-1} \equiv 1 \pmod{p^2}.$$

This concludes the proof. □

4.8 Applications of the Main Theorem

We now present several applications of Theorem 4.4.

1. If the integer a appearing as the numerator of the point $Q = mP$ in the theorem behaves sufficiently randomly, then the heuristic probability that $\mu_p(E) + \lambda_p(E) > 1$ is approximately $\frac{1}{p}$. Equivalently, for a fixed elliptic curve of rank 1, one expects that for a set of ordinary primes of density 1 we have $\mu_p = 0$ and $\lambda_p = 1$. Recall that if $\lambda_p = 1$, then the rank of E remains stable throughout the cyclotomic $\mathbb{Z}_p$-extension.

2. The factor N_p^2 in Theorem 4.3 cancels with the p-adic regulator in Theorem 4.4. Thus, unlike the rank 0 case, it is possible for an ordinary prime p to divide N_p while still having $\mu_p = 0$ and $\lambda_p = 1$.

   For example, consider the elliptic curve $E : y^2 + y = x^3 + x^2$, which has rank 1. Using SageMath [Tea24], one finds that $p = 5$ is a good ordinary prime that does not divide $\mathrm{Tam}(E)$, $\#E(\mathbb{Q})_{\mathrm{tors}}$, or $\#Ш(E/\mathbb{Q})$. Moreover, $N_5 = 10$, yet $\mu_5(E) = 0$ and $\lambda_5(E) = 1$.

3. The explicit nature of the criterion permits large-scale computation, as reflected in Table 4.1 below. The data support the heuristic that $\mu_p = 0$ and $\lambda_p = 1$ with probability $1 - \frac{1}{p}$. Both the code and the results are available at [Foi25].

p	**# Rank 1 Curves Tested**	$\mu_p = 0, \lambda_p = 1$	$\mu_p + \lambda_p > 1$
5	13,517	9,882	3,635
7	17,060	14,085	2,975
11	19,304	17,349	1,955
13	24,953	22,889	2,064
17	24,722	23,201	1,521
23	22,972	22,024	948
29	26,806	25,829	977
31	25,521	24,673	848
43	28,776	28,065	711
47	24,800	24,296	504

Table 4.1: Elliptic curves of rank 1 with ordinary reduction at p and their Iwasawa invariants.

Chapter 5: Iwasawa Theory of Elliptic Curves at Supersingular Primes

We now turn to the supersingular case, which presents several additional difficulties:

1. The Iwasawa module $\mathfrak{X}(E/\mathbb{Q}_\infty)$ is no longer **torsion** as a Λ-module. At first glance, this suggests that it is not even meaningful to attach Iwasawa invariants to the Selmer group.

2. Mazur's Control Theorem fails at supersingular primes.

3. There is no canonical p-adic height taking values in $\mathbb{Q}_p$.

Despite these obstacles, one can still formulate a p-adic BSD conjecture in the supersingular setting, due to Perrin-Riou. Moreover, Pollack introduced signed p-adic L-functions on the analytic side [Pol03], and Kobayashi introduced signed Selmer groups on the algebraic side [Kob03]; together, these constructions allow one to overcome the aforementioned issues.

In this chapter, we develop these ideas and ultimately establish an analogue of Theorem 4.4 in the supersingular setting. Throughout, we assume that $p \geq 5$. In particular, this implies that the trace of Frobenius satisfies $a_p = 0$.

5.1 Dieudonné Module

As noted above, in the supersingular case there is no canonical p-adic height with values in $\mathbb{Q}_p$. Instead, we work with the Dieudonné module D_pE. For our purposes, it suffices to

view D_pE as a 2-dimensional $\mathbb{Q}_p$-vector space generated by ω_E and $\eta := x\omega_E$, where ω_E denotes the invariant differential.

There is an action of Frobenius ϕ on D_pE, with characteristic polynomial $X^2 + \frac{1}{p}$ (since $a_p = 0$ and $p \geq 5$). We write

$$\phi = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}_{(\omega,\eta)}.$$

We record some useful properties of these coefficients from Lemme 2.1 of [PR84].

Proposition 5.1 (Perrin-Riou–Bernardi)**.** *With the above notation:*

1. $\gamma \in \mathbb{Z}_p^\times$,
2. $\alpha \in \mathbb{Z}_p$,
3. $\mathrm{ord}_p(\beta) = -1$.

It turns out that $(\omega, \phi(\omega))$ is also a basis for D_pE. In this basis, Frobenius acts as

$$\phi = \begin{bmatrix} 0 & -\frac{1}{p} \\ 1 & 0 \end{bmatrix}_{(\omega,\phi(\omega))}.$$

A straightforward change-of-basis computation yields

$$(A,B)_{(\omega,\eta)} = \left(A - \frac{\alpha}{\gamma}B, \frac{1}{\gamma}B\right)_{(\omega,\phi(\omega))}. \tag{5.1}$$

5.2 The p-adic Height

Having defined the Dieudonné module D_pE, we now define, for each $v \in D_pE$, a p-adic height function

$$h_v : E(\mathbb{Q}) \to \mathbb{Q}_p,$$

which depends $\mathbb{Q}_p$-linearly on v.

1. For $v = \omega$, define

$$h_\omega(P) = \log_{\hat{E}}^2(P) \tag{5.2}$$

for $P \in E^1(\mathbb{Q}_p)$, where $\log_{\hat{E}}$ denotes the formal group p-adic logarithm associated to E. This definition extends to all of $E(\mathbb{Q})$ by setting $h_\omega(P) := \frac{1}{N_p^2} h_\omega(N_p P)$ for $P \in E(\mathbb{Q}) \setminus E^1(\mathbb{Q}_p)$, noting that $N_p P \in E^1(\mathbb{Q}_p)$ and $p \nmid N_p$.

Under the identification

$$E^1(\mathbb{Q}_p) \xrightarrow{\sim} p\mathbb{Z}_p,$$

which sends $P = (x,y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$ to $t = -\frac{x}{y} = -\frac{a}{b}d$, we obtain the expansion

$$h_\omega(t) = t^2 + a_1 t^3 + O(t^4). \tag{5.3}$$

In particular,

$$\mathrm{ord}_p(h_\omega(P)) \geq 2, \tag{5.4}$$

and

$$\mathrm{ord}_p(h_\omega(P)) > 2 \iff P \in E^2(\mathbb{Q}_p) \iff p^2 \mid d. \tag{5.5}$$

If $P \in E(\mathbb{Q}) \setminus E^1(\mathbb{Q}_p)$ and p is supersingular, the same criterion still applies: indeed,

$$h_\omega(P) = \frac{1}{N_p^2} h_\omega(N_p P),$$

and $p \nmid N_p$.

2. For $v = \eta$, the definition of h_η is analogous to the ordinary case, except that one uses Bernardi's σ-function instead of the ordinary p-adic σ_p-function. More precisely,

for $P \in E(\mathbb{Q})$, choose $m \geq 1$ such that

$$Q := mP = \left(\frac{a}{d^2}, \frac{b}{d^3} \right) \in E^1(\mathbb{Q}_p) \cap E^0(\mathbb{Q}).$$

Then we define

$$h_\eta(P) := \frac{2}{m^2} \log_p \left(\frac{d}{\sigma(Q)} \right) = -\frac{2}{m^2} \log_p \left(\frac{\sigma(Q)}{d} \right),$$

where σ is Bernardi's σ-function attached to the chosen Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and has expansion

$$\sigma(t) = t + \frac{a_1}{2}t^2 + \frac{a_1^2 + a_2}{3}t^3 + \frac{a_1^3 + 2a_1a_2 + 3a_3}{4}t^4 + \cdots.$$

Remark 5.1. *For the proof of Theorem 4.4, we only needed the first two terms of the expansion of σ_p. Since the first two terms of σ and σ_p coincide, the same computation applies to h_η in the supersingular setting.*

3. For $v = a\omega + b\eta \in D_p(E)$, we define

$$h_v := a\,h_\omega + b\,h_\eta.$$

Thus, for each $v \in D_p(E)$, we obtain a quadratic p-adic height on $E(\mathbb{Q})$.

At a supersingular prime there is no distinguished $\mathbb{Q}_p$-valued height, so it is natural to package the family $\{h_v\}_{v \in D_p(E)}$ into a single $D_p(E)$-valued height. Following

[SW13], let $[\ ,\ ] : D_p(E) \times D_p(E) \to \mathbb{Q}_p$ be the alternating pairing normalized by

$$[\omega, \eta] = 1.$$

If $v = a\omega + b\eta \notin \mathbb{Q}_p\omega$, define

$$H_p(P) := \frac{1}{b}\big(h_v(P)\omega - h_\omega(P)v\big) \in D_p(E).$$

Since $h_v = ah_\omega + bh_\eta$, this simplifies to

$$H_p(P) = h_\eta(P)\,\omega - h_\omega(P)\,\eta = (h_\eta(P), -h_\omega(P))_{(\omega,\eta)},$$

so $H_p(P)$ is independent of the auxiliary choice of v. Moreover, for every $v = a\omega + b\eta \in D_p(E)$, one has

$$[H_p(P), v] = a\,h_\omega(P) + b\,h_\eta(P) = h_v(P).$$

In this sense, $H_p(P)$ simultaneously records all the scalar heights $h_v(P)$.

5.3 The p-adic Regulator

The preceding discussion explains the form of the supersingular p-adic regulator. In general, if $\operatorname{rank} E(\mathbb{Q}) = r > 0$, one defines $\operatorname{Reg}_p(E/\mathbb{Q}) \in D_p(E)$ by the property

$$[\operatorname{Reg}_p(E/\mathbb{Q}), v] = \frac{\operatorname{Reg}_v(E/\mathbb{Q})}{[\omega, v]^{r-1}} \qquad (v \notin \mathbb{Q}_p\omega),$$

where $\mathrm{Reg}_v(E/\mathbb{Q})$ denotes the scalar regulator attached to the height h_v; see [SW13, Lemma 4.2]. When $r = 1$ and P generates $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$, we have

$$\mathrm{Reg}_v(E/\mathbb{Q}) = h_v(P),$$

so the above characterization reduces simply to

$$\mathrm{Reg}_p(E/\mathbb{Q}) = H_p(P).$$

Hence, suppressing the dependence on the generator P, we write

$$\mathrm{Reg}_p = (h_\eta, -h_\omega)_{(\omega,\eta)}.$$

Using the change-of-basis formula

$$(A,B)_{(\omega,\eta)} = \left(A - \frac{\alpha}{\gamma}B, \frac{1}{\gamma}B\right)_{(\omega,\phi(\omega))},$$

we obtain

$$\mathrm{Reg}_p = \left(h_\eta + \frac{\alpha}{\gamma}h_\omega, -\frac{1}{\gamma}h_\omega\right)_{(\omega,\phi(\omega))}.$$

This basis is convenient because the Frobenius matrix is

$$\phi = \begin{pmatrix} 0 & -1/p \\ 1 & 0 \end{pmatrix}_{(\omega,\phi(\omega))},$$

and therefore

$$(1-\phi)^2 = \begin{pmatrix} 1-\frac{1}{p} & \frac{2}{p} \\ -2 & 1-\frac{1}{p} \end{pmatrix}_{(\omega,\phi(\omega))}.$$

Applying this matrix to the coordinates of Reg_p gives

$$\begin{aligned}(1-\phi)^2\mathrm{Reg}_p &= \left(\left(1-\frac{1}{p}\right)\left(h_\eta+\frac{\alpha}{\gamma}h_\omega\right)-\frac{2}{p\gamma}h_\omega,\ -2\left(h_\eta+\frac{\alpha}{\gamma}h_\omega\right)-\left(1-\frac{1}{p}\right)\frac{1}{\gamma}h_\omega\right)_{(\omega,\phi(\omega))}\\ &= \left(\frac{(p\gamma-\gamma)h_\eta+(p\alpha-\alpha-2)h_\omega}{p\gamma},\frac{-2p\gamma h_\eta-(2p\alpha+p-1)h_\omega}{p\gamma}\right)_{(\omega,\phi(\omega))}.\end{aligned} \tag{5.6}$$

This is the form that naturally enters Perrin-Riou's supersingular p-adic BSD conjecture.

5.4 The p-adic BSD Conjecture

We now briefly recall the p-adic Birch and Swinnerton-Dyer conjecture in the supersingular case.

Let a_p denote the trace of Frobenius. Then x^2-a_px+p is the characteristic polynomial. For each root α with $\mathrm{ord}_p(\alpha)<1$, one can construct a p-adic L-series $L_p(E,\alpha,T)$ using modular symbols (see [SW13]).

For $p\geq 5$, the characteristic polynomial becomes x^2+p, whose roots α and $\bar{\alpha}$ both satisfy $\mathrm{ord}_p(\alpha)<1$. However, $L_p(E,\alpha,T)$ may fail to have integral coefficients in $\mathbb{Q}_p(\alpha)$. Nevertheless, one can write

$$L_p(E,\alpha,T)=G^+(T)+\alpha G^-(T),\quad G^\pm(T)\in\mathbb{Q}_p[[T]].$$

Perrin-Riou [PR84] defines a vector-valued p-adic L-series with coefficients in $D_p(E)\otimes\mathbb{Q}_p[[T]]$ by

$$L_p(E,T)=\left(G^+(T),-pG^-(T)\right)_{(\omega,\phi(\omega))}. \tag{5.7}$$

The p-adic Birch and Swinnerton-Dyer conjecture, as stated in [BPR93], is as follows.

Conjecture 5.1 (p-adic BSD)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with supersingular reduction at a prime p.*

1. *The order of vanishing of $L_p(E,T)$ at $T=0$ equals the rank $r=\operatorname{rank}E(\mathbb{Q})$.*

2. *The leading term $L_p^*(E,0)$ satisfies*

$$L_p^*(E,0)=\frac{\prod_v c_v\cdot \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\text{tors}})^2}\cdot(1-\phi)^2\cdot\frac{\operatorname{Reg}_p(E/\mathbb{Q})}{p}\in D_p(E). \tag{5.8}$$

Although $G^+(T)$ and $G^-(T)$ may not have integral coefficients, Pollack [Pol03] observed that one can factor out canonical divisors with infinitely many zeros. Using interpolation properties originally explored by Perrin-Riou [PR90], he showed that:

- $G^+(T)$ vanishes at $\zeta_{2n}-1$,
- $G^-(T)$ vanishes at $\zeta_{2n-1}-1$,

where ζ_n denotes a p^n-th root of unity. In particular, both series have infinitely many zeros.

Pollack constructed p-adic power series $\log_p^+(T)$ and $\log_p^-(T)$ vanishing precisely at these points:

$$\log_p^+(T)=\frac{1}{p}\prod_{n\geq 1}\frac{\Phi_{2n}(1+T)}{p}, \tag{5.9}$$

$$\log_p^-(T)=\frac{1}{p}\prod_{n\geq 1}\frac{\Phi_{2n-1}(1+T)}{p}, \tag{5.10}$$

where Φ_n denotes the p^n-th cyclotomic polynomial.

Define the signed p-adic L-functions:

$$L_p^+(E,T):=\frac{G^+(T)}{\log_p^+(T)},\qquad L_p^-(E,T):=\frac{G^-(T)}{\log_p^-(T)}. \tag{5.11}$$

Pollack proved that these power series have bounded coefficients in $\mathbb{Z}_p$ and hence only finitely many zeros. The corresponding Iwasawa invariants $\mu_p^{\pm}$ and $\lambda_p^{\pm}$ are called the *analytic* Iwasawa invariants.

Conjecture 5.2 (Pollack)**.** *For every supersingular prime p, we have*

$$\mu_p^{\pm}(E) = 0.$$

This contrasts with the ordinary setting, where the μ-invariant can be positive.

5.5 Signed Selmer Groups and the Main Conjecture

As before, assume throughout this subsection that p is an odd prime of good supersingular reduction for $E/\mathbb{Q}$ and that $a_p(E) = 0$ (which is automatic for $p \geq 5$). Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension, let $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, and identify

$$\Lambda = \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]].$$

Pollack constructed the signed p-adic L-functions $L_p^{\pm}(E,T) \in \Lambda$ by decomposing the supersingular p-adic L-function as

$$L_p(E,\alpha,T) = L_p^{+}(E,T)\log_p^{+}(T) + \alpha L_p^{-}(E,T)\log_p^{-}(T)$$

[Pol03, Theorem 5.6]. On the algebraic side, Kobayashi defined the signed Selmer groups $\mathrm{Sel}_{p^\infty}^{\pm}(E/\mathbb{Q}_n)$ and $\mathrm{Sel}_{p^\infty}^{\pm}(E/\mathbb{Q}_\infty)$, obtained from the usual Selmer groups by imposing stronger local conditions at p, and proved that

$$X^{\pm}(E/\mathbb{Q}_\infty) := \mathrm{Sel}_{p^\infty}^{\pm}(E/\mathbb{Q}_\infty)^{\vee}$$

is a finitely generated torsion Λ-module [Kob03, Definition 1.1 and Theorem 1.2].

Accordingly, one has *signed* algebraic Iwasawa invariants

$$\mu_p^{\pm,\mathrm{alg}}, \qquad \lambda_p^{\pm,\mathrm{alg}},$$

and *signed* analytic Iwasawa invariants

$$\mu_p^{\pm,\mathrm{an}}, \qquad \lambda_p^{\pm,\mathrm{an}}$$

attached to $L_p^{\pm}(E,T)$; see [Pol03, Definition 6.1]. If $f_E^{\pm}(T) \in \Lambda$ is a characteristic power series of $\mathfrak{X}^{\pm}(E/\mathbb{Q}_\infty)$, the supersingular main conjecture asserts:

Conjecture 5.3 (Main Conjecture)**.**

$$\mathrm{Char}_\Lambda\big(\mathfrak{X}^{\pm}(E/\mathbb{Q}_\infty)\big) = \big(L_p^{\pm}(E,T)\big),$$

Equivalently, this can be written as

$$\big(f_E^{\pm}(T)\big) = \big(L_p^{\pm}(E,T)\big).$$

Pollack and Rubin proved this conjecture for CM elliptic curves [PR04]. For non-CM curves, Kobayashi proved, using Kato's Euler system, the one divisibility

$$\big(L_p^{\pm}(E,T)\big) \subseteq_\Lambda \big(\mathfrak{X}^{\pm}(E/\mathbb{Q}_\infty)\big)$$

for almost all supersingular primes p [Kob03, Theorem 1.3].

The relevant control theorem in the supersingular setting is a *signed* control theorem.

Writing

$$X_n^{\pm} := \mathrm{Sel}_{p^\infty}^{\pm}(E/\mathbb{Q}_n)^\vee, \qquad X_\infty^{\pm} := \mathrm{Sel}_{p^\infty}^{\pm}(E/\mathbb{Q}_\infty)^\vee,$$

Kobayashi proves that the natural maps

$$X_\infty^{\pm}/\omega_n^{\pm} X_\infty^{\pm} \longrightarrow X_n^{\pm}/\omega_n^{\pm} X_n^{\pm}$$

are surjective with finite kernel, bounded independently of n [Kob03, Theorem 9.3].[1]

However, unlike the ordinary case, one should *not* conclude from this that

$$\mathrm{rank}\, E(\mathbb{Q}_n) \leq \lambda_p^{\pm,\mathrm{alg}} \qquad \text{for all } n \geq 0.$$

The correct finite-layer estimate involves *both* signs. More precisely, after passing to the trivial Δ-component of [Kob03, Proposition 10.1 and Corollary 10.2], one obtains

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) + \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n) \leq \lambda_p^{+,\mathrm{alg}} + \lambda_p^{-,\mathrm{alg}} \qquad (n \geq 0).$$

Assuming $Ш(E/\mathbb{Q})[p^\infty]$ is finite, so that

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = \mathrm{rank}\, E(\mathbb{Q}),$$

it follows that

$$\mathrm{rank}\, E(\mathbb{Q}_n) \leq \mathrm{rank}\, E(\mathbb{Q}_\infty) \leq \lambda_p^{+,\mathrm{alg}} + \lambda_p^{-,\mathrm{alg}} - \mathrm{rank}\, E(\mathbb{Q}) \qquad (n \geq 0).$$

[1] Kobayashi formulates Theorem 9.3 over $K_n = \mathbb{Q}(\mu_{p^{n+1}})$; the corresponding statement over $\mathbb{Q}_n$ is obtained by taking the trivial Δ-component. See also [Kim13, Lemma 3.9] for a related control statement in greater generality.

In particular, if

$$\lambda_p^{+,\mathrm{alg}} = \lambda_p^{-,\mathrm{alg}} = \operatorname{rank} E(\mathbb{Q}),$$

then

$$\operatorname{rank} E(\mathbb{Q}_n) = \operatorname{rank} E(\mathbb{Q}) \qquad \text{for all } n \geq 0.$$

Finally, if

$$r_E^{\pm} := \operatorname{ord}_{T=0} f_E^{\pm}(T),$$

then assuming that $Ш(E/\mathbb{Q})$ is finite and that $r_E^{\pm} \leq 1$ one has

$$r_E^{\pm} = \operatorname{rank} E(\mathbb{Q})$$

in the good supersingular case [RS23, Proposition 5.1, Lemma 3.3]. Thus $\lambda_p^{\pm,\mathrm{alg}} \geq \operatorname{rank} E(\mathbb{Q})$, but for $n > 0$ the finite-layer Mordell–Weil rank is controlled by the *sum* of the two signed λ-invariants, not by either one separately.

We stress that the algebraic and analytic signed Iwasawa invariants are *a priori* different. Under the main conjecture, they coincide sign by sign:

$$\mu_p^{\pm,\mathrm{alg}} = \mu_p^{\pm,\mathrm{an}}, \qquad \lambda_p^{\pm,\mathrm{alg}} = \lambda_p^{\pm,\mathrm{an}}.$$

5.6 Main Result

We are now ready to state and prove the main result of this section.

Theorem 5.1. *Let E be an elliptic curve over $\mathbb{Q}$ of rank 1, and let p be a prime of supersingular reduction. Assume that E is given by a minimal model. Let P be a generator of*

the free part of the Mordell–Weil group and let m be the smallest positive integer such that

$$Q := m \cdot P = \left(\frac{a}{d^2}, \frac{b}{d^3} \right) \in E^1(\mathbb{Q}_p) \cap E^0(\mathbb{Q}).$$

Assume that $p \nmid \prod_v c_v$, $p \nmid \#Ш(E/\mathbb{Q})$, and that Conjecture 5.1 holds.

Let

$$q_p(u) := \frac{u^{p-1} - 1}{p} \qquad (u \in \mathbb{Z}_p^\times),$$

and write the Frobenius action on D_pE in the basis $(\omega_E, x\omega_E)$ as

$$\varphi = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}_{(\omega_E, x\omega_E)}.$$

Then $\gamma \in \mathbb{Z}_p^\times$, and the following hold:

1. $$\mu_p^{+,\mathrm{an}}(E) + \lambda_p^{+,\mathrm{an}}(E) = 1 \iff a^{p-1} \not\equiv 1 \pmod{p^2}.$$

2. $$\mu_p^{-,\mathrm{an}}(E) + \lambda_p^{-,\mathrm{an}}(E) = 1 \iff 2\gamma q_p(a) + a^{-1} \left(\frac{d}{p} \right)^2 \not\equiv 0 \pmod{p}.$$

3. *In particular, if*

$$\mu_p^{+,\mathrm{an}}(E) + \lambda_p^{+,\mathrm{an}}(E) > 1 \qquad \textit{(equivalently, } a^{p-1} \equiv 1 \pmod{p^2}\textit{)},$$

then

$$\mu_p^{-,\mathrm{an}}(E) + \lambda_p^{-,\mathrm{an}}(E) = 1 \iff d \not\equiv 0 \pmod{p^2}.$$

Proof. The strategy is conceptually straightforward, though it requires some care in the

computations. We relate the Iwasawa invariants $\mu^{\pm}$ and $\lambda^{\pm}$ to the power series $G^{\pm}$. The p-adic BSD conjecture then links the leading terms of $G^{\pm}$ to the p-adic regulator. To simplify notation, we write $\mu_p^{\pm}$ and $\lambda_p^{\pm}$ in place of $\mu_p^{\pm,\mathrm{an}}(E)$ and $\lambda_p^{\pm,\mathrm{an}}(E)$, respectively.

Write

$$G^+(T) = g_0^+ + g_1^+ T + O(T^2), \qquad G^-(T) = g_0^- + g_1^- T + O(T^2),$$

with $g_i^{\pm} \in \mathbb{Q}_p$.

Lemma 5.1. *The signed p-adic L-functions admit the expansions*

$$L_p^+(T) = pg_0^+ + \left(pg_1^+ + \frac{p^2 g_0^+}{2(p+1)} \right) T + O(T^2),$$

$$L_p^-(T) = pg_0^- + \left(pg_1^- + \frac{pg_0^-}{2(p+1)} \right) T + O(T^2).$$

Proof. From the product expansion

$$\frac{\Phi_r(1+T)}{p} = 1 + \frac{p^{r-1}(p-1)}{2} T + O(T^2),$$

we compute

$$\prod_{n\geq 1} \frac{\Phi_{2n}(1+T)}{p} = 1 - \frac{p}{2(p+1)} T + O(T^2), \qquad \prod_{n\geq 1} \frac{\Phi_{2n-1}(1+T)}{p} = 1 - \frac{1}{2(p+1)} T + O(T^2).$$

If $h(T) = h_0 + h_1 T + \cdots$, then

$$\frac{1}{h(T)} = \frac{1}{h_0} - \frac{h_1}{h_0^2} T + \cdots.$$

Applying this to the definitions of $L_p^{\pm}$, the result follows. □

Corollary 5.1. *Assume that E has rank 1 and that p is supersingular. Under Conjecture 5.1, we have*

$$\mu_p^{\pm} + \lambda_p^{\pm} = 1 \iff \mathrm{ord}_p(g_1^{\pm}) = -1.$$

Proof. Since $\mathrm{rank}\, E(\mathbb{Q}) = 1$, we have $g_0^{\pm} = 0$. The claim now follows from Lemma 5.1. □

Now assume that $p \nmid \prod c_v$ and $p \nmid \#Ш(E/\mathbb{Q})$. Since p is supersingular, we also have $p \nmid \#E(\mathbb{Q})_{tors}$. Therefore Equation (5.8) implies that

$$(g_1^+, -pg_1^-)_{(\omega,\phi(\omega))} \sim (1-\phi)^2 \cdot \frac{\mathrm{Reg}_p(E/\mathbb{Q})}{p}$$

up to a p-adic unit.

Using Equation 5.6, we obtain

$$(1-\phi)^2 \cdot \frac{\mathrm{Reg}_p}{p} = \left(\frac{(p-1)\gamma h_\eta + \big((p-1)\alpha - 2\big)h_\omega}{p^2\gamma}, \frac{-2p\gamma h_\eta - \big(2p\alpha + p - 1\big)h_\omega}{p^2\gamma} \right)_{(\omega,\phi(\omega))}.$$

By Corollary 5.1, the condition detected by the above computation is

$$\mu_p^{\pm} + \lambda_p^{\pm} = 1 \iff \mathrm{ord}_p(g_1^{\pm}) = -1.$$

Since $\gamma \in \mathbb{Z}_p^\times$, $\alpha \in \mathbb{Z}_p$, and

$$\mathrm{ord}_p(h_\omega(Q)) \geq 2, \qquad \mathrm{ord}_p(h_\eta(Q)) \geq 1,$$

the first coordinate shows that

$$\mu_p^+ + \lambda_p^+ = 1 \iff \mathrm{ord}_p(g_1^+) = -1 \iff \mathrm{ord}_p(h_\eta(Q)) = 1.$$

Now let

$$z := \frac{\sigma(Q)}{d(Q)}.$$

Since Bernardi's sigma has expansion

$$\sigma(t) = t + \frac{a_1}{2}t^2 + O(t^3),$$

and $t = -x(Q)/y(Q) = -ad/b$, we have

$$z = -\frac{a}{b} + \frac{a_1}{2}\frac{a^2}{b^2}d + O(d^2) \in \mathbb{Z}_p^\times.$$

Thus the same calculation as in the proof of Theorem 4.4 gives

$$q_p(z) = -\frac{1}{2}q_p(a).$$

By definition of the supersingular height,

$$h_\eta(Q) = 2\log_p\left(\frac{d(Q)}{\sigma(Q)}\right) = -2\log_p(z).$$

Since for every $u \in \mathbb{Z}_p^\times$,

$$\frac{\log_p(u)}{p} \equiv -q_p(u) \pmod{p},$$

we deduce that

$$\frac{h_\eta(Q)}{p} = -2\frac{\log_p(z)}{p} \equiv 2q_p(z) \equiv -q_p(a) \pmod{p}.$$

Hence

$$\mathrm{ord}_p(h_\eta(Q)) = 1 \iff q_p(a) \neq 0 \iff a^{p-1} \not\equiv 1 \pmod{p^2}.$$

For the minus part, one can proceed without imposing any hypothesis on the plus part. Indeed,

$$\mu_p^- + \lambda_p^- = 1 \iff \operatorname{ord}_p(g_1^-) = -1 \iff \operatorname{ord}_p(-pg_1^-) = 0.$$

Using the second coordinate of (5.8) together with (5.6), we obtain

$$-pg_1^- \sim -\frac{2p\gamma h_\eta(Q) + (2p\alpha + p - 1)h_\omega(Q)}{p^2\gamma}.$$

Since $\gamma \in \mathbb{Z}_p^\times$, $\alpha \in \mathbb{Z}_p$, and

$$\operatorname{ord}_p(h_\omega(Q)) \geq 2, \qquad \operatorname{ord}_p(h_\eta(Q)) \geq 1,$$

it follows that

$$\mu_p^- + \lambda_p^- > 1 \iff 2\gamma\frac{h_\eta(Q)}{p} + (2p\alpha + p - 1)\frac{h_\omega(Q)}{p^2} \equiv 0 \pmod{p}.$$

Next, write

$$t = -\frac{x(Q)}{y(Q)} = -\frac{ad}{b}.$$

By (5.5),

$$h_\omega(Q) = t^2 + a_1 t^3 + O(t^4).$$

Since $Q \in E_1(\mathbb{Q}_p)$, we have $p \mid d$, hence

$$\frac{h_\omega(Q)}{p^2} \equiv \left(\frac{t}{p}\right)^2 = \left(\frac{ad}{bp}\right)^2 \pmod{p}.$$

Reducing the Weierstrass equation modulo p and using $p \mid d$ gives

$$b^2 \equiv a^3 \pmod{p},$$

so

$$\frac{h_\omega(Q)}{p^2} \equiv a^{-1}\left(\frac{d}{p}\right)^2 \pmod{p}.$$

Substituting these congruences into the criterion above, and using

$$2p\alpha + p - 1 \equiv -1 \pmod{p},$$

we obtain

$$\mu_p^- + \lambda_p^- > 1 \iff -2\gamma q_p(a) - a^{-1}\left(\frac{d}{p}\right)^2 \equiv 0 \pmod{p}.$$

Equivalently,

$$\mu_p^- + \lambda_p^- = 1 \iff 2\gamma q_p(a) + a^{-1}\left(\frac{d}{p}\right)^2 \not\equiv 0 \pmod{p}.$$

In particular, if

$$\mu_p^+ + \lambda_p^+ > 1,$$

then $q_p(a) = 0$, and the above criterion simplifies to

$$\mu_p^- + \lambda_p^- = 1 \iff a^{-1}\left(\frac{d}{p}\right)^2 \not\equiv 0 \pmod{p} \iff p^2 \nmid d.$$

This proves Theorem 5.1. □

5.7 Generalized Wieferich Primes and Computations

The numerical criterion obtained in the previous section for the minus part is reminiscent of the classical notion of Wieferich primes.

Silverman [Sil88] introduces the following definition.

Definition 5.1 (Silverman [Sil88, Def., p. 227])**.** *Let $A/\mathbb{Q}$ be a commutative algebraic*

group and let $P \in A(\mathbb{Q})$ be a point of infinite order. Fix a model $\mathscr{A}/\mathbb{Z}$ with generic fibre A and let $U \subset \mathrm{Spec}(\mathbb{Z})$ be a non-empty open subscheme over which $\mathscr{A}$ is a group scheme. For each prime $p \in U$, set

$$N_p := \#\mathscr{A}(\mathbb{Z}/p\mathbb{Z}),$$

and let O denote the identity section of $\mathscr{A}$. A set of non-Wieferich primes *for (A,P) is a set of the form*

$$W_{A,P} := \{\, p \in U : N_p P \not\equiv O \pmod{p^2} \,\},$$

where the congruence is taken in $\mathscr{A}(\mathbb{Z}/p^2\mathbb{Z})$ via reduction modulo p^2.

Remark 5.2. *Although $W_{A,P}$ depends on the choice of the model $\mathscr{A}/\mathbb{Z}$, any two such sets differ by only finitely many primes.*

When $A = \mathbb{G}_m$, this recovers the classical notion

$$W_{\mathbb{G}_m,a} = \{p : a^{p-1} \not\equiv 1 \mod p^2\}.$$

When $A = E$ is an elliptic curve of rank 1 and P is a generator of the free part of the Mordell–Weil group, we have

$$W_{E,P} = \{p : N_p P \in E^1(\mathbb{Q}_p) \setminus E^2(\mathbb{Q}_p)\} = \{p : p^2 \nmid d_{N_p}\},$$

where $N_p P = \left(\frac{a_{N_p}}{d_{N_p}^2}, \frac{b_{N_p}}{d_{N_p}^3}\right)$. This is precisely the set that appears in Theorem 5.1. Similarly, we can define

$$\Lambda_{E,P} := \{p : a_{N_p}^{p-1} \not\equiv 1 \mod p^2\}.$$

It would be interesting to find a more conceptual expression for $\Lambda_{E,P}$, analogous to Definition 5.1.

Silverman proves that the ABC conjecture implies that $W_{E,P}$ is infinite. Conjecturally,

$W_{E,P}$ has density 1, and its complement is infinite. The simple heuristic reasoning, adapted to our case, is as follows:

If the sequences $\{a_{N_p}\}$ and $\{d_{N_p}\}$ behave sufficiently randomly as N_p varies, then the probability that $q_p(a_{N_p}) = 0$ is roughly $\frac{1}{p}$. Consequently, the complement of $\Lambda_{E,P}$ should be infinite and of density 0. Similarly, the probability that $p^2 \mid d_{N_p}$ is also about $\frac{1}{p}$. Thus, the probability that both events occur simultaneously is approximately $\frac{1}{p^2}$, suggesting that their intersection is finite. As is the case for classical Wieferich primes, such heuristics are out of reach of current techniques, and it is even an open question to prove that $\Lambda_{E,P}$ and $W_{E,P}$ are non-empty. However, all the computational evidence supports these predictions, as illustrated in Table 5.1 below.

Overall, the above heuristics can be summarized in the following conjecture.

Conjecture 5.4. *Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E^0(\mathbb{Q})$ be a non-torsion point. Then:*

1. *$\Lambda_{E,P}$ has density 1 and its complement is infinite.*
2. *$W_{E,P}$ has density 1 and its complement is infinite.*
3. *For any elliptic curve $E/\mathbb{Q}$ of rank 1, the rank of the elliptic curve remains stable in the cyclotomic $\mathbb{Z}_p$-extension for density one of the primes p.*

These conjectures agree with the conjectures found in [Wut04, Conj 1] and [KR21, Conj 3.17].

We conclude with a table of Iwasawa invariants for elliptic curves of rank 1 with supersingular reduction at p, computed using [Tea24]. Conjecturally, one expects $\mu_p^{\pm} = 0$ for all supersingular primes p. The code and data can be found at [Foi25].

p	**Total # of Elliptic Curves Tested**	$\lambda^+ > 1$	$\lambda^+ > 1$ and $\lambda^- > 1$
5	4427	856	109
7	5146	670	57
11	6777	592	28
13	2185	168	9
17	3533	201	8
19	3764	174	11
23	6252	285	5

Table 5.1: Elliptic curves with supersingular reduction at p and their $\lambda^{\pm}$ invariants.

Chapter 6: The Index $[E(\mathbb{Q}) : E^0(\mathbb{Q})]$ in Non-Minimal Weierstrass Models

In the construction of the ordinary p-adic height, it is important to ensure that for any point $P \in E(\mathbb{Q})$ one can find an integer m such that $mP \in E^0(\mathbb{Q})$. As noted earlier, if E is given by a *global minimal* Weierstrass model, then the choice $m = \prod_\ell c_\ell$ works automatically, where

$$c_\ell := [E(\mathbb{Q}_\ell) : E^0(\mathbb{Q}_\ell)]$$

is the local Tamagawa number at ℓ (and $c_\ell = 1$ for primes of good reduction). However, if the model is not minimal, then the local index $[E(\mathbb{Q}_\ell) : E^0(\mathbb{Q}_\ell)]$ generally changes.

In this chapter, we study how the local index $[E(\mathbb{Q}_\ell) : E^0(\mathbb{Q}_\ell)]$ varies under changes of Weierstrass models. This allows us to compute a constant C_E such that $C_E P \in E^0(\mathbb{Q})$ for all $P \in E(\mathbb{Q})$. We note, for example, that the short Weierstrass model is typically not minimal, which illustrates the relevance of this analysis. For computational purposes, we also describe a more efficient algorithm which, for a fixed point P, produces an integer m such that $mP \in E^0(\mathbb{Q})$. Although this m depends on P, it is typically smaller than C_E and is often more efficient in practice.

Throughout this section, we fix a prime p and write $v_p := \mathrm{ord}_p$ for the normalized p-adic valuation.

6.1 Division Polynomials

Let $P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \in E(\mathbb{Q})$. For any integer $n \geq 1$, we write

$$nP = \left(\frac{a_n}{d_n^2}, \frac{b_n}{d_n^3}\right) = \left(\frac{g_n}{f_n^2}, \frac{\omega_n}{f_n^3}\right) = \left(\frac{\hat{g}_n}{d^2\hat{f}_n^2}, \frac{\hat{\omega}_n}{d^3\hat{f}_n^3}\right),$$

where f_n, g_n, ω_n are the usual division polynomials (see [Sil86, Exercise 3.7]). When no ambiguity arises, we suppress the dependence on P and simply write f_n, g_n, etc.

We need the following well-known result (see [CH98, Lemma 1]).

Lemma 6.1. *Let $P \in E^1(\mathbb{Q}_p)$, written as $P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$. Then*

$$v_p(d_n) = v_p(d) + v_p(n).$$

The next proposition is central and can be found in [Aya92, Theorem A].

Proposition 6.1. *Let $P \in E(\mathbb{Q}_p) \setminus E^1(\mathbb{Q}_p)$. The following are equivalent:*

1. $v_p(f_2(P)), v_p(f_3(P)) > 0$.
2. $v_p(f_n(P)) > 0$ *for all* $n \geq 2$.
3. *There exists* $m_0 \geq 2$ *such that* $v_p(f_{m_0}(P)), v_p(f_{m_0+1}(P)) > 0$.
4. *There exists* $n_0 \geq 2$ *such that* $v_p(f_{n_0}(P)), v_p(g_{n_0}(P)) > 0$.
5. $P \notin E^0(\mathbb{Q}_p)$.

Remark 6.1. *From the proof of Proposition 6.1, it follows that if $P \notin E^0(\mathbb{Q}_p)$ then (3) and (4) hold for every $m_0, n_0 \geq 2$.*

Define

$$u_n(P) := \frac{d(P)^{n^2} f_n(P)}{d(nP)},$$

called the **cancellation term**. We will use the following refinement.

Proposition 6.2. *Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\mathbb{Q})$. Then for any $n \geq 2$,*

$$P \in E^0(\mathbb{Q}_p) \iff u_n(P) \in \mathbb{Z}_p^\times.$$

Proof. The forward direction appears in [Wut04, Proposition 1]. For the converse, suppose that $P \notin E^0(\mathbb{Q}_p)$ and write $P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$ in lowest terms. Then necessarily $v_p(d) = 0$.

Fix $n \geq 2$. By Proposition 6.1 and the remark following it, we have $v_p(f_n(P)) > 0$ and $v_p(g_n(P)) > 0$.

If $nP \notin E^1(\mathbb{Q}_p)$, then $v_p(d(nP)) = 0$, hence

$$v_p(u_n(P)) = v_p\big(d(P)^{n^2} f_n(P)\big) - v_p(d(nP)) = v_p(f_n(P)) > 0.$$

If $nP \in E^1(\mathbb{Q}_p)$, write

$$nP = \left(\frac{a_n}{d_n^2}, \frac{b_n}{d_n^3}\right)$$

in lowest terms. Since $v_p(d_n) > 0$ and $\gcd(a_n, d_n) = 1$, we have $p \nmid a_n$, and thus

$$v_p(x(nP)) = v_p\left(\frac{a_n}{d_n^2}\right) = -2v_p(d_n).$$

On the other hand,

$$x(nP) = \frac{g_n(P)}{f_n(P)^2}.$$

Since $v_p(d) = 0$, the factor d^{n^2} is a p-adic unit, hence

$$v_p(u_n(P)) = v_p(f_n(P)) - v_p(d_n) \qquad \text{and in particular} \qquad v_p(f_n(P)) = v_p(d_n) + v_p(u_n(P)).$$

Substituting into

$$v_p(x(nP)) = v_p(g_n(P)) - 2v_p(f_n(P))$$

gives

$$-2v_p(d_n) = v_p(g_n(P)) - 2\big(v_p(d_n) + v_p(u_n(P))\big),$$

so $v_p(g_n(P)) = 2v_p(u_n(P))$. Since $v_p(g_n(P)) > 0$, it follows that $v_p(u_n(P)) > 0$, i.e. $u_n(P) \notin \mathbb{Z}_p^\times$. □

By taking all primes p into account, we recover Proposition 6.3, which we recall here for convenience.

Proposition 6.3. *Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\mathbb{Q})$ be given by*

$$P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right), \quad d(P) := d.$$

Then for any $n \geq 2$,

$$P \in E^0(\mathbb{Q}) \quad \Longleftrightarrow \quad d(nP) = \left| d(P)^{n^2} f_n(P) \right|.$$

Remark 6.2. *In practice, this provides an efficient algorithm that given a point $P \in E(\mathbb{Q})$, produces the smallest integer m such that $mP \in E^0(\mathbb{Q})$: simply compute $d(2mP)$ and $d(mP)^4 f_2(mP)$ for increasing values of m until they are equal. The downside is that this algorithm depends on P. Our goal in the next subsections is to find a single universal constant C_E that works for all points in $E(\mathbb{Q})$.*

6.2 Change of Coordinates

Let $E/\mathbb{Q}$ be an elliptic curve in Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We use the convention that a change of coordinates $[u,r,s,t]$ sends a point (x,y) on E to a point (x',y') on a new model E' via

$$x' = u^2x + r, \qquad y' = u^3y + u^2sx + t.$$

Since $[u,r,s,t] = [u,0,0,0] \circ [1,r,s,t]$ and $[1,r,s,t]$ does not affect the discriminant, it suffices for our purposes to study changes of the form $[u,0,0,0]$, which we write as $(x,y) \mapsto (u^2x, u^3y)$.

Fix a prime p, and let $v := v_p$ denote the p-adic valuation. Then:

Corollary 6.1. *Let $[u,0,0,0]\colon E \to E'$ be a change of coordinates. Then:*

1. $\Delta' = u^{12}\Delta$. *In particular, if $u = p^r$, then $r = \frac{v(\Delta') - v(\Delta)}{12}$.*
2. $a_i' = u^i a_i$ *for each i.*
3. $f_2'(P') = u^3 f_2(P)$ *and* $f_3'(P') = u^8 f_3(P)$, *where* $P' = [u,0,0,0](P)$.

Proof. Parts (1) and (2) follow directly from the definitions. For (3), recall the explicit formulas

$$f_2(x,y) = 2y + a_1x + a_3, \qquad f_3(x,y) = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$$

where b_2, b_4, b_6, b_8 are the usual polynomials in the a_i (cf. Silverman). Substituting $x' = u^2x$, $y' = u^3y$, and $a_i' = u^i a_i$ gives the claim. □

6.3 Main Result

We now state the main theorem of this section.

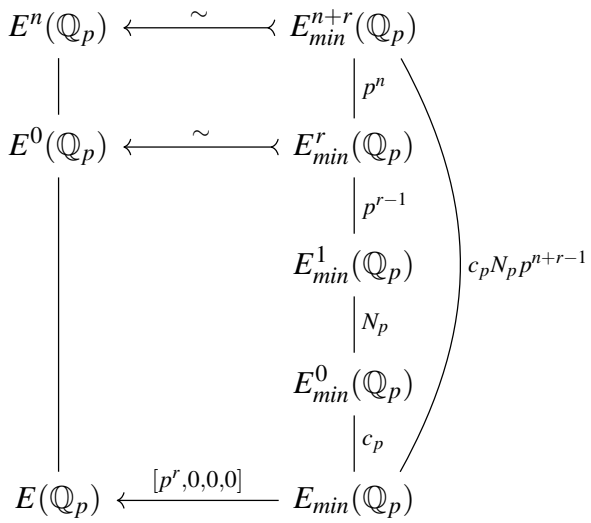
Theorem 6.1. *Let $r \geq 0$ and let $[p^r,0,0,0]\colon E \to E'$ be a change of coordinates. Then for all $i \geq 0$,*

$$E^{r+i}(\mathbb{Q}_p) \cong (E')^i(\mathbb{Q}_p).$$

In particular,

$$[E(\mathbb{Q}_p) : E^r(\mathbb{Q}_p)] = [E'(\mathbb{Q}_p) : (E')^0(\mathbb{Q}_p)].$$

We summarize Theorem 6.1 in the following diagram.



Proof. Let $\phi\colon E(\mathbb{Q}_p) \xrightarrow{\sim} E'(\mathbb{Q}_p)$ be the isomorphism induced by $[p^r,0,0,0]$, so that $\phi(x,y) = (p^{2r}x, p^{3r}y)$. Write $v := v_p$.

How f_2 and f_3 transform: If $P \in E(\mathbb{Q}_p)$ and $P' = \phi(P)$, then Corollary 6.1 gives

$$v\big(f_2'(P')\big) = 3r + v\big(f_2(P)\big), \tag{6.1}$$

$$v\big(f_3'(P')\big) = 8r + v\big(f_3(P)\big). \tag{6.2}$$

Valuation of f_2 and f_3 on $E^1(\mathbb{Q}_p)$: If $P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \in E^1(\mathbb{Q}_p)$, then Lemma 6.1 gives $v(d_m) = v(d) + v(m)$. Since $P \in E^1(\mathbb{Q}_p) \subseteq E^0(\mathbb{Q}_p)$, Proposition 6.2 implies $u_m(P) \in \mathbb{Z}_p^\times$, hence

$$v\big(f_m(P)\big) = v(d_m) - m^2 v(d) = (1-m^2)v(d) + v(m). \tag{6.3}$$

In particular,

$$v\big(f_2(P)\big) = -3v(d) + v(2) = \begin{cases} -3v(d), & p \neq 2, \\ -3v(d)+1, & p = 2, \end{cases} \tag{6.4}$$

and

$$v\big(f_3(P)\big) = -8v(d) + v(3) = \begin{cases} -8v(d), & p \neq 3, \\ -8v(d)+1, & p = 3. \end{cases} \tag{6.5}$$

The case $i = 0$: We claim that ϕ restricts to an isomorphism $E^r(\mathbb{Q}_p) \xrightarrow{\sim} (E')^0(\mathbb{Q}_p)$.

(i) If $P \in E^r(\mathbb{Q}_p)$ then $P' = \phi(P) \in (E')^0(\mathbb{Q}_p)$. Indeed, $P \in E^r(\mathbb{Q}_p)$ implies $P \in E^1(\mathbb{Q}_p)$ and $v(d(P)) \geq r$. Hence (6.4)–(6.5) give

$$v\big(f_2(P)\big) \leq -3r + v(2), \qquad v\big(f_3(P)\big) \leq -8r + v(3).$$

Using (6.1)–(6.2), we obtain

$$v\big(f_2'(P')\big) \leq v(2), \qquad v\big(f_3'(P')\big) \leq v(3).$$

In particular, at least one of $v(f_2'(P'))$ and $v(f_3'(P'))$ is ≤ 0 (namely f_2' if $p \neq 2$, and f_3' if $p = 2$). By Proposition 6.1, a point fails to lie in $(E')^0(\mathbb{Q}_p)$ only if both $v(f_2')$ and $v(f_3')$ are strictly positive; hence $P' \in (E')^0(\mathbb{Q}_p)$.

(ii) If $P' \in (E')^0(\mathbb{Q}_p)$ then $P = \phi^{-1}(P') \in E^r(\mathbb{Q}_p)$. If $r = 0$ there is nothing to prove, so assume $r \geq 1$ and set $P = \phi^{-1}(P')$. Since $P' \in (E')^0(\mathbb{Q}_p)$, Proposition 6.1 implies that at least one of $v(f_2'(P'))$ and $v(f_3'(P'))$ is ≤ 0. Using (6.1)–(6.2) in reverse, this gives

$$v\big(f_2(P)\big) \leq -3r \quad \text{or} \quad v\big(f_3(P)\big) \leq -8r,$$

and in particular at least one of $v(f_2(P))$, $v(f_3(P))$ is *negative*. But if $P \notin E^1(\mathbb{Q}_p)$, then $v(d(P)) = 0$ and $x(P), y(P) \in \mathbb{Z}_p$, so $f_2(P), f_3(P) \in \mathbb{Z}_p$ and hence $v(f_2(P)), v(f_3(P)) \geq 0$, a contradiction. Thus $P \in E^1(\mathbb{Q}_p)$, and now (6.4)–(6.5) imply $v(d(P)) \geq r$. Equivalently, $P \in E^r(\mathbb{Q}_p)$.

Combining (i) and (ii), we obtain $\phi\big(E^r(\mathbb{Q}_p)\big) = (E')^0(\mathbb{Q}_p)$, hence $E^r(\mathbb{Q}_p) \cong (E')^0(\mathbb{Q}_p)$.

The case $i \geq 1$: For $i \geq 1$, we have $E^{r+i}(\mathbb{Q}_p) \subseteq E^1(\mathbb{Q}_p)$. Let $t = -x/y$ be the standard formal parameter at O. Under $\phi = [p^r, 0, 0, 0]$ one has $t(P') = p^{-r} t(P)$ whenever $P \in E^1(\mathbb{Q}_p)$. Hence $t(P) \in p^{r+i}\mathbb{Z}_p$ if and only if $t(P') \in p^i \mathbb{Z}_p$, which yields $E^{r+i}(\mathbb{Q}_p) \cong (E')^i(\mathbb{Q}_p)$ for all $i \geq 1$.

The final index identity follows immediately from the case $i = 0$. □

Corollary 6.2. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$ given in a **short** Weierstrass model, with $A, B \in \mathbb{Z}$, and let $E_{\min}/\mathbb{Q}$ be a global minimal model of E. Assume that the given short model is ℓ-minimal for every prime $\ell \geq 5$ (equivalently, $v_\ell(\Delta(E)) = v_\ell(\Delta(E_{\min}))$ for all $\ell \geq 5$). For $p \in \{2, 3\}$, write*

$$r_p := \frac{v_p(\Delta(E)) - v_p(\Delta(E_{\min}))}{12} \in \mathbb{Z}_{\geq 0}.$$

Set

$$m := \operatorname{lcm}\big(N_2(E_{\min}) \cdot 2^{\max(r_2 - 1, 0)},\ N_3(E_{\min}) \cdot 3^{\max(r_3 - 1, 0)}\big).$$

Then for every $P \in E(\mathbb{Q})$ one has

$$(m \cdot \mathrm{Tam}(E))\, P \in E^0(\mathbb{Q}).$$

Remark 6.3. *If $r_2, r_3 \in \{0,1\}$ (for example, for the usual integral short Weierstrass model), then*

$$m = \mathrm{lcm}(N_2(E_{\min}), N_3(E_{\min})).$$

Proof. For each prime ℓ, set

$$G_\ell := E(\mathbb{Q}_\ell)/E^0(\mathbb{Q}_\ell).$$

The diagonal embedding $E(\mathbb{Q}) \hookrightarrow \prod_\ell E(\mathbb{Q}_\ell)$ induces a homomorphism

$$E(\mathbb{Q}) \longrightarrow \prod_\ell G_\ell,$$

whose kernel is exactly

$$E^0(\mathbb{Q}) = E(\mathbb{Q}) \cap \bigcap_\ell E^0(\mathbb{Q}_\ell).$$

Hence

$$E(\mathbb{Q})/E^0(\mathbb{Q}) \hookrightarrow \prod_\ell G_\ell.$$

Moreover, all but finitely many G_ℓ are trivial.

For primes $\ell \geq 5$, the hypothesis that the short model is ℓ-minimal implies that E and $E_{\min}$ are related over $\mathbb{Z}_\ell$ by a change of variables with $u \in \mathbb{Z}_\ell^\times$. Such a change of variables is an isomorphism of Weierstrass models over $\mathbb{Z}_\ell$, hence it identifies the nonsingular loci of the special fibers. Therefore

$$\#G_\ell = [E(\mathbb{Q}_\ell) : E^0(\mathbb{Q}_\ell)] = [E_{\min}(\mathbb{Q}_\ell) : E^0_{\min}(\mathbb{Q}_\ell)] = c_\ell \qquad (\ell \geq 5).$$

Now fix $p \in \{2,3\}$. Since E and $E_{\min}$ are isomorphic over $\mathbb{Q}_p$, there is a p-adic change of variables

$$[u,r,s,t]\colon E_{\min} \to E.$$

Because $\Delta(E) = u^{12}\Delta(E_{\min})$, we have

$$v_p(u) = \frac{v_p(\Delta(E)) - v_p(\Delta(E_{\min}))}{12} = r_p.$$

Write

$$u = p^{r_p}u_0, \qquad u_0 \in \mathbb{Z}_p^{\times},$$

and let E_p' be the model obtained from $E_{\min}$ by the scaling

$$[p^{r_p},0,0,0]\colon E_{\min} \to E_p'.$$

Then

$$[u,r,s,t] = [u_0,r,s,t] \circ [p^{r_p},0,0,0].$$

The map

$$[u_0,r,s,t]\colon E_p' \to E$$

is defined over $\mathbb{Z}_p$ and has unit scaling factor u_0, so it is an isomorphism of Weierstrass models over $\mathbb{Z}_p$. In particular, it identifies $(E_p')^0(\mathbb{Q}_p)$ with $E^0(\mathbb{Q}_p)$. Therefore

$$[E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)] = [E_p'(\mathbb{Q}_p) : (E_p')^0(\mathbb{Q}_p)].$$

Applying Theorem 6.1 to the scaling

$$[p^{r_p},0,0,0]\colon E_{\min} \to E_p',$$

we obtain

$$[E'_p(\mathbb{Q}_p) : (E'_p)^0(\mathbb{Q}_p)] = [E_{\min}(\mathbb{Q}_p) : E^{r_p}_{\min}(\mathbb{Q}_p)].$$

Hence

$$\#G_p = [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)] = [E_{\min}(\mathbb{Q}_p) : E^{r_p}_{\min}(\mathbb{Q}_p)].$$

If $r_p = 0$, then

$$\#G_p = [E_{\min}(\mathbb{Q}_p) : E^0_{\min}(\mathbb{Q}_p)] = c_p.$$

If $r_p \geq 1$, then

$$[E_{\min}(\mathbb{Q}_p) : E^{r_p}_{\min}(\mathbb{Q}_p)] = [E_{\min}(\mathbb{Q}_p) : E^0_{\min}(\mathbb{Q}_p)]\,[E^0_{\min}(\mathbb{Q}_p) : E^1_{\min}(\mathbb{Q}_p)]\,[E^1_{\min}(\mathbb{Q}_p) : E^{r_p}_{\min}(\mathbb{Q}_p)].$$

The first factor is c_p, the second factor is

$$[E^0_{\min}(\mathbb{Q}_p) : E^1_{\min}(\mathbb{Q}_p)] = \#\widetilde{E}_{\min,\mathrm{ns}}(\mathbb{F}_p) = N_p(E_{\min}),$$

and the third factor is p^{r_p-1}, since each successive quotient

$$E^n_{\min}(\mathbb{Q}_p)/E^{n+1}_{\min}(\mathbb{Q}_p) \qquad (n \geq 1)$$

has order p. Thus

$$\#G_p = \begin{cases} c_p, & r_p = 0, \\ c_p\, N_p(E_{\min})\, p^{r_p-1}, & r_p \geq 1. \end{cases}$$

In particular,

$$\#G_p \mid c_p\, N_p(E_{\min})\, p^{\max(r_p-1,0)} \qquad (p = 2,3).$$

By definition,

$$\mathrm{Tam}(E) = \mathrm{lcm}_\ell(c_\ell),$$

so every c_ℓ divides $\mathrm{Tam}(E)$. Also, by construction,

$$m$$

is divisible by

$$N_2(E_{\min})\,2^{\max(r_2-1,0)} \quad \text{and} \quad N_3(E_{\min})\,3^{\max(r_3-1,0)}.$$

Hence

$$\#G_\ell \mid m \cdot \mathrm{Tam}(E) \qquad \text{for every prime } \ell.$$

Therefore multiplication by $m \cdot \mathrm{Tam}(E)$ is zero on each G_ℓ, hence also on $\prod_\ell G_\ell$. Since $E(\mathbb{Q})/E^0(\mathbb{Q})$ injects into this product, it is also annihilated by $m \cdot \mathrm{Tam}(E)$. Equivalently,

$$(m \cdot \mathrm{Tam}(E))\,P \in E^0(\mathbb{Q}) \qquad \text{for all } P \in E(\mathbb{Q}).$$

□

Example 6.1. *Let $E\colon y^2 + y = x^3 - x$ be an elliptic curve of rank 1 over $\mathbb{Q}$, given in its global minimal model (label `37a1` in the Cremona database). Using Sage, we find that*

$$\mathrm{Tam}(E) = 1,$$

and that the point $P = (0,-1)$ generates the free part of $E(\mathbb{Q})$. Since $\mathrm{Tam}(E) = 1$, we have $c_\ell = 1$ for all primes ℓ, hence $E(\mathbb{Q}_\ell) = E^0(\mathbb{Q}_\ell)$ for all ℓ, and therefore

$$E(\mathbb{Q}) = E^0(\mathbb{Q})$$

for this minimal model.

Now consider the corresponding short Weierstrass form of E:

$$E_1 : y^2 = x^3 - 16x + 16,$$

with $P_1 = (0,-4) \in E_1(\mathbb{Q})$ the image of P. Reducing modulo 2 gives

$$\tilde{E}_1 : y^2 = x^3,$$

which is singular, and $\tilde{P}_1 = (0,0)$ is the singular point. Thus,

$$P_1 \notin E_1^0(\mathbb{Q}).$$

This agrees with Proposition 6.2, since on the short model $f_2(x,y) = 2y$ and (here $d(P_1) = 1$) one has

$$u_2(P_1) = f_2(P_1) = 2y(P_1) = -8,$$

which is divisible by 2. In fact one checks that

$$5P_1 = (1,1) \in E_1(\mathbb{Q}) \qquad \text{and} \qquad u_2(5P_1) = 1,$$

so $5P_1$ has non-singular reduction at 2 (and it is clear from the integral coordinates that it has non-singular reduction away from 2). Hence $5P_1 \in E_1^0(\mathbb{Q})$.

Since $E_1(\mathbb{Q}) \cong \mathbb{Z}$ is generated by P_1 (rank 1 and no torsion), the subgroup $E_1^0(\mathbb{Q})$ has the form $n\mathbb{Z} \cdot P_1$ for a unique $n \geq 1$. The facts $P_1 \notin E_1^0(\mathbb{Q})$ and $5P_1 \in E_1^0(\mathbb{Q})$ force $n = 5$, so

$$[E_1(\mathbb{Q}) : E_1^0(\mathbb{Q})] = 5.$$

Finally, in Corollary 6.2 one has $v_2(\Delta(E_1)) = 12$ *and* $v_2(\Delta(E_{\min})) = 0$*, hence* $r_2 = 1$*, and* $r_3 = 0$*. Also* $N_2(E_{\min}) = \#E(\mathbb{F}_2) = 5$ *and* $N_3(E_{\min}) = \#E(\mathbb{F}_3) = 7$*, so* $m = \operatorname{lcm}(5,7) = 35$ *and* $\operatorname{Tam}(E) = 1$*. Thus the corollary predicts that* $E_1(\mathbb{Q})/E_1^0(\mathbb{Q})$ *is annihilated by* 35*, which is compatible with the sharper computation above showing* $[E_1(\mathbb{Q}) : E_1^0(\mathbb{Q})] = 5$*.*

Chapter 7: Further thoughts and future directions

In this chapter, we discuss some future directions.

My research, in general, focuses on understanding the behaviour of the Iwasawa invariants of class groups and elliptic curves. There are numerous important results in the setting of class groups, and generalizing them to elliptic curves is often a difficult task. Here, we present three research directions that are worth exploring in the near future.

7.1 Vanishing of the μ-invariant

One of the main questions in Iwasawa theory is understanding the behaviour of the μ-invariant. While Ferrero–Washington [FW79] proved that $\mu_p(K) = 0$ for every abelian number field K, the analogous statement for elliptic curves fails in general: there are examples where $\mu_p(E/\mathbb{Q}) > 0$. Nevertheless, a conjecture by Greenberg predicts the following:

Conjecture 7.1 (Greenberg)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and p a prime of good ordinary reduction. Then there exists an elliptic curve $E'/\mathbb{Q}$, p-isogenous to E, such that $\mu_p(E'/\mathbb{Q}) = 0$. In particular, if $E[p]$ is irreducible, then $\mu_p(E/\mathbb{Q}) = 0$.*

In particular, this would imply that for a fixed elliptic curve $E/\mathbb{Q}$, $\mu_p(E) = 0$ for all $p > 37$ of good ordinary reduction.

Recent progress by Chakravarthy [Cha24] shows that for each elliptic curve E, there is a constant M_E such that $\mu_p(E) \leq 1$ for all $p > M_E$. His method translates μ_p into a

non-vanishing problem for p-adic L-functions expressed through modular symbols, ultimately proving that a certain sum of modular symbols is nonzero modulo p^4. My proposed direction is to aim to prove the stronger statement:

Problem: For any elliptic curve $E/\mathbb{Q}$, we have $\mu_p(E/\mathbb{Q}) = 0$ for all but finitely many primes p.

The guiding philosophy is to adapt Ferrero–Washington's method. Their argument reduced to showing that for all d, there exists $\alpha \in \mathbb{Z}_p$ and $n \in \mathbb{Z}$ such that

$$\sum_{\zeta \in \mu_{p-1}} t_m(a\zeta)\zeta^d \not\equiv 0 \mod p$$

where t_m denotes the $m-$th digit in the $p-$adic expansion. They achieved this through joint normality and equidistribution arguments over the p-adic integers.

In the elliptic curve setting, the analogous exponential sums are replaced by modular-symbol sums. Proving $\mu_p(E/\mathbb{Q}) = 0$ can be reduced to proving that there exists $a \in \mathbb{Z}_p$ and $n \in \mathbb{N}$ such that

$$\sum_{\zeta \in \mu_{p-1}} a_p \left[\frac{\zeta a}{p^n}\right] - \left[\frac{\zeta a}{p^{n-1}}\right] \not\equiv 0 \mod p.$$

where a_p is the trace of Frobenius of E. Understanding the distribution of the modular symbols is the key obstacle. The central challenge—and opportunity—is therefore to establish an analogue of equidistribution for modular symbols. Recent advances in this area [CN22], [LP24], [LS25] suggest that such results are within reach, and developing the right equidistribution framework could allow one to generalize Ferrero–Washington's strategy to the elliptic curve case.

In short, my plan is to combine:

- **Analytic input:** non-vanishing results for L-functions as in [Chi02],
- **Probabilistic/equidistribution heuristics:** in the spirit of joint normality.

- Ferrero–Washington's technique in [FW79]

The ultimate goal is to prove $\mu_p(E) = 0$ for almost all primes p, sharpening existing bounds and bringing the elliptic curve case closer to the classical abelian setting.

7.2 Bound of the μ-invariant for varying number fields

In an old paper [Fri85], Friedman proves the following:

Theorem 7.1 (Friedman)**.** *Let K be any number field of degree $d = [K : \mathbb{Q}]$ and K_{cyc}/K its cyclotomic $\mathbb{Z}_p$-extension for a prime p. Then*

$$\mu_p(K) < [K : \mathbb{Q}] \qquad \textit{for all sufficiently large } p$$

with an explicit (finite) set of exceptional primes depending only on K.

In summary, his idea proceeds as follows: Denote by A_1 the p-primary part of the class group of K_n. By purely algebraic methods, one has that

$$\mu_p(K)(p-1)\log p \leq \log|A_1| \leq \log h(K_1).$$

Applying the theorem of Brauer-Siegel to the family $\{K_1\}_p$, one has

$$\log\big(h(K_1)\,R(K_1)\big) \;\sim\; \tfrac{1}{2}\log d_{K_1} \qquad (p \to \infty).$$

The conductor-discriminant formula gives an asymptotic

$$\log d_{K_1} \;=\; d\,(p-1)\log p \;+\; O(\log d_K).$$

Finally, a uniform lower bound on regulators by Zimmert allows Friedman to isolate $\log h(K_1)$,

obtaining the desired bound.

Inspired by his approach, I ask the following question:

Question: Let E/K be an elliptic curve. Is it possible to find a non-trivial bound for $\mu_p(E/K)$ that depends only on the number field K and the conductor of the elliptic curve?

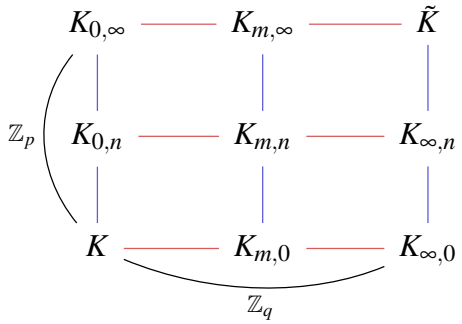
The main obstacle is the lack of a suitable analogue of the Brauer-Siegel theorem for Selmer groups. To that end, I plan to explore two directions.

Firstly, there has been recent progress with the work of Hindry-Pacheco [HP16] and Griffon [Gri18a] [Gri18b], who developed a Brauer-Siegel type result for abelian varieties over function fields. I plan to build on top of their work and explore whether their techniques can be adapted to the number field setting, for elliptic curves of rank 0.

Secondly, I plan to explore an analogue of Friedman's results in the case of fine Selmer groups, which are a subgroup of the classical Selmer group that is often easier to study. For example, in [LKM16] it was shown that the class groups of number fields and the fine Selmer groups are closely related in $\mathbb{Z}_p$-extensions where primes are finitely decomposed. Taking advantage of this relation, we can attempt to prove a bound for the μ-invariant of the fine Selmer group that depends only on the number field K or the conductor of the elliptic curve.

7.3 Iwasawa theory over $\mathbb{Z}_p \times \mathbb{Z}_q$-extensions

Let $K/\mathbb{Q}$ be an abelian number field. Let $p \neq q$ be two odd primes and consider $\tilde{K}$ to be the cyclotomic $\mathbb{Z}_p \times \mathbb{Z}_q$-extension of K. This creates the following diagram:



We have that $\lambda_p(K_{m,0}) \leq \lambda_p(K_{m+1,0})$. A natural question is to ask whether the sequence $\{\lambda_p(K_{m,0})\}_m$ converges as m tends to infinity.

In the case of class groups, Friedman [Fri81] gave a positive answer. His proof uses the basic structure of Iwasawa modules and depends on two crucial facts:

1) Ferrero-Washington's theorem that $\mu_p(K) = 0$ for an abelian number field K.

2) Stabilization of $|Cl(K_{m,0})(p)|$ as m goes to infinity; see [Was78].

Question: For an elliptic curve $E/\mathbb{Q}$ and primes p, q of good ordinary reduction, does the sequence $\{\lambda_p(E/K_{m,0})\}_m$ converge?

The main issue is that both analogues of the above two results are false. In particular, although rare, the μ-invariant of the elliptic curve can be positive. More crucially, it was proven [DD15] that it is possible to construct elliptic curves such that $|Ш(E/K_{m,0})(p)|$ would grow to infinity. However, it is worthwhile to notice that this construction crucially requires the assumption that $\mu_p(E) > 0$. This indicates that the positivity of the μ-invariant is actually the only real obstruction to the problem. In particular, assuming that $\mu_p(E/\mathbb{Q}) = 0$, I plan to explore if the sequence $\{\lambda_p(E/K_{m,0})\}_m$ converges.

Apart from these questions, it is worth exploring the ideas explored in [BL23], where the authors analyze the structure of the $\mathbb{Z}_p[[\mathbb{Z}_q]]$ Iwasawa module, providing a fresh approach to the results (1) and (2) mentioned above.

Finally, in the case of fine Selmer groups, there are already results by Kundu-Lei

[KL23]. They prove that under some assumptions, there exists an N such that $\mathrm{Sel}_0(E/K_{m,0}) \simeq \mathrm{Sel}_0(E/K_{N,0})$ for all $m \geq N$, where $\mathrm{Sel}_0(E/K_{m,0})$ is the p-primary part of the fine Selmer group of E over $K_{m,0}$.

Bibliography

[Aya92] Mohamed Ayad. Points *S*-entiers des courbes elliptiques. *Manuscripta Math.*, 76(3-4):305–324, 1992.

[Bal16] Jennifer S. Balakrishnan. On 3-adic heights on elliptic curves. *J. Number Theory*, 161:119–134, 2016.

[BL23] Andrea Bandini and Ignazio Longhi. The algebra $\mathbb{Z}_\ell[[\mathbb{Z}_p]]$ and applications to Iwasawa theory, 2023.

[BPR93] Dominique Bernardi and Bernadette Perrin-Riou. Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier). *C. R. Acad. Sci. Paris Sér. I Math.*, 317(3):227–232, 1993.

[CH98] J. Cheon and S. Hahn. Explicit valuations of division polynomials of an elliptic curve. *Manuscripta Math.*, 97(3):319–328, 1998.

[Cha24] Adithya Chakravarthy. The iwasawa μ of elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:2408.07826*, 2024.

[Chi02] Gautam Chinta. Analytic ranks of elliptic curves over cyclotomic fields. *J. Reine Angew. Math.*, 544:13–24, 2002.

[CN22] Petru Constantinescu and Asbjørn Christian Nordentoft. Residual equidistribution of modular symbols and cohomology classes for quotients of hyperbolic n-space. *Trans. Amer. Math. Soc.*, 375(10):7001–7034, 2022.

[DD15] Tim Dokchitser and Vladimir Dokchitser. Growth of Ш in towers for isogenous curves. *Compos. Math.*, 151(11):1981–2005, 2015.

[FG81] Leslie Jane Federer and Benedict H. Gross. Regulators and Iwasawa modules. *Invent. Math.*, 62(3):443–457, 1981. With an appendix by Warren Sinnott.

[Foi25] Foivos Chnaras. Sage Computations, 2025. `https://github.com/foivoshn/Sage_Iwasawa`.

[Fri81] Eduardo C. Friedman. Ideal class groups in basic $\mathbf{Z}_{p_1} \times \cdots \times \mathbf{Z}_{p_s}$-extensions of abelian number fields. *Invent. Math.*, 65(3):425–440, 1981.

[Fri85] Eduardo Friedman. Iwasawa invariants. *Math. Ann.*, 271(1):13–30, 1985.

[FW79] Bruce Ferrero and Lawrence C. Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. of Math. (2)*, 109(2):377–395, 1979.

[Gol74] Robert Gold. The nontriviality of certain Z_1-extensions. *J. Number Theory*, 6:369–373, 1974.

[Gre99] Ralph Greenberg. Iwasawa theory for elliptic curves. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 51–144. Springer, Berlin, 1999.

[Gri18a] Richard Griffon. Analogue of the Brauer-Siegel theorem for Legendre elliptic curves. *J. Number Theory*, 193:189–212, 2018.

[Gri18b] Richard Griffon. Explicit *L*-functions and a Brauer-Siegel theorem for Hessian elliptic curves. *J. Théor. Nombres Bordeaux*, 30(3):1059–1084, 2018.

[Har08] David Harvey. Efficient computation of *p*-adic heights. *LMS J. Comput. Math.*, 11:40–59, 2008.

[HP16] Marc Hindry and Amílcar Pacheco. An analogue of the Brauer-Siegel theorem for abelian varieties in positive characteristic. *Mosc. Math. J.*, 16(1):45–93, 2016.

[Ito15] Akiko Ito. On certain infinite families of imaginary quadratic fields whose Iwasawa λ-invariant is equal to 1. *Acta Arith.*, 168(4):301–340, 2015.

[Joc94] Naomi Jochnowitz. A p-adic conjecture about derivatives of L-series attached to modular forms. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, volume 165 of *Contemp. Math.*, pages 239–263. Amer. Math. Soc., Providence, RI, 1994.

[Kat76] Nicholas M. Katz. *p*-adic interpolation of real analytic Eisenstein series. *Ann. of Math. (2)*, 104(3):459–571, 1976.

[Kat04] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. Number 295, pages ix, 117–290. 2004. Cohomologies p-adiques et applications arithmétiques. III.

[Kim13] Byoung Du Kim. The plus/minus Selmer groups for supersingular primes. *J. Aust. Math. Soc.*, 95(2):189–200, 2013.

[KL23] Debanjana Kundu and Antonio Lei. Growth of p-parts of ideal class groups and fine Selmer groups in $\mathbb{Z}_q$-extensions with $p \neq q$. *Acta Arith.*, 207(4):297–313, 2023.

[Kob03] Shin-ichi Kobayashi. Iwasawa theory for elliptic curves at supersingular primes. *Invent. Math.*, 152(1):1–36, 2003.

[KR21] Debanjana Kundu and Anwesh Ray. Statistics for Iwasawa invariants of elliptic curves. *Trans. Amer. Math. Soc.*, 374(11):7945–7965, 2021.

[LKM16] Meng Fai Lim and V. Kumar Murty. The growth of fine Selmer groups. *J. Ramanujan Math. Soc.*, 31(1):79–94, 2016.

[LLS+23] Yeuk Hay Joshua Lam, Yuan Liu, Romyar Sharifi, Preston Wake, and Jiuya Wang. Generalized Bockstein maps and Massey products. *Forum Math. Sigma*, 11:Paper No. e5, 41, 2023.

[LP24] Jungwon Lee and Bharathwaj Palvannan. An ergodic approach towards an equidistribution result of Ferrero-Washington. *J. Théor. Nombres Bordeaux*, 36(3):805–833, 2024.

[LS25] Jungwon Lee and Hae-Sang Sun. Dynamics of continued fractions and distribution of modular symbols. *J. Eur. Math. Soc. (JEMS)*, 27(9):3527–3582, 2025.

[McC96] Gary McConnell. On the Iwasawa theory of CM elliptic curves at supersingular primes. *Compositio Math.*, 101(1):1–19, 1996.

[MST06] Barry Mazur, William Stein, and John Tate. Computation of p-adic heights and log convergence. *Doc. Math.*, pages 577–614, 2006.

[MT91] B. Mazur and J. Tate. The p-adic sigma function. *Duke Math. J.*, 62(3):663–688, 1991.

[Pol03] Robert Pollack. On the p-adic L-function of a modular form at a supersingular prime. *Duke Math. J.*, 118(3):523–558, 2003.

[PR84] Bernadette Perrin-Riou. Arithmétique des courbes elliptiques et théorie d'Iwasawa. *Mém. Soc. Math. France (N.S.)*, (17):130, 1984.

[PR90] Bernadette Perrin-Riou. Théorie d'Iwasawa p-adique locale et globale. *Invent. Math.*, 99(2):247–292, 1990.

[PR04] Robert Pollack and Karl Rubin. The main conjecture for CM elliptic curves at supersingular primes. *Ann. of Math. (2)*, 159(1):447–464, 2004.

[Qi24] Peikai Qi. Iwasawa lambda invariant and Massey product. *arXiv preprint arXiv:2402.06028*, 2024.

[RS23] Anwesh Ray and R. Sujatha. Euler characteristics and their congruences for multisigned Selmer groups. *Canad. J. Math.*, 75(1):298–321, 2023.

[Rub99] Karl Rubin. Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 167–234. Springer, Berlin, 1999.

[San93] Jonathan W. Sands. On the nontriviality of the basic Iwasawa λ-invariant for an infinitude of imaginary quadratic fields. *Acta Arith.*, 65(3):243–248, 1993.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Sil88] Joseph H. Silverman. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory*, 30(2):226–237, 1988.

[Sto24] Matt Stokes. On CM elliptic curves and the cyclotomic λ-invariants of imaginary quadratic fields. *J. Number Theory*, 256:160–169, 2024.

[SW13] William Stein and Christian Wuthrich. Algorithms for the arithmetic of elliptic curves using Iwasawa theory. *Math. Comp.*, 82(283):1757–1792, 2013.

[Tea24] Sage Development Team. SageMath development team. `https://www.sagemath.org`, 2024. Version 10.4.

[Was78] Lawrence C. Washington. The non-p-part of the class number in a cyclotomic $\mathbf{Z}_p$-extension. *Invent. Math.*, 49(1):87–97, 1978.

[Was82] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[Wut04] Christian Wuthrich. On p-adic heights in families of elliptic curves. *J. London Math. Soc. (2)*, 70(1):23–40, 2004.