# Generalizations of the Signed Selmer Groups for Cyclotomic Extensions

by

Alexander Reamy

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Approved April 2023 by the
Graduate Supervisory Committee:

Florian Sprung, Co-Chair
Nancy Childress, Co-Chair
Steven Kaliszewski
Jonathan Montaño
Julien Paupert

ARIZONA STATE UNIVERSITY

May 2023

ABSTRACT

Let E be an elliptic curve defined over a number field K, p a rational prime, and $\Lambda(\Gamma)$ the Iwasawa module of the cyclotomic extension of K. A famous conjecture by Mazur states that the p-primary component of the Selmer group of E is $\Lambda(\Gamma)$-cotorsion when E has good ordinary reduction at all primes of K lying over p. The conjecture was proven in the case that K is the field of rationals by Kato, but is known to be false when E has supersingular reduction type. To salvage this result, Kobayashi introduced the signed Selmer groups, which impose stronger local conditions than their classical counterparts.

Part of the construction of the signed Selmer groups involves using Honda's theory of commutative formal groups to define a canonical system of points. In this paper I offer an alternate construction that appeals to the Functional Equation Lemma, and explore a possible way of generalizing this method to elliptic curves defined over p-adic fields by passing from formal group laws to formal modules.

TABLE OF CONTENTS

Page

CHAPTER

# Chapter 1

# BACKGROUND

## 1.1 The Classical Selmer Group

Let $K$ be a number field and $E$ an elliptic curve that is defined over $K$. The Selmer group is an object that arises in the proof of the Mordell-Weil Theorem. Fix an algebraic closure $\bar{K}$ of $K$, and let $G_K$ denote the Galois group $\mathrm{Gal}(\bar{K}/K)$. Note $G_K$ is the inverse limit of the system of groups $\mathrm{Gal}(L/K)$, where $L$ ranges over the finite Galois extensions of $K$. If $E_{\mathrm{tors}}$ denotes the subgroup of torsion points of $E(\bar{K})$, then there is a natural action of $G_K$ on $E_{\mathrm{tors}}$ that is continuous with respect to the profinite topology on $G_K$ and the discrete topology on $E_{\mathrm{tors}}$; thus we may view $E_{\mathrm{tors}}$ as a $G_K$-module, and consider the first cohomology group $H^1(G_K, E_{\mathrm{tors}})$.

Let $P \in E(K)$ and $n \geq 1$. Since the multiplication-by-$n$ isogeny $[n] : E \to E$ is surjective, there exists some $Q \in E(\bar{K})$ such that $nQ = P$. Suppose $\sigma \in G_K$ and write $Q' = \sigma(Q)$, so that $nQ' = P$. It follows that $n(Q' - Q) = 0$; that is,

$$\sigma(Q) - Q \in E_{\mathrm{tors}}.$$

Thus the map $\varphi : G_K \to E_{\mathrm{tors}}$ defined by $\varphi(\sigma) = \sigma(Q) - Q$ is a 1-cocycle, and we may consider the corresponding class $[\varphi]$ of $H^1(G_K, E_{\mathrm{tors}})$. We define the *Kummer map* to be the injective homomorphism

$$\begin{aligned} \kappa : E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) &\to H^1(G_K, E_{\mathrm{tors}}) \\ P \otimes \left(\frac{1}{n} + \mathbb{Z}\right) &\mapsto [\varphi]. \end{aligned}$$

Let $M_K$ be the set of primes of the number field $K$. If $v \in M_K$, let $K_v$ denote the completion of $K$ at $v$. For each $v$, choose an algebraic closure $\bar{K}_v$ of $K_v$, and let $G_{K_v} = \mathrm{Gal}(\bar{K}_v/K_v)$ be the absolute Galois group. By a similar logic as above, we can define a *$v$-adic Kummer map*

$$\kappa_v : E(K_v) \otimes (\mathbb{Q}/\mathbb{Z}) \to H^1(G_{K_v}, E_{\mathrm{tors}}).$$

If we choose an embedding $\bar{K} \hookrightarrow \bar{K}_v$ that extends the natural embedding $K \hookrightarrow K_v$, then $G_{K_v}$ may be viewed as a subgroup of $G_K$; thus, after applying Galois cohomology, we obtain a restriction map $H^1(G_K, E_{\mathrm{tors}}) \to H^1(G_{K_v}, E_{\mathrm{tors}})$.

**Definition 1.1.1.** The *Selmer group* $\mathrm{Sel}_E(K)$ of $E$ over the number field $K$ is defined to be

$$\mathrm{Sel}_E(K) = \ker \left\{ H^1(G_K, E_{\mathrm{tors}}) \to \prod_{v \in M_K} \frac{H^1(G_{K_v}, E_{\mathrm{tors}})}{E(K_v) \otimes (\mathbb{Q}/\mathbb{Z})} \right\},$$

where we identify $E(K_v) \otimes (\mathbb{Q}/\mathbb{Z})$ with its image under the $v$-adic Kummer map. It can be shown that this definition is independent of our choice of extensions.

We typically study the structure of $\mathrm{Sel}_E(K)$ by analyzing its $p$-primary subgroups. Let $p$ be a fixed prime, and for any $n \geq 1$, let $E[p^n]$ denote the group of $p^n$-torsion points of $E$; furthermore, let $E[p^\infty] = \bigcup_{n \geq 1} E[p^n]$. Also let $\kappa_{v,p}$ be the restriction of the $v$-adic Kummer map $\kappa_v$ to the $p$-primary subgroup of $E(K_v) \otimes (\mathbb{Q}/\mathbb{Z})$.

**Definition 1.1.2.** The *$p$-Selmer group* $\mathrm{Sel}_E(K)_p$ of $E$ over the number field $K$ is defined to be

$$\mathrm{Sel}_E(K)_p = \ker \left\{ H^1(G_K, E[p^\infty]) \to \prod_{v \in M_K} \frac{H^1(G_{K_v}, E[p^\infty])}{E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)} \right\}.$$

## 1.2 Iwasawa Theory of the Classical Selmer Group

Let $K_\infty$ be an infinite Galois extension of $K$ whose Galois group is a $p$-adic Lie group of positive dimension. (Later, we will mostly be interested in the case where $K_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $K$.) We can extend the definition of the Selmer group as follows:

**Definition 1.2.1.** The *$p$-Selmer group* $\mathrm{Sel}_E(K_\infty)_p$ of $E$ over the infinite field extension $K_\infty$ is

$$\mathrm{Sel}_E(K_\infty)_p = \varinjlim \mathrm{Sel}_E(L)_p,$$

where $L$ runs over the finite extensions of $K$ contained in $K_\infty$ and the direct limit is taken with respect to the restriction maps.

Denote the Galois group of $K_\infty$ over $K$ by $\Gamma$. There is a natural action of $\Gamma$ on the cohomology group $H^1(K_\infty, E[p^\infty])$ and hence on the subgroup $\mathrm{Sel}_E(K_\infty)_p$. Viewing $\mathrm{Sel}_E(K_\infty)_p$ as a discrete $\mathbb{Z}_p$-module, we note that this action is both continuous and $\mathbb{Z}_p$-linear; thus it makes the $p$-Selmer group into a discrete $\Lambda(\Gamma)$-module, where $\Lambda(\Gamma)$ is the completed group algebra of $\Gamma$ over $\mathbb{Z}_p$. That is,

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

where $N$ runs over the open normal subgroups of $\Gamma$. We refer to $\Lambda(\Gamma)$ as the *Iwasawa algebra* of $\Gamma$. It is a useful fact that if $\gamma$ is a topological generator of $\Gamma$, then the map $\gamma \mapsto 1 + T$ induces an isomorphism $\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$, where the latter is the ring of formal power series with coefficients in $\mathbb{Z}_p$. In particular, $\Lambda(\Gamma)$ is a complete Noetherian local ring of Krull dimension 2.

Our goal is to describe the structure of $\mathrm{Sel}_E(K_\infty)_p$ as a $\Lambda(\Gamma)$-module. It is sometimes more convenient to examine its dual:

**Definition 1.2.2.** If $M$ is a $\Lambda(\Gamma)$-module, then the *Pontryagin dual* of $M$, denoted $\widehat{M}$, is the group of continuous homomorphisms $M \to \mathbb{Q}_p/\mathbb{Z}_p$, i.e.,

$$\widehat{M} = \mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p).$$

The module $M$ is said to be $\Lambda(\Gamma)$-*cotorsion* if its dual is $\Lambda(\Gamma)$-torsion.

Many of the arguments ultimately reduce to analyzing the structure of a particular commutative diagram. Let $S$ be a finite set of primes of $K$ that contains all the primes dividing $p$ and all the primes where $E$ has bad reduction. Let $K_S$ be the maximal extension of $K$ that is unramified outside of $S$ and the Archimedean primes of $K$, and assume $K_\infty \subset K_S$ (this is certainly true when we take $K_\infty$ to be the cyclotomic $\mathbb{Z}_p$-extension). Also put $G_S = \mathrm{Gal}(K_S/K)$ and $G_{S,\infty} = G(K_S/K_\infty)$.

For a finite extension $L$ of $K$ contained in $K_\infty$ and a prime $v$ of $K$, write

$$J_v(L) = \bigoplus_{w|v} H^1(G_{L_w}, E)[p^\infty],$$

where the direct sum is taken over the primes $w$ of $L$ lying over $v$; we then define

$$J_v(K_\infty) = \varinjlim J_v(L),$$

where, as above, $L$ runs over the the finite extensions of $K$ contained in $K_\infty$ and the direct limit is taken with respect to the restriction maps. The $p$-Selmer group of $E$ over $K$ is characterized by the exact sequence of $\Gamma$-modules

$$0 \to \mathrm{Sel}_E(K)_p \to H^1(G_S, E[p^\infty]) \xrightarrow{\lambda} \bigoplus_{v \in S} J_v(K),$$

where $\lambda$ is the localization map. Taking direct limits over the intermediate fields then yields an analogous exact sequence

$$0 \to \mathrm{Sel}_E(K_\infty) \to H^1(G_{S,\infty}, E[p^\infty]) \xrightarrow{\lambda_\infty} \bigoplus_{v \in S} J_v(K_\infty).$$

These exact sequences are in turn related by the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}_E(K_\infty)_p^\Gamma & \longrightarrow & H^1(G_{S,\infty}, E[p^\infty])^\Gamma & \xrightarrow{\lambda_\infty^\Gamma} & \bigoplus_{v\in S} J_v(K_\infty)^\Gamma \\ & & \uparrow & & \uparrow & & \uparrow \\ 0 & \longrightarrow & \mathrm{Sel}_E(K)_p & \longrightarrow & H^1(G_S, E[p^\infty]) & \xrightarrow{\lambda} & \bigoplus_{v\in S} J_v(K), \end{array}$$

where the rows are exact and the vertical arrows are the restriction maps. This is referred to as the *fundamental diagram* in (Coates and Sujatha 2010).

## 1.3 The Case of the Cyclotomic Extension

Henceforth we will assume that $K_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $K$. More precisely, let $\mu_{p^\infty}$ denote the set of $p$-power roots of unity in $\bar{K}$. We choose $K_\infty$ to be the fixed field of the torsion subgroup of $\mathrm{Gal}(K(\mu_{p^\infty})/K)$; equivalently, $K_\infty$ is the unique subfield of $K(\mu_{p^\infty})$ over $K$ for which $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Put $K_{-1} = K$ and $K_n = K(\mu_{p^{n+1}})$ for each $n \geq 0$, so that $K_n$ is the $n^{\text{th}}$ layer of the extension.

Analyzing the structure of the fundamental diagram in this situation shows that the dual of $\mathrm{Sel}_E(K_\infty)_p^\Gamma$ has finite rank over $\mathbb{Z}_p$, from which the following result may be deduced:

**Proposition 1.3.1.** The dual of $\mathrm{Sel}_E(K_\infty)_p$ is finitely generated as a $\Lambda(\Gamma)$-module.

In fact, a stronger result has been conjectured in (Mazur 1972), which captures one of the central problems of the Iwasawa theory of elliptic curves:

**Conjecture 1.3.2** (Mazur)**.** Let $p$ be a rational prime and $E$ be an elliptic curve with good ordinary reduction at all primes of $K$ lying over $p$. Then $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda(\Gamma)$-cotorsion.

The conjecture is known to be true in several special cases. An 'easy' case occurs if we assume the Selmer group over $K$ is finite.

**Definition 1.3.3.** Let $E$ be an elliptic curve defined over a number field $K$, and let $v$ be a prime of $K$ dividing $p$. We say $E$ has *potential good ordinary (resp. supersingular) reduction at* $v$ if there exists a finite extension $L$ of $K_v$ such that $E$ has good ordinary (resp. supersingular) reduction over $L$.

**Theorem 1.3.4.** Assume that $\mathrm{Sel}_E(K)_p$ is finite and $E$ has potential good ordinary reduction at all primes of $K$ dividing $p$. Then $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda(\Gamma)$-cotorsion.

The most significant advance in this area was made in (Kato 2004) by studying Euler systems associated to modular forms.

**Theorem 1.3.5** (Kato 2004, Theorem 14.4)**.** Let $A$ be an Abelian variety over $\mathbb{Q}$ such that there is a surjective homomorphism $J_1(N) \to A$ for some $N \geq 1$. Then for any $m \geq 1$, $A(\mathbb{Q}(\mu_{p^\infty}))$ is finitely generated as an Abelian group.

Here $J_1(N)$ denotes the Jacobian associated to the congruence subgroup $\Gamma_1(N)$. An analogous result for $J_0(N)$ was previously shown in (Kolyvagin and Logachev 1990). In particular, if $E$ is an elliptic curve with conductor $N_E$, a version of the Modularity Theorem guarantees the existence of such a surjection $J_1(N_E) \to E$, so that $E(\mathbb{Q}(\mu_{p^\infty}))$ is a finitely generated Abelian group for any prime $p$. This has the important consequence:

**Theorem 1.3.6.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with good ordinary reduction at the prime $p$. Then $\mathrm{Sel}_E(\mathbb{Q}(\mu_{p^\infty}))$ is $\Lambda(\Gamma)$-cotorsion.

A common attribute of these theorems is the assumption that $E$ has (potential) good ordinary reduction at the prime $p$ (or more generally the primes lying over $p$); this condition turns out to be essential, as (Schneider 1985) has shown that $\mathrm{Sel}_E(K_\infty)_p$ fails to be $\Lambda(\Gamma)$-cotorsion when $E$ has good supersingular reduction at $p$. To elaborate on

this point, let $Q(\Gamma)$ denote the total quotient ring of $\Lambda(\Gamma)$. For any finitely generated $\Lambda(\Gamma)$-module $X$, we define the $\Lambda(\Gamma)$-*rank of* $X$ to be the dimension of $X \otimes_{\Lambda(\Gamma)} Q(\Gamma)$ over $Q(\Gamma)$. Let $P_{p,E}(K)$ be the set of primes $v$ of $K$ dividing $p$ such that $E$ has potential good supersingular reduction at $v$. If $P_{p,E}(K)$ is nonempty, we say that $E$ is of *supersingular type at* $p$. Define

$$r_{p,E}(K) = \begin{cases} \sum_{v \in P_{p,E}(K)} [K_v : \mathbb{Q}_p], & \text{if } E \text{ is of supersingular type at } p, \\ 0, & \text{else.} \end{cases}$$

Then Mazur's Conjecture is a special case of the following:

**Conjecture 1.3.7** (Schneider)**.** For every prime $p$, the $\Lambda(\Gamma)$-rank of $\widehat{\mathrm{Sel}_E(K_\infty)}_p$ is equal to $r_{p,E}(K)$.

As above, this is known to be true when $\mathrm{Sel}_E(K_\infty)$ is finite and $E$ has potential good reduction at all primes of $K$ dividing $p$. For more general elliptic curve, we at least have:

**Theorem 1.3.8.** For every prime $p$, the $\Lambda(\Gamma)$-rank of $\widehat{\mathrm{Sel}_E(K_\infty)}_p$ is greater than or equal to $r_{p,E}(K)$.

*Proof.* See (Schneider 1985), §3, Corollary 5 or alternatively (Coates and Sujatha 2010), Theorem 2.6. □

**Corollary 1.3.9.** If $E$ has supersingular reduction at a prime $v$ of $K$ dividing $p$, then $\widehat{\mathrm{Sel}_E(K_\infty)}_p$ has positive rank as a $\Lambda(\Gamma)$-module.

*Proof.* This follows immediately from Theorem 1.3.8 since $P_{p,E}(K)$ is nonempty. □

## 1.4 The Construction of the Signed Selmer Groups

(Kobayashi 2003) introduced the signed Selmer groups as a way of salvaging Iwasawa theory for elliptic curves in the case of supersingular reduction. The strategy involves imposing stronger local conditions at $p$ than required in the definition of the classical $p$-Selmer group. Let $E$ be an elliptic curve over $\mathbb{Q}$ with good reduction at $p$. Recall that the Frobenius endomorphism of the reduced elliptic curve $\tilde{E}/\mathbb{F}_p$ has trace $a_p := 1 + p - \#\tilde{E}(\mathbb{F}_p)$. We assume that $a_p = 0$; for primes $p \geq 5$, this is equivalent to stating that $E$ has supersingular reduction at $p$.

Let $K$, $K_\infty$, and $K_n$ ($n \geq 0$) be as above. If $v$ is a prime of $K_n$, denote the completion of $K_n$ at $v$ by $K_{n,v}$. We define the subgroups $E^{\pm}(K_{n,v})$ of $E(K_{n,v})$ by

$$E^+(K_{n,v}) = \{P \in E(K_{n,v}) : \mathrm{Tr}_{n/m+1} P \in E(K_{m,v}) \text{ for even } m \ (0 \leq m < n)\},$$
$$E^-(K_{n,v}) = \{P \in E(K_{n,v}) : \mathrm{Tr}_{n/m+1} P \in E(K_{m,v}) \text{ for odd } m \ (-1 \leq m < n)\},$$

where $\mathrm{Tr}_{n/m+1} : E(K_{n,v}) \to E(K_{m+1,v})$ is the trace map $P \mapsto \sum_{\sigma \in \mathrm{Gal}(K_{n,v}/K_{m+1,v})} P^\sigma$.

**Definition 1.4.1.** The *even (resp. odd) p-Selmer group of $E$ over $K_n$* is defined to be

$$\mathrm{Sel}_E^{\pm}(K_n)_p = \ker \left\{ H^1(G_{K_n}, E[p^\infty]) \to \prod_{v \in M_{K_n}} \frac{H^1(G_{K_{n,v}}, E[p^\infty])}{E^{\pm}(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right\}.$$

We extend this definition to the cyclotomic $\mathbb{Z}_p$-extension by setting

$$\mathrm{Sel}_E^{\pm}(K_\infty)_p = \varinjlim \mathrm{Sel}_E^{\pm}(K_n)_p.$$

Using this new machinery, we have the following (see Kobayashi 2003, Theorem 1.2):

**Theorem 1.4.2** (Kobayashi)**.** $\widehat{\mathrm{Sel}_E^{\pm}(K_n)_p}$ are finitely generated torsion $\Lambda(\Gamma)$-modules.

We mention here a few important details in the proof. Let $E$ be an elliptic curve over $\mathbb{Q}_p$. Put $\mathfrak{m}_{-1} = p\mathbb{Z}_p$ and for each $n \geq 0$, let $\mathfrak{m}_n$ be the maximal ideal of $\mathbb{Z}_p[\zeta_{p^{n+1}}]$, where $\zeta_{p^{n+1}}$ denotes a primitive $p^{n+1}$st root of unity. Also, for a formal group $\mathcal{F}$, let $\mathrm{Tr}_{m/n} : \mathcal{F}(\mathfrak{m}_m) \to \mathcal{F}(\mathfrak{m}_n)$ be the trace map. Honda's theory of formal commutative groups is used to construct a canonical system of points $(c_n)_n \in \prod_{n\geq -1} \widehat{E}(\mathfrak{m}_n)$ satisfying $\mathrm{Tr}_{n+1/n}(c_{n+1}) = -c_{n-1}$. This system, in turn, is used to define the $n$th even and odd Coleman maps $\mathrm{Col}_n^{\pm} : H^1(\mathbb{Q}_p(\zeta_{p^{n+1}}), T) \to \Lambda(\Gamma)$, where $T$ is the $p$-adic Tate module of $E$. The subgroups $E^{\pm}(K_{n,v})$ are then constructed to be the exact annihilators with respect to the Tate pairing of the kernels of $\mathrm{Col}_n^{\pm}$.

Kobayashi's approach has two main limitations: (i) it only defines the signed Selmer groups for the cyclotomic $\mathbb{Z}_p$-extension; and (ii) the duals of the signed Selmer groups are only shown to be $\Lambda(\Gamma)$-torsion in the case that $K = \mathbb{Q}$. Since its publication, there have been many attempts to generalize this method so as to remove these constraints.

## 1.5 Some Known Results

An early result concerning the growth of the signed Selmer groups comes from (Iovita and Pollack 2006). Let $E/\mathbb{Q}$ be an elliptic curve and $K, K_n, K_\infty$ be as above. Let $S$ be a finite set of primes of $K$ containing all the primes lying above $p$, the Archimedean primes, and the primes of bad reduction for $E$; further let $K_S$ be the maximal extension of $K$ that is unramified outside $S$. By Lemma 7.6 and Corollary 7.7 from (Iovita and Pollack 2006), we have:

**Proposition 1.5.1.** Assume that the prime $p$ splits completely in $K$ and that each prime of $K$ lying above $p$ is totally ramified in $K_\infty$. The corank of $\mathrm{Sel}_E(K_n)_p$ over $\mathbb{Z}_p$

is bounded if and only if $\widehat{\mathrm{Sel}_E^{\pm}(K_\infty)}_p$ are torsion $\Lambda(\Gamma)$-modules. Furthermore, in this situation, $H^2(K_S/K_\infty, E[p^\infty]) = 0$.

The condition $H^2(K_S/K_\infty, E[p^\infty]) = 0$ may be thought of as a cohomological restatement of the weak Leopoldt conjecture. As it turns out, the weak Leopoldt conjecture is related to this problem in a fundamental way. We define another variant of the Selmer group:

**Definition 1.5.2.** The *fine p-Selmer group* $\mathrm{Sel}_E^0(K)_p$ of $E$ over a number field $K$ is

$$\mathrm{Sel}_E^0(K)_p = \ker \left\{ H^1(G_K, E[p^\infty]) \to \prod_{v \in M_K} H^1(G_{K_v}, E[p^\infty]) \right\}.$$

For the extension $K_\infty$, we define

$$\mathrm{Sel}_E^0(K_\infty)_p = \varinjlim \mathrm{Sel}_E^0(L)_p,$$

where as usual the direct limit is taken over the intermediate fields.

**Lemma 1.5.3** (Coates and Sujatha 2005, Lemma 3.1)**.** $\widehat{\mathrm{Sel}_E^0(K_\infty)}_p$ is $\Lambda(\Gamma)$-torsion if and only if $H^2(K_S/K_\infty, E[p^\infty]) = 0$.

This lemma still holds when we replace the cyclotomic $\mathbb{Z}_p$-extension $K_\infty$ with an *$S$-admissible p-adic Lie extension of $K$*; that is, a Galois extension $K_\infty$ containing the cyclotomic $\mathbb{Z}_p$-extension such that $K_\infty \subset K_S$ and $\mathrm{Gal}(K_\infty/K)$ is a $p$-adic Lie group that is pro-$p$ and contains no element of order $p$.

A recent paper (Lei and Sujatha 2020) establishes a similar result for the signed Selmer groups; however, an additional assumption is needed. First, we notice that we can interpret the signed Selmer groups using the local terms $J_v$ defined previously. Let $K$ be a number field, $K'$ a subfield of $K$, and $E/K'$ an elliptic curve with good reduction at all primes above $p$. Let $S_p^{ss}$ be the set of primes of $K'$ lying above $p$

for which $E$ has supersingular reduction and $S_{p,K}^{ss}$ the set of primes in $K$ lying above those in $K'$; assume $S_p^{ss}$ is nonempty. For any $v \in S_p^{ss}$, we require: (i) $K'_v = \mathbb{Q}_p$; (ii) $a_v = 1 + p - \#\tilde{E}(K'_v) = 0$; and (iii) $v$ is unramified in $K$. Then the signed $p$-Selmer groups of $E$ over the $n^{\text{th}}$ layer of the $\mathbb{Z}_p$-cyclotomic extension have the equivalent definition

$$\mathrm{Sel}_E^{\pm}(K_n)_p = \ker\left\{ \mathrm{Sel}_E(K_n)_p \to \bigoplus_{v \in S_{p,K}^{ss}} \frac{H^1(G_{K_{n,v}}, E[p^\infty])}{E^{\pm}(K_{n,v}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)} \right\},$$

and similarly for $\mathrm{Sel}_E^{\pm}(K_\infty)_p$.

For $n \geq 0$ and a prime $v \in S_{p,K}^{ss}$, define

$$J_v^{\pm}(K_n) = \bigoplus_{w|v} \frac{H^1(G_{K_{n,w}}), E[p^\infty])}{E^{\pm}(K_{n,w}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)},$$

with the direct sum taken over all primes $w$ of $K_n$ lying over $v$. Also let

$$J_v^{\pm}(K_\infty) = \varinjlim J_v^{\pm}(K_n).$$

If $v \notin S_{p,K}^{ss}$, put $J_v^{\pm}(K_n) = J_v(K_n)$ and $J_v^{\pm}(K_\infty) = J_v(K_\infty)$. As in the discussion of the classical Selmer groups, we can construct exact sequences relating the signed Selmer groups to the local terms $J_v^{\pm}$; this produces a map

$$\lambda_\infty^{\pm} : H^1(K_S/K_\infty, E[p^\infty]) \to \bigoplus_{v \in S} J_v^{\pm}(F_\infty),$$

and a 'signed' version of the fundamental diagram:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_E^{\pm}(K_\infty)_p^{\Gamma} & \longrightarrow & H^1(K_S/K_\infty, E[p^\infty])^{\Gamma} & \xrightarrow{\lambda_\infty^{\pm,\Gamma}} & \bigoplus_{v \in S} J_v^{\pm}(K_\infty)^{\Gamma} \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & \mathrm{Sel}_E(K)_p & \longrightarrow & H^1(K_S/K_\infty, E[p^\infty]) & \xrightarrow{\lambda} & \bigoplus_{v \in S} J_v(K),
\end{array}$$

**Theorem 1.5.4** (Lei and Sujatha 2020, Proposition 4.4)**.** $\widehat{\mathrm{Sel}_E^{\pm}(K_\infty)}_p$ is $\Lambda(\Gamma)$-torsion if and only if the maps $\lambda_\infty^{\pm}$ are surjective and $H^2(K_S/K_\infty, E[p^\infty]) = 0$.

An interesting result on the triviality of finite $\Lambda(\Gamma)$-submodules of $\widehat{\mathrm{Sel}_E^{\pm}(K_\infty)_p}$ comes from (Kitajima and Otsuki 2016). The method employed is very similar to that in (Kobayashi 2003), but applies to elliptic curves defined over suitably chosen extensions of $\mathbb{Q}$.

**Theorem 1.5.5** (Kitajima and Otsuki 2016, Main Theorem 1.3)**.** Let $K$ be a finite extension of $\mathbb{Q}$, $K_\infty/K$ the cyclotomic $\mathbb{Z}_p$-extension, and $E$ an elliptic curve defined over a subfield $K'$ of $K$. Let $S_p^{ss}$ be the set of primes of $K'$ lying above $p$ where $E$ has supersingular reduction. Assume the following:

(i) $E$ has good reduction at any prime of $K'$ lying above $p$;

(ii) $S_p^{ss}$ is nonempty;

(iii) any prime $v \in S_p^{ss}$ is unramified in $K$;

(iv) $K'_v = \mathbb{Q}_p$ for any prime $v \in S_p^{ss}$;

(v) $a_v = 1 + p - \#\tilde{E}_v(\mathbb{F}_p)$ for any prime $v \in S_p^{ss}$; and

(vi) both $\widehat{\mathrm{Sel}_E^{\pm}(K_\infty)_p}$ are $\Lambda(\Gamma)$-torsion.

Then both $\widehat{\mathrm{Sel}_E^{\pm}(K_\infty)_p}$ have no nontrivial finite $\Lambda(\Gamma)$-submodule.

Both (Lei and Sujatha 2020) and (Kitajima and Otsuki 2016) require us to assume that the field $K'$ over which $E$ is defined satisfies $K'_v = \mathbb{Q}_p$ for any prime $v$ of $K'$ of supersingular reduction. (When $K' = \mathbb{Q}$, as in Kobayahi's proof, this is automatic.) The importance of this condition is that it allows us to apply certain results from Honda theory, as explained in the next chapter.

Chapter 2

# HONDA THEORY AND CANONICAL SYSTEMS OF POINTS

## 2.1 Definitions and Important Properties

Let $R$ be a ring. Two power series $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in R[[x_1, \ldots, x_n]]$ are said to be *congruent modulo degree* $m$ if they are congruent modulo the closure of the ideal in $R[[x_1, \ldots, x_n]]$ generated by all monomials of the form $x_1^{i_1} \cdots x_n^{i_n}$, where $i_1 + \cdots + i_n \geq m$. In this situation, we write $f(x_1, \ldots, x_n) \equiv g(x_1, \ldots, x_n) \pmod{\deg m}$.

**Definition 2.1.1.** A *(one-dimensional) formal group law over the ring* $R$ is a formal power series $F(X, Y) \in R[[X, Y]]$ such that

(i) $F(X, Y) \equiv X + Y \pmod{\deg 2}$

(ii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$.

Condition (ii) is called *associativity*.

We say the formal group law $F(X, Y)$ is *commutative* if $F(X, Y) = F(Y, X)$. It is well-known that if the ring $R$ has no elements that are simultaneously torsion and nilpotent, then any formal group law over $R$ is commutative. Relevant to our purposes, any formal group law over a ring of characteristic 0 or a finite field is commutative.

Two simple but important examples are the additive formal group law $\widehat{\mathbb{G}}_a(X, Y)$ and the multiplicative formal group law $\widehat{\mathbb{G}}_m(X, Y)$, defined as follows:

$$\widehat{\mathbb{G}}_a(X, Y) = X + Y \qquad \text{and} \qquad \widehat{\mathbb{G}}_m(X, Y) = X + Y + XY.$$

**Definition 2.1.2.** Let $F(X,Y)$ and $G(X,Y)$ be two formal group laws over the ring $R$. A *homomorphism from* $F(X,Y)$ *to* $G(X,Y)$ *over* $R$ is a power series $f(T) \in R[[T]]$ with zero constant term such that

$$f(F(X,Y)) = G(f(X), f(Y)).$$

If further there exists a homomorphism $g(T)$ from $G(X,Y)$ to $F(X,Y)$ such that $f(g(T)) = g(f(T)) = T$, then $f$ is called an *isomorphism between* $F(X,Y)$ *and* $G(X,Y)$ *over* $R$. This isomorphism is said to be *strict* if $f(T) \equiv T \pmod{\deg 2}$.

By general facts involving power series, a homomorphism $f(T) : F(X,Y) \to G(X,Y)$ over $R$ is an isomorphism if and only if the coefficient of $T$ in $f(T)$ is a unit of $R$.

An example of an endomorphism of the formal group law $F(X,Y)$ is the *multiplication-by-n map* $[n] : F(X,Y) \to F(X,Y)$. It is defined inductively for any $n \in \mathbb{Z}$ by

$$[0](T) = 0, \qquad [n+1](T) = F(T, [n](T)).$$

If $F(X,Y)$ is a formal group defined over a ring $R$ of characteristic $p > 0$, we say $F(X,Y)$ has *height* $\infty$ if $[p](T) = 0$. Otherwise the *height of* $F(X,Y)$ is the smallest positive integer $h$ such that

$$[p](T) \equiv 0 \pmod{\deg p^h}.$$

Furthermore, if $R = \mathcal{O}_K$ is the ring of integers of a local field $K$ of characteristic 0 whose residue field $k$ has characteristic $p > 0$, then the *height* of a formal group law $F(X,Y)$ over $R$ is the height of the reduced formal group law over $k$.

When $R = \mathcal{O}_K$, in order to establish a strict isomorphism between formal group laws defined over $R$, it suffices to find isomorphisms over the rings of integers of the

local completions of $K$. Given a valuation $\nu$ of $K$, let $K_\nu$ denote the completion of $K$ with respect to $\nu$, and $\mathcal{O}_\nu$ its valuation ring.

**Theorem 2.1.3** (Local-Global Principle)**.** If $F(X,Y)$ and $G(X,Y)$ are formal group laws over $\mathcal{O}_K$, then they are strictly isomorphic over $\mathcal{O}_K$ if and only if they are strictly isomorphic over $\mathcal{O}_\nu$ for all non-Archimedean primes $\nu$ of $K$.

*Proof.* See (Hazewinkel 2012), Theorem 20.5.2. □

Because of this principle, we will generally be interested in studying formal group laws over rings of integers of local fields. If we take $K = \mathbb{Q}$, then the local case can be further reduced:

**Theorem 2.1.4.** Two formal group laws $F(X,Y)$ and $G(X,Y)$ are isomorphic over $\mathbb{Z}_p$ if and only if their reductions modulo $p$ are isomorphic over $\mathbb{F}_p$.

*Proof.* (Hazewinkel 2012), Theorem 22.1.10. □

Unfortunately, this theorem does not generalize to rings of integers of finite extensions of $\mathbb{Q}_p$. For instance, it is possible to construct non-isomorphic formal group laws over $\mathbb{Z}_3[i]$ whose reductions modulo 3 are isomorphic over $\mathbb{F}_9$. (See (Hazewinkel 2012), Example 22.1.12.) This will be consequential in our discussion of formal group laws associated to elliptic curves.

Suppose $F(X,Y)$ is a formal group law over a complete local ring $R$ with maximal ideal $\mathfrak{m}$. If $X$ and $Y$ take values in $\mathfrak{m}$, then the power series $F(X,Y)$ actually converges, giving $\mathfrak{m}$ the structure of a group. More precisely, given the formal group law $F(X,Y)$ over $R$, the *formal group law associated to* $F(X,Y)$, denoted $\mathcal{F}(\mathfrak{m})$, is the set $\mathfrak{m}$

equipped with the operations

$$x \oplus_{\mathcal{F}} y = F(x, y) \qquad \text{for } x, y \in \mathfrak{m}$$
$$\ominus_{\mathcal{F}} x = i(x) \qquad \text{for } x \in \mathfrak{m},$$

where $i(x)$ is the unique power series in $R[[x]]$ such that $F(x, i(x)) = 0$. Similarly, for a positive integer $n$, $\mathcal{F}(\mathfrak{m}^n)$ will denote the set $\mathfrak{m}^n$ equipped with the same group operations.

**Proposition 2.1.5.** Let $F(X, Y)$ be a formal group law defined over a complete local ring $R$ with maximal ideal $\mathfrak{m}$. Then for each $n \geq 1$, the identity map induces a group isomorphism

$$\frac{\mathcal{F}(\mathfrak{m}^n)}{\mathcal{F}(\mathfrak{m}^{n+1})} \cong \frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}.$$

*Proof.* See (Silverman 2009), §IV.3, Proposition 3.2. □

## 2.2 Honda's Theory of Commutative Formal Groups

One method for analyzing the structure of commutative formal groups comes from (Honda 1970). In this section we will summarize a few of the main results.

**Theorem 2.2.1** (Honda 1970, Theorem 1)**.** Let $R$ be a ring of characteristic 0 and $K$ the field of fractions of $R$. If $F(X, Y)$ is a formal group law over $R$, then there exists a unique power series $f(T) \in K[[T]]$ satisfying $F(X, Y) = f^{-1}(f(X) + f(Y))$.

We refer to $f$ as the *formal logarithm* (or simply *logarithm*) of the formal group law $F(X, Y)$ and denote it by $\log_F$. In fact, the proof of the above theorem provides us with a method for computing the logarithm. Let $P(T) \in \mathcal{O}_K[[T]]$ be the power

series defined by

$$P(T)\frac{\partial F}{\partial X}(0,T) = 1.$$

Then $P(T)dT$ is a right-invariant differential form on $F(X,Y)$, called the *invariant differential of the formal group law* $F(X,Y)$. Set

$$Q(T) = \int P(T)dT \in K[[T]].$$

It is easy to show that $Q(F(X,Y)) = Q(X) + Q(Y)$; thus $\log_F(T) = Q(T)$ is the desired power series. Applying this technique to the additive and multiplicative formal group laws, we obtain

$$\log_{\widehat{\mathbb{G}}_a}(T) = T \qquad \text{and} \qquad \log_{\widehat{\mathbb{G}}_m}(T) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}T^n}{n}.$$

**Corollary 2.2.2.** Let $R$ be a ring of characteristic 0 and $K$ the field of fractions of $R$. If $F(X,Y)$ is a formal group law over $R$, then $\log_F(T) : F(X,Y) \to \widehat{\mathbb{G}}_a(X,Y)$ is a strict isomorphism over $K$.

*Proof.* The fact that it is a homomorphism follows immediately from the definition of the logarithm, since

$$\log_F(F(X,Y)) = F(X) + F(Y) = \widehat{\mathbb{G}}_a(F(X), F(Y)).$$

To see that it has leading term $T$, notice that the power series $P(T) = \left(\frac{\partial F}{\partial X}(0,T)\right)^{-1}$ has leading term 1. □

The inverse power series is a homomorphism $\widehat{\mathbb{G}}_a \to F(X,Y)$ over $R$, called the *formal exponential* (or simply *exponential*) and denoted $\exp_F$.

We now approach the problem from the reverse direction. Given a ring $R$ with field of fractions $K$ and a power series $f(T) \in K[[T]]$ with zero constant term, it is clear that $F(X,Y) = f^{-1}(f(X) + f(Y))$ defines a commutative formal group law over

$K$; we would like to find reasonable restrictions on $K$ such that $F(X,Y)$ actually has coefficients in $R$.

Let $K$ be a discretely valued field with characteristic 0. Denote the ring of integers of $K$ and its maximal ideal by $\mathcal{O}_K$ and $\mathfrak{m}_K$, respectively, and suppose the residue field $k = \mathcal{O}_K/\mathfrak{m}_K$ has characteristic $p > 0$. We also assume that there is an endomorphism $\sigma$ of $K$ such that

$$\sigma(x) \equiv x^q \pmod{\mathfrak{m}_K}$$

for all $x \in \mathcal{O}_K$, where $q$ is a power of $p$. For instance, if $K$ is a finite extension of $\mathbb{Q}_p$, we can take $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$ to be the Frobenius endomorphism. Fix a prime element $\pi \in \mathcal{O}_K$.

Let $K_\sigma[[T]]$ (resp. $\mathcal{O}_\sigma[[T]]$) be the non-commutative ring of formal power series in $T$ with multiplication law $Tx = \sigma(x)T$ for $x \in K$ (resp. $x \in \mathcal{O}_K$). For $f \in K[[x]]$ with zero constant term and $u = \sum_{i=0}^{\infty} c_i T^i \in K_\sigma[[T]]$, we define an element $u \star f$ of $K[[x]]$ with zero constant term by

$$(u \star f)(x) = \sum_{i=0}^{\infty} c_i f^{\sigma^i}(x^{q^i}).$$

**Definition 2.2.3.** An element $u \in \mathcal{O}_\sigma[[T]]$ is *special* if $u \equiv \pi \pmod{\deg 1}$. Given a special element $u \in \mathcal{O}_\sigma[[T]]$, we say that $f \in K[[x]]$ has *Honda type* $u$ if $f(x) \equiv x \pmod{\deg 2}$ and $(u \star f)(x) \equiv 0 \pmod{\mathfrak{m}_K}$.

The special elements now provide us with a way of generating formal group laws over $\mathcal{O}_K$:

**Theorem 2.2.4** (Honda 1970, Theorem 2)**.** Let $u \in \mathcal{O}_\sigma[[T]]$ be a special element. If $f \in K[[x]]$ has Honda type $u$, then $F(X,Y) = f^{-1}(f(X) + f(Y))$ is a formal group law over $\mathcal{O}_K$. If $g \in K[[x]]$ also has Honda type $u$ and $G(X,Y) = g^{-1}(g(X) + g(Y))$, then $\exp_G \circ \log_F : F(X,Y) \to G(X,Y)$ is a strict isomorphism over $\mathcal{O}_K$.

So in this setting, studying strict isomorphisms between formal group laws reduces to analyzing the Honda type of their associated logarithms. If $\mathcal{O}_K = \mathbb{Z}_p$, then the special elements $u$ can be chosen to have the form $u(T) = p + a_1T + \cdots + a_hT^h$, where $p \mid a_i$ for each $1 \leq i \leq n-1$ and $h$ is the height of $F(X,Y)$; thus we have a 1-1 correspondence between strong isomorphism classes of formal group laws of height $h$ over $\mathbb{Z}_p$ and Eisenstein polynomials of degree $h$ in $\mathbb{Z}_p[T]$.

## 2.3 Formal Groups Associated with Elliptic Curves

Let $K$ be a complete local field with ring of integers $\mathcal{O}_K$ and maximal ideal $\mathfrak{m}_K$. Also let $E$ be an elliptic curve defined over $K$ with minimal model

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

Using the change of variables $z = -\dfrac{x}{y}$, we can expand the group law on $E$ as a formal power series in $z_1$ and $z_2$:

$$\widehat{E}(z_1, z_2) = z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) + \cdots \in \mathcal{O}_K[[z_1, z_2]].$$

Since addition on $E$ is both commutative and associative, the same is true for $\widehat{E}(z_1, z_2)$. We refer to $\widehat{E}(X,Y)$ as the *formal group law associated with the minimal model of* $E$. The corresponding formal group is denoted $\widehat{E}(\mathfrak{m}_K)$.

Suppose $E$ is defined over $\mathbb{Q}_p$, $E$ has good reduction at the prime $p$, and let $\sigma$ be the Frobenius endomorphism for the reduced curve $E/\mathbb{F}_p$. Then $\sigma$ has characteristic polynomial $\Psi(T) = T^2 - a_pT + p$, where $a_p = \mathrm{tr}(\sigma) = 1 + p - \#E(\mathbb{F}_p)$, and it follows that $\log_{\widehat{E}}$ satisfies

$$p\log_{\widehat{E}}(T) - a_p\log_{\widehat{E}}(T^p) + \log_{\widehat{E}}(T^{p^2}) \equiv 0 \pmod{p\mathbb{Z}_p}.$$

So the Honda type of $\log_{\widehat{E}}$ is the unique Eisenstein factor of the polynomial $\Psi(T)$. Recall that $a_p \equiv 0 \pmod{p}$ if and only if $E$ has supersingular reduction at $p$; so if $E$ has good ordinary reduction at $p$, then the Honda type of $\log_{\widehat{E}}$ is a linear factor of $\Psi(T)$, whereas if $E$ has good supersingular reduction at $p$, then the Honda type of $\log_{\widehat{E}}$ is $\Psi(T)$ itself. This establishes a useful result:

**Proposition 2.3.1.** Let $E/\mathbb{Q}_p$ be an elliptic curve with good reduction at $p$. Then the associated formal group law $\widehat{E}(X,Y)$ over $\mathbb{Z}_p$ has

(i) height 1, if $E$ has ordinary reduction at $p$;

(ii) height 2, if $E$ has supersingular reduction at $p$.

Instead of examining $\widehat{E}(X,Y)$ directly, it is often preferable to study a strictly isomorphic formal group law, which is closely related to the $L$-function of $E$.

**Definition 2.3.2.** If $E$ is an elliptic curve over $\mathbb{Q}$, then the *local $L$-function $L_p(s)$ of $E$ at the prime $p$* is defined as follows:

(i) If $E$ has good reduction at $p$, then $L_p(s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$, where $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)$ and $\tilde{E}(\mathbb{F}_p)$ is the reduction of $E$ modulo $p\mathbb{Z}_p$.

(ii) If $E$ has split multiplicative reduction at $p$, then $L_p(s) = (1 - p^{-s})^{-1}$.

(iii) If $E$ has nonsplit multiplicative reduction at $p$, then $L_p(s) = (1 + p^{-s})^{-1}$.

(iv) If $E$ has additive reduction at $p$, then $L_p(s) = 1$.

The *global $L$-function $L(s)$ of $E$* is the product of $L_p(s)$ over all primes $p$.

Suppose $L(s) = \sum_{n=1}^{\infty} a(n) n^{-s}$; we associate a power series $f_L(T)$ with $L(s)$ by defining

$$f_L(T) = \sum_{n=1}^{\infty} \frac{a(n)}{n} T^n.$$

**Theorem 2.3.3.** The power series $F_L(X,Y) = f_L^{-1}(f_L(X) + f_L(Y))$ is a formal group law over $\mathbb{Z}$ that is strictly isomorphic to $\widehat{E}(X,Y)$ over $\mathbb{Z}$.

*Proof.* See (Honda 1970), Theorem 9 or (Hazewinkel 2012), Propositions 33.1.8 and 33.1.16. Note that by Theorem 2.1.3, it suffices to prove that $\widehat{E}(X,Y)$ and $F_L(X,Y)$ are strictly isomorphic as formal group laws over $\mathbb{Z}_p$ for each prime $p$. □

## 2.4 Constructing a Canonical System of Points

We now examine Kobayashi's method of constructing a canonical system of points, which is replicated (in a slightly more general setting) in (Kitajima and Otsuki 2016). Fix an odd prime $p$, and for each $n \geq 0$, choose a primitive $p^n$th root of unity $\zeta_{p^n}$ such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. Also put $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ and $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$.

Define an endomorphism $\varphi$ of $\mathbb{Q}_p[[T]]$ by

$$\varphi\left(\sum_{n=0}^{\infty} a_n T^n\right) = \sum_{n=0}^{\infty} a_n \varphi(T)^n,$$

where $\varphi(T) = (1+T)^p - 1$. Consider the power series

$$f(T) = \sum_{n=0}^{\infty} \frac{(-1)^n \varphi^{2n}(T)}{p^n} = \sum_{n=0}^{\infty} \frac{(1+T)^{p^{2n}} - 1}{p^n}.$$

Then $f(T)$ has Honda type $T^2 + p$, so it is the logarithm of a formal group law $F(X,Y)$ over $\mathbb{Z}_p$ that is strictly isomorphic to $\widehat{E}(X,Y)$ for an elliptic curve $E$ with trace of Frobenius $a_p = 0$. (Recall that for $p \geq 5$, this is equivalent to the condition that $E$ has supersingular reduction at $p$.)

Put $\mathfrak{m}_{-1} = p\mathbb{Z}_p$ and let $\mathfrak{m}_n$ be the maximal ideal of $\mathbb{Z}_p[\zeta_{p^{n+1}}]$ for $n \geq 0$. By Corollary 2.2.2, $\log_F : F(X,Y) \to \widehat{\mathbb{G}}_a(X,Y)$ is an isomorphism, so it induces a bijection of the corresponding formal groups $\mathcal{F}(p\mathbb{Z}_p) \to \widehat{\mathbb{G}}_a(p\mathbb{Z}_p)$, where $\widehat{\mathbb{G}}_a(p\mathbb{Z}_p)$ is

simply the group $p\mathbb{Z}_p$ with its usual addition operation; thus we can select $\epsilon \in p\mathbb{Z}_p$ such that $\log_F(\epsilon) = \dfrac{p}{p+1}$.

**Definition 2.4.1.** Define a system of points $(c_n)_{n\geq -2}$ by $c_{-2} = [2]\epsilon$, $c_{-1} = \epsilon$, and $c_n = \epsilon[+]_{\mathcal{F}}(\zeta_{p^{n+1}} - 1)$, where $[+]_{\mathcal{F}}$ denotes the addition operation on the formal group $\mathcal{F}(p\mathbb{Z}_p)$.

For $m \geq n$, let $\mathrm{Tr}_{m/n} : \mathcal{F}(\mathfrak{m}_m) \to \mathcal{F}(\mathfrak{m}_n)$ denote the trace map

$$\mathrm{Tr}_{m/n}(x) = \sum_{\sigma \in \mathrm{Gal}(K_m/K_n)} x^\sigma.$$

Then the system of points $(c_n)_{n\geq -2}$ possesses two essential properties:

**Proposition 2.4.2.** (i) $\mathrm{Tr}_{0/-1}(c_0) = -2c_{-1}$.

(ii) $\mathrm{Tr}_{n+1/n}(c_{n+1}) = -c_{n-1}$ for all $n \geq 0$.

(iii) The points $c_n^\sigma$ ($\sigma \in G_n$) generate $\mathcal{F}(\mathfrak{m}_n)/\mathcal{F}(\mathfrak{m}_{n-1})$ as a $\mathbb{Z}_p$-module.

*Proof.* See (Kobayashi 2003), Lemma 8.9 for (i)-(ii) and Proposition 8.11 for (iii). □

These properties, in turn, enable the construction of the Coleman maps that are at the heart of Kobayashi's theory. What follows is a brief summary of §8.5 from (Kobayashi 2003). Define sequences $(c_n^+)_{n\geq 0}$ and $(c_n^-)_{n\geq 0}$ by

$$c_n^+ = \begin{cases} (-1)^{(n+2)/2} c_n, & \text{if } n \text{ is even,} \\ (-1)^{(n+1)/2} c_{n-1}, & \text{if } n \text{ is odd,} \end{cases} \qquad c_n^- = \begin{cases} (-1)^{(n+1)/2} c_n, & \text{if } n \text{ is odd,} \\ (-1)^{n/2} c_{n-1}, & \text{if } n \text{ is even.} \end{cases}$$

Also define the *nth even (resp. odd) norm subgroup* $\widehat{E}^{\pm}(\mathfrak{m}_n)$ of $\widehat{E}(\mathfrak{m}_n)$ by

$$\widehat{E}^+(\mathfrak{m}_n) = \{P \in \widehat{E}(\mathfrak{m}_n) \mid \mathrm{Tr}_{n/m+1} P \in \widehat{E}(\mathfrak{m}_m) \text{ for even } m,\ 0 \leq m < n\}$$

$$\widehat{E}^-(\mathfrak{m}_n) = \{P \in \widehat{E}(\mathfrak{m}_n) \mid \mathrm{Tr}_{n/m+1} P \in \widehat{E}(\mathfrak{m}_m) \text{ for odd } m,\ -1 \leq m < n\}$$

It can be shown as a consequence of Proposition 2.4.2 that the groups $\widehat{E}(\mathfrak{m}_n)$ are generated as $\mathbb{Z}_p$-modules by the images of $c_n^{\pm}$ under the strict isomorphism $\mathcal{F}(\mathfrak{m}_n) \to \widehat{E}(\mathfrak{m}_n)$. If we allow $k_n$ to be the cyclotomic field $\mathbb{Q}_p(\zeta_{p^{n+1}})$, then the norm subgroups are related to the groups $E^{\pm}$ defined in Section 1.4 via isomorphisms $\widehat{E}^{\pm}(\mathfrak{m}_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to E^{\pm}(k_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$.

Let $T$ be the Tate module of $E$ and $V = T \otimes \mathbb{Q}_p$. Now $\widehat{E}^{\pm}(\mathfrak{m}_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$ may be thought of as subgroups of $H^1(k_n, V/T)$ via the Kummer map; so we may define $H^1_{\pm}(k_n, T)$ to be the exact annihilators of the subgroups $\widehat{E}^{\pm}(\mathfrak{m}_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$ with respect to the Tate pairing

$$H^1(k_n, V/T) \times H^1(k_n, T) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

As it turns out, $H^1_{\pm}(k_n, T)$ are the kernels of the maps

$$P_n^{\pm} : H^1(k_n, T) \to \mathbb{Z}_p[G_n], \qquad x \mapsto \sum_{\sigma \in G_n} (x^{\sigma}, c_n^{\pm})_n \sigma,$$

where $(\cdot, \cdot)_n : \mathcal{F}(\mathfrak{m}_n) \times H^1(k_n, T) \to \mathbb{Z}_p$ is the pairing induced by the cup product.

Let $G_\infty = \varprojlim G_n$, $\Lambda = \mathbb{Z}_p[[G_\infty]]$, and $\gamma_n$ be a topological generator for $\Lambda$. Also let $\gamma_n$ be the image of $\gamma$ in $\Lambda_n = \mathbb{Z}_p[G_n]$. If $\omega_n(x) = (1+x)^{p^n} - 1$, then we may identify $\Lambda_n$ with $\mathbb{Z}_p[\Delta][x]/(\omega_n(x))$, where $\Delta \cong \mathbb{Z}/(p-1)\mathbb{Z}$, via the map $\gamma_n \mapsto 1 + x$. Specializing to the even and odd cases, define

$$\tilde{\omega}_n^+(x) = \prod_{2 \le m \le n,\ m \text{ even}} \Phi_m(1+x),$$
$$\tilde{\omega}_n^-(x) = \prod_{1 \le m \le n,\ m \text{ odd}} \Phi_m(1+x),$$

where $\Phi_m(x)$ is the $p^m$th cyclotomic polynomial. Set $\Lambda_n^{\pm} := \mathbb{Z}_p[\Delta][x]/(\omega_n^{\pm}(x))$. Then the *nth even (resp. odd) Coleman map* is the map $\mathrm{Col}_n^{\pm}$ that makes the following diagram commute:

$$\begin{array}{ccc} H^1(k_n,T) & \xrightarrow{\mathrm{Col}_n^{\pm}} & \Lambda_n^{\pm} \\ \downarrow & & \downarrow \\ \frac{H^1(k_n,T)}{H^1_{\pm}(k_n,T)} & \xrightarrow{P_n^{\pm}} & \Lambda_n \end{array}$$

(The right vertical arrow is multiplication by $\tilde{\omega}_n^{\mp}$.) These maps are compatible, and accordingly the *even (resp. odd) Coleman map* $\mathrm{Col}^{\pm} : H^1_{\mathrm{Iw}}(T) \to \Lambda$ is defined by taking the limit of the maps $\mathrm{Col}_n^{\pm}$.

In the next chapter we will consider an alternate way of constructing logarithms of formal group laws strictly isomorphic to $\widehat{E}(X,Y)$ over $\mathbb{Z}_p$, and show that it is still possible to construct a system of points satisfying the conditions of Proposition 2.4.2. Thus the Coleman maps may be arrived at using the same argument.

Chapter 3

# FORMAL GROUPS OF ELLIPTIC CURVES VIA FUNCTIONAL EQUATIONS

## 3.1 The Functional Equation Lemma

Let $K$ be a ring with subring $R$, $\sigma : K \to K$ a ring homomorphism, $I$ an ideal of $R$, $p$ a rational prime, $q$ a power of $p$, and $s_1, s_2, \ldots \in K$. We follow (Hazewinkel 2012) in outlining a method for generating commutative formal group laws over $R$. Assume the following:

(i) $\sigma(x) \equiv x^q \pmod{I}$ for all $x \in R$,

(ii) $p \in I$,

(iii) $s_i I \subset R$ for $i = 1, 2, \ldots$,

(iv) $I^r x \subset I$ implies $I^r \sigma(x) \subset I$ for all $r \in \mathbb{N}$, $x \in K$.

For instance, these conditions are satisfied when we take $K$ to be a local field with finite residue field $k$, $R = \mathcal{O}_K$ its ring of integers, $I = \mathfrak{m}_K$ the maximal ideal of $\mathcal{O}_K$, $p$ the characteristic of $k$, $q = p$, $\sigma$ the Frobenius endomorphism, and $s_i \in \pi^{-1}\mathcal{O}_K$, where $\pi$ denotes a fixed uniformizer of $\mathcal{O}_K$.

Suppose we have a power series $g(T) = \sum_{n=1}^{\infty} b_n T^n$ with coefficients in $R$. We define a new power series $f_g(T) \in K[[T]]$ by means of the functional equation

$$f_g(T) = g(T) + \sum_{n=1}^{\infty} s_n \sigma_*^n f_g(t^{q^n}),$$

where $\sigma_*^n f_g(T)$ is the power series obtained by applying $\sigma^n$ to the coefficients of $f_g(T)$. In practice, the coefficients of $f_g(T)$ can be computed as follows: Write

$f_g(T) = \sum_{n=1}^{\infty} d_n T^n$. For an index $n \geq 1$, suppose $n = p^r n'$, where $p \nmid n'$. Then

$$d_n = b_n + s_1 \sigma(d_{n/p}) + s_2 \sigma^2(d_{n/p^2}) + \cdots + s_r \sigma^r(d_{n/p^r}).$$

If we fix our choice of $R$, $K$, $I$, $\sigma$, $p$, and $q$, then the definition of $f_g(T)$ depends only on the power series $g(T)$ and the numbers $s_1, s_2, \ldots$. In this situation, we say that $f_g(T)$ *satisfies a functional equation with parameters* $s_1, s_2, \ldots$. If $f_g(T)$ and $f_h(T)$ are two power series satisfying functional equations with the same parameters, we say they *satisfy a functional equation of the same type.*

**Theorem 3.1.1** (Functional Equation Lemma)**.** Let $R$, $K$, $I$, $\sigma$, $p$, $q$, and $s_1, s_2, \ldots$ be as above. Let $g(T) = \sum_{n=1}^{\infty} b_n T^n$ and $h(T) = \sum_{n=1}^{\infty} c_n T^n$ be two power series over $R$, and suppose $b_1$ and $c_1$ are invertible in $R$. Then

(i) $F_g(X, Y) = f_g^{-1}(f_g(X) + f_g(Y))$ is a commutative formal group law over $R$.

(ii) Suppose $F_g(X, Y) = f_g^{-1}(f_g(X) + f_g(Y))$ and $F_h(X, Y) = f_h^{-1}(f_h(X) + f_h(Y))$ are two formal group laws over $R$. Then $F_g(X, Y)$ and $F_h(X, Y)$ are strictly isomorphic over $R$ if and only if $f_g$ and $f_h$ satisfy a functional equation of the same type. In this case, the strict isomorphism is given by $f_h^{-1}(f_g(T)) : F_g(X, Y) \to F_h(X, Y)$.

*Proof.* This is a slightly modified statement of the Functional Equation Lemma in §2.2 of (Hazewinkel 2012). □

The Functional Equation Lemma provides us with a useful generalization of Theorem 2.2.4. Note that the power series $f_g$ and $f_g^{-1}$ that appear in the Functional Equation Lemma are the logarithm and exponential of the formal group law $F_g(X, Y)$, respectively.

For an example of how to describe a formal group law via the functional equation parameters of its logarithm, take $R = \mathbb{Z}_p$, $K = \mathbb{Q}_p$, $I = p\mathbb{Z}_p$, $q = p$, $\sigma = \mathrm{id}$, $s_1 = \dfrac{1}{p}$, and $s_2 = s_3 = \cdots = 0$. Define

$$g(T) = \begin{cases} \sum_{n \text{ odd}} \frac{T^n - T^{2n}}{n}, & \text{if } p = 2, \\ \sum_{(n,p)=1} \frac{(-1)^{n-1} T^n}{n}, & \text{else.} \end{cases}$$

Then, recalling the logarithm of the multiplicative formal group law from §2.1, we see that

$$\log_{\widehat{\mathbb{G}}_m}(T) = g(T) + \frac{1}{p} f_g(T^p),$$

so $\log_{\widehat{\mathbb{G}}_m}$ satisfies a functional equation with parameters $\dfrac{1}{p}, 0, 0, \ldots$ over the ring $\mathbb{Z}_p$.

## 3.2 Functional Equations and Linear Recurrence Relations

Fix a rational prime $p$ and let $g(T) = b_1 T + \cdots + b_{p-1} T^{p-1} \in \mathbb{Z}_p[T]$ be a polynomial of degree less than $p$ with zero constant term. In this section we describe a method for deriving an explicit formula for the coefficients of the power series $f_g(T)$ when $\sigma = \mathrm{id}$, $q = p$, and there are only finitely many nonzero parameters $s_1, s_2, \ldots$.

Suppose $s_i = 0$ for all $i \geq r$, where $r$ is some positive integer. Then $f_g(T)$ is defined via the functional equation

$$f_g(T) = g(T) + s_1 g(T^p) + s_2 g(T^{p^2}) + \cdots + s_r g(T^{p^r}).$$

If we write $f_g(T) = \sum_{n=1}^{\infty} d_n T^n$, then the coefficients $d_n$ obey the recursion

$$d_n = b_n + s_1 d_{n/p} + \cdots + s_r d_{n/p^r}.$$

(We let $b_n = 0$ for all $n \geq p$.) For a fixed $k$ with $1 \leq k \leq p-1$, define the sequence $(D_n^{(k)})_{n \geq 0}$ by $D_n^{(k)} = d_{kp^n}$. Due to our restriction on $g(T)$, the sequence $D_n^{(k)}$ satisfies a

homogenous linear recursion of order $r$:

$$D_n^{(k)} = s_1 D_{n-1}^{(k)} + \cdots + s_r D_{n-r}^{(k)} \qquad (n \geq r).$$

There is a standard method for solving recursions of this form. For instance, if $s_i = 0$ for all $i \geq 3$, then we obtain:

**Proposition 3.2.1.** Let $g(T) = b_1 T + \cdots + b_{p-1} T^{p-1} \in \mathbb{Z}_p[T]$ and $f_g(T)$ be a power series defined by the functional equation

$$f_g(T) = g(T) + s_1 f_g(T^p) + s_2 f_g(T^{p^2}).$$

(i) If $s_1^2 + 4s_2 \neq 0$, write $f_g(T) = \sum_{n=1}^{\infty} d_n T^n$; then

$$d_n = \begin{cases} b_k \dfrac{\left(s_1+\sqrt{s_1^2+4s_2}\right)^{r+1} - \left(s_1-\sqrt{s_1^2+4s_2}\right)^{r+1}}{2^{r+1}\sqrt{s_1^2+4s_2}}, & \text{if } n = kp^r \text{ for } 1 \leq k \leq p-1 \text{ and } r \geq 0, \\ 0, & \text{else.} \end{cases}$$

(ii) If $s_1^2 + 4s_2 = 0$, then

$$f_g(T) = \sum_{r=0}^{\infty} \frac{(r+1)s_1^r g(T^{p^r})}{2^r}.$$

*Proof.* (i) By the above, we have a homogeneous linear recursion

$$D_n^{(k)} = s_1 D_{n-1}^{(k)} + s_2 D_{n-2}^{(k)} \qquad (n \geq 2).$$

This recursion has characteristic polynomial $\Psi(x) = x^2 - s_1 x - s_2$. If $s_1^2 + 4s_2 \neq 0$, then $\Psi(x)$ has distinct roots $\alpha_{1,2} = \dfrac{1}{2}\left(s_1 \pm \sqrt{s_1^2 + 4s_2}\right)$ in some fixed algebraic closure of $\mathbb{Q}_p$, so

$$D_n^{(k)} = c_1^{(k)} \alpha_1^n + c_2^{(k)} \alpha_2^n$$

for constants $c_1^{(k)}$ and $c_2^{(k)}$. Letting $n = 0$ and then $n = 1$, we obtain the system of equations

$$\begin{cases} c_1^{(k)} + c_2^{(k)} = b_k, \\ c_1^{(k)} \alpha_1 + c_2^{(k)} \alpha_2 = s_1 b_k, \end{cases}$$

which we can use to solve for $c_1^{(k)}$ and $c_2^{(k)}$:

$$c_1^{(k)} = b_k \frac{s_1 + \sqrt{s_1^2 + 4s_2}}{2\sqrt{s_1^2 + 4s_2}} \qquad \text{and} \qquad c_2^{(k)} = b_k \frac{s_1 - \sqrt{s_1^2 + 4s_2}}{2\sqrt{s_1^2 + 4s_2}}.$$

Substituting these values into our expression for $D_n^{(k)}$ gives the desired result.

(ii) If $s_1^2 + 4s_2 = 0$, then the characteristic polynomial $\Psi(x)$ has the unique root $\alpha = \frac{s_1}{2}$, so that

$$D_n^{(k)} = \left(c_1^{(k)} + c_2^{(k)} n\right) \alpha^n.$$

Letting $n = 0$ and then $n = 1$, it is easy to see that $c_1^{(k)} = c_2^{(k)} = b_k$, and consequently

$$D_n^{(k)} = (n+1) \left(\frac{s_1}{2}\right)^n b_k.$$

Since $d_n = 0$ whenever $n \geq p$ and $p \nmid n$, the power series $f_g(T)$ may be written as

$$\begin{aligned} f_g(T) &= \sum_{r=0}^{\infty} \sum_{k=1}^{p-1} (r+1) \left(\frac{s_1}{2}\right)^r b_k T^{kp^r} \\ &= \sum_{r=0}^{\infty} \frac{(r+1)s_1^r}{2^r} \sum_{k=1}^{p-1} b_k T^{kp^r} \\ &= \sum_{r=0}^{\infty} \frac{(r+1)s_1^r}{2^r} g(T^{p^r}). \end{aligned}$$

□

## 3.3 Functional Equation Parameters of Formal Groups Associated with Elliptic Curves

Throughout this section, we will assume that $E$ is an elliptic curve defined over $\mathbb{Q}$ and let $\widehat{E}(X, Y)$ denote the formal group law over $\mathbb{Z}$ associated with the minimal

model of $E$. Let $L(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ be the $L$-function of $E$ and

$$f_L(T) = \sum_{n=1}^{\infty} \frac{a(n)}{n} T^n$$

be the associated power series, introduced in §2.3. Our first goal is to find the functional equation parameters of the logarithm of $\widehat{E}(X, Y)$. To handle the case of good reduction, we will need a technical result. We say that an Euler product

$$\prod_{p \text{ prime}} \left(1 + a(p)p^{-s} + \cdots + a(p^m)p^{-ms} + \cdots\right)$$

has *degree* $k$ if for each prime $p$, there is a polynomial $P_p(T) \in \mathbb{C}[T]$ of degree at most $k$ with zero constant term such that

$$1 + a(p)T + \cdots + a(p^m)T^m = \frac{1}{1 - P_p(T)}.$$

**Lemma 3.3.1.** An Euler product with $a(1) = 1$ is of degree 2 if and only if for each prime $p$ there exists $d_p \in \mathbb{C}$ satisfying

$$a(p^m) = a(p)a(p^{m-1}) + d_p a(p^{m-2})$$

for all $m \geq 2$. In this situation, the $p$th Euler factor is given by

$$\frac{1}{1 - a(p)p^{-s} - d_p p^{-2s}}.$$

*Proof.* See (Knapp 1992), Corollary 7.8. □

In particular, the Euler product expansion of $L(s)$ has degree 2 (we set $d_p = -p$ if $E$ has good reduction at $p$ and $d_p = 0$ for the other primes). Thus the coefficients $a(n)$ may be computed recursively using the above formula.

**Proposition 3.3.2.** Fix a prime $p$ and let $a_p$ be the trace of the Frobenius endomorphism.

(i) If $E$ has good reduction at $p$, then $\log_{\widehat{E}}$ satisfies a functional equation with parameters $\frac{a_p}{p}, -\frac{1}{p}, 0, 0, \ldots$ over $\mathbb{Z}_p$.

(ii) If $E$ has split multiplicative reduction at $p$, then $\log_{\widehat{E}}$ satisfies a functional equation with parameters $\frac{1}{p}, 0, 0, \ldots$ over $\mathbb{Z}_p$; that is, $\widehat{E}(X, Y)$ is strictly isomorphic to the multiplicative formal group $\widehat{\mathbb{G}}_m(X, Y)$ over $\mathbb{Z}_p$.

(iii) If $E$ has nonsplit multiplicative reduction at $p$, then $\log_{\widehat{E}}$ satisfies a functional equation with parameters $-\frac{1}{p}, 0, 0, \ldots$ over $\mathbb{Z}_p$.

(iv) If $E$ has additive reduction at $p$, then $\log_{\widehat{E}}(T) = T$; that is, $\widehat{E}(X, Y)$ is strictly isomorphic to the additive formal group $\widehat{\mathbb{G}}_a(X, Y)$ over $\mathbb{Z}_p$.

*Proof.* By Theorem 2.3.3, it suffices to prove that the power series $f_L(T)$ satisfies a functional equation with the given parameters. Suppose $E$ has good reduction at $p$. Then the local $L$-function of $E$ at $p$ is $L_p(s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$, so by Lemma 3.2.1, we have the recursion relation

$$a(p^m) = a_p a(p^{m-1}) - p a(p^{m-2})$$

for $m \geq 2$. (Note we have used the fact that the trace of Frobenius $a_p$ is equal to the term $a(p)$.) Dividing on both sides by $p^m$ gives

$$\frac{a(p^m)}{p^m} = \frac{a_p}{p} \frac{a(p^{m-1})}{p^{m-1}} - \frac{1}{p} \frac{a(p^{m-2})}{p^{m-2}}.$$

Since the numbers $a(n)$ are multiplicative, the same argument establishes that

$$\frac{a(n)}{n} = \frac{a_p}{p} \frac{a(n/p)}{n/p} - \frac{1}{p} \frac{a(n/p^2)}{n/p^2}$$

whenever $p^2 \mid n$. If $p \mid n$ and $p^2 \nmid n$, then by the multiplicative property we have simply

$$\frac{a(n)}{n} = \frac{a_p}{p} \frac{a(n/p)}{n/p}.$$

Recognizing $\dfrac{a(n)}{n}$, $\dfrac{a(n/p)}{n/p}$, and $\dfrac{a(n/p^2)}{n/p^2}$ as the coefficients of $T^n$ in the power series $f_L(T)$, $f_L(T^p)$, and $f_L(T^{p^2})$, respectively, we see that

$$g(T) := f_L(T) - \frac{a_p}{p} f_L(T^p) + \frac{1}{p} f_L(T^{p^2})$$

has coefficient 0 for all terms of order divisible by $p$. In particular, the denominators of all coefficients of $g(T)$ are not divisible by $p$, and so $g(T) \in \mathbb{Z}_p[T]$. Thus we have the functional equation

$$f_L(T) = g(T) + \frac{a_p}{p} f_L(T^p) - \frac{1}{p} f_L(T^{p^2}),$$

which establishes (i).

Now assume that $E$ has multiplicative reduction at $p$. Then the local $L$-function of $E$ at $p$ is $L_p(s) = (1 - \epsilon p^{-s})^{-1}$, where $\epsilon = 1$ if the multiplicative reduction is split and $\epsilon = -1$ if it is nonsplit. It follows that

$$L_p(s) = \sum_{n=0}^{\infty} \frac{\epsilon^n}{(p^n)^s},$$

so

$$a(m) = \begin{cases} \epsilon^n, & \text{if } m = p^n \text{ for some } n \geq 0, \\ 0, & \text{else.} \end{cases}$$

Therefore the power series $f_L(T)$ may be written as

$$f_L(T) = \sum_{n=0}^{\infty} \left(\frac{\epsilon}{p}\right)^n T^{p^n}.$$

This clearly satisfies the functional equation

$$f_L(T) = T + \frac{\epsilon}{p} f_L(T^p),$$

thus establishing (ii) and (iii). Case (iv) is immediate. □

**Corollary 3.3.3.** Let $E$ be an elliptic curve of good reduction at the prime $p$, and choose $b_1, \ldots, b_{p-1} \in \mathbb{Z}_p$. Then the power series $f(T) = \sum_{n=1}^{\infty} d_n T^n$ with coefficients given by the rule

$$d_n = \begin{cases} b_k \frac{\left(a_p + \sqrt{a_p^2 - 4p}\right)^{r+1} - \left(a_p - \sqrt{a_p^2 - 4p}\right)^{r+1}}{2^{r+1} p^r \sqrt{a_p^2 - 4p}}, & \text{if } n = kp^r \text{ for } 1 \leq k \leq p-1 \text{ and } r \geq 0, \\ 0, & \text{else,} \end{cases}$$

is the logarithm of a formal group law that is strictly isomorphic to $\widehat{E}(X, Y)$ over $\mathbb{Z}_p$.

*Proof.* Apply Proposition 3.2.1(i) with $s_1 = \dfrac{a_p}{p}$ and $s_2 = -\dfrac{1}{p}$. □

## 3.4 The Case of Supersingular Reduction

As in the previous section, we will let $E/\mathbb{Q}$ be an elliptic curve and $\widehat{E}(X, Y)$ the formal group law over $\mathbb{Z}$ associated with its global minimal model. Now assume $E$ has supersingular reduction at an odd prime $p$. By a well-known result, this is equivalent to stating that the trace of the Frobenius endomorphism $a_p$ for the reduced elliptic curve $E/\mathbb{F}_p$ satisfies $a_p \equiv 0 \pmod{p}$. Combining this with the Hasse bound $|a_p| \leq 2\sqrt{p}$, we see immediately that for $p \geq 5$, the elliptic curve $E$ has supersingular reduction at $p$ if and only if $a_p = 0$. The cases $p = 2, 3$ with nonzero trace will need to be treated separately.

If $a_p = 0$, then the expression for $d_n$ in Corollary 3.3.3 simplifies to

$$d_n = \begin{cases} b_k \frac{\sqrt{-4p}^{r+1} - (-\sqrt{-4p})^{r+1}}{2^{r+1} p^r \sqrt{-4p}}, & \text{if } n = kp^r \text{ for } 1 \leq k \leq p-1 \text{ and } r \geq 0, \\ 0, & \text{else.} \end{cases}$$

Note that

$$b_k \frac{\sqrt{-4p}^{r+1} - (-\sqrt{-4p})^{r+1}}{2^{r+1}p^r\sqrt{-4p}} = b_k \frac{(-p)^{r/2}(1-(-1)^{r+1})}{2p^r}$$
$$= \begin{cases} b_k \left(-\frac{1}{p}\right)^{r/2}, & \text{if } r \text{ is even,} \\ 0, & \text{if } r \text{ is odd.} \end{cases}$$

Thus we can construct a formal group law strictly isomorphic to $\widehat{E}(X,Y)$ over $\mathbb{Z}_p$ by taking as our logarithm a power series $f_g(T) = \sum_{n=1}^{\infty} d_n T^n$ with coefficients

$$d_n = \begin{cases} \frac{(-1)^r b_k}{p^r}, & \text{if } n = kp^{2r} \text{ for } 1 \le k \le p-1 \text{ and } r \ge 0, \\ 0, & \text{else.} \end{cases}$$

We may write $f_g(T)$ as

$$f_g(T) = \sum_{r=0}^{\infty}\sum_{k=1}^{p-1} \frac{(-1)^r b_k}{p^r} T^{kp^{2r}} = \sum_{n=0}^{\infty} \frac{(-1)^r}{p^r} \sum_{k=1}^{p-1} b_k T^{kp^{2r}}$$
$$= \sum_{n=0}^{\infty} \frac{(-1)^r g(T^{p^{2r}})}{p^r}.$$

In short, we have proven the following:

**Proposition 3.4.1.** Let $p$ be prime. Suppose $E/\mathbb{Q}_p$ is an elliptic curve with good supersingular reduction at $p$ and $a_p = 0$. Then, for any polynomial $g(T) \in \mathbb{Z}_p[T]$ of degree less than $p$ with zero constant term, the power series

$$f_g(T) = \sum_{r=0}^{\infty} \frac{(-1)^r g(T^{p^{2r}})}{p^r}$$

is the logarithm of a formal group law that is strictly isomorphic to $\widehat{E}(X,Y)$ over $\mathbb{Z}_p$.

Now suppose $E$ has good supersingular reduction at $p = 3$, but $a_3 \neq 0$. By Hasse's bound, the only other possible values for the trace are $a_3 = \pm 3$. Substituting $a_3 = 3$

into the value for the trace in Corollary 3.3.3, we obtain

$$d_n = \begin{cases} b_k \frac{(3+\sqrt{-3})^{r+1}-(3-\sqrt{-3})^{r+1}}{2^{r+1}\cdot 3^r\sqrt{-3}}, & \text{if } n = k\cdot 3^r \text{ for } k = 1 \text{ or } 2 \text{ and } r \geq 0, \\ 0, & \text{else.} \end{cases}$$

Observe that

$$\begin{aligned} b_k \frac{(3+\sqrt{-3})^{r+1}-(3-\sqrt{-3})^{r+1}}{2^{r+1}\cdot 3^r\sqrt{-3}} &= \frac{b_k i^r}{3^{r/2}}\left[\left(\frac{(1-i\sqrt{3}}{2}\right)^{r+1} - \left(\frac{-1-i\sqrt{3}}{2}\right)^{r+1}\right] \\ &= \frac{b_k i^r}{3^{r/2}}(\zeta_6^{r+1} - \zeta_3^{r+1}), \end{aligned}$$

where we allow $\zeta_6$ to denote the primitive sixth root of unity $\zeta_6 = \frac{1}{2}(1-i\sqrt{3})$ and $\zeta_3$ the primitive third root of unity $\zeta_3 = \zeta_6^2 = \frac{1}{2}(-1-i\sqrt{3})$. The value of this expression depends on the congruence class of $r$ modulo 12; by straightforward computation, we find that $\frac{b_k i^r}{3^{r/2}}(\zeta_6^{r+1} - \zeta_3^{r+1})$ simplifies to

(i) $\frac{b_k}{3^{r/2}}$, if $r \equiv 0 \pmod{12}$,
(ii) $\frac{\sqrt{3}b_k}{3^{r/2}}$, if $r \equiv 1 \pmod{12}$,
(iii) $\frac{2b_k}{3^{r/2}}$, if $r \equiv 2 \pmod{12}$,
(iv) $\frac{\sqrt{3}b_k}{3^{r/2}}$, if $r \equiv 3 \pmod{12}$,
(v) $\frac{b_k}{3^{r/2}}$, if $r \equiv 4 \pmod{12}$,
(vi) $0$, if $r \equiv 5 \pmod{12}$,
(vii) $-\frac{b_k}{3^{r/2}}$, if $r \equiv 6 \pmod{12}$,
(viii) $-\frac{\sqrt{3}b_k}{3^{r/2}}$, if $r \equiv 7 \pmod{12}$,
(ix) $-\frac{2b_k}{3^{r/2}}$, if $r \equiv 8 \pmod{12}$,
(x) $-\frac{\sqrt{3}b_k}{3^{r/2}}$, if $r \equiv 9 \pmod{12}$,
(xi) $-\frac{b_k}{3^{r/2}}$, if $r \equiv 10 \pmod{12}$,
(xii) $0$, if $r \equiv 11 \pmod{12}$.

All of the above cases reduce to the form $\frac{\delta_r b_k}{3^{r/2}}$, where $\delta_r = 0, \pm 1, \pm\sqrt{3}$, or $\pm 2$, depending on the congruence class of $r$. So we can generate a formal group law strictly isomorphic to $\widehat{E}(X,Y)$ over $\mathbb{Z}_3$ by taking as our logarithm the power series with coefficients

$$d_n = \begin{cases} \frac{\delta_r b_k}{3^{r/2}}, & \text{if } n = k\cdot 3^r \text{ for } k = 1 \text{ or } 2 \text{ and } r \geq 0, \\ 0, & \text{else.} \end{cases}$$

Therefore $f_g(T)$ has the form

$$f_g(T) = \sum_{r=0}^{\infty} \sum_{k=1}^{2} \frac{\delta_r b_k}{3^{r/2}} T^{k \cdot 3^r} = \sum_{r=0}^{\infty} \frac{\delta_r}{3^{r/2}} \left( b_1 T^{3^r} + b_2 T^{2 \cdot 3^r} \right)$$
$$= \sum_{r=0}^{\infty} \frac{\delta_r}{3^{r/2}} g(T^{3^r}).$$

If $a_3 = -3$, then running through a similar series of computations, we see that

$$d_n = \begin{cases} \frac{b_k i^r}{3^{r/2}} (\zeta_6^{5r+5} - \zeta_6^{4r+4}), & \text{if } n = k \cdot 3^r \text{ for } k = 1 \text{ or } 2 \text{ and } r \geq 0, \\ 0, & \text{else.} \end{cases}$$

Once again, the value of the coefficient $d_n$ depends on the congruence class of $r$ modulo 12; testing each possibility shows that $\frac{b_k i^r}{3^{r/2}} (\zeta_6^{5r+5} - \zeta_6^{4r+4})$ simplifies to

(i) $\frac{b_k}{3^{r/2}}$, if $r \equiv 0 \pmod{12}$,
(ii) $-\frac{\sqrt{3} b_k}{3^{r/2}}$, if $r \equiv 1 \pmod{12}$,
(iii) $\frac{2b_k}{3^{r/2}}$, if $r \equiv 2 \pmod{12}$,
(iv) $-\frac{\sqrt{3} b_k}{3^{r/2}}$, if $r \equiv 3 \pmod{12}$,
(v) $\frac{b_k}{3^{r/2}}$, if $r \equiv 4 \pmod{12}$,
(vi) $0$, if $r \equiv 5 \pmod{12}$,
(vii) $-\frac{b_k}{3^{r/2}}$, if $r \equiv 6 \pmod{12}$,
(viii) $\frac{\sqrt{3} b_k}{3^{r/2}}$, if $r \equiv 7 \pmod{12}$,
(ix) $-\frac{2b_k}{3^{r/2}}$, if $r \equiv 8 \pmod{12}$,
(x) $\frac{\sqrt{3} b_k}{3^{r/2}}$, if $r \equiv 9 \pmod{12}$,
(xi) $-\frac{b_k}{3^{r/2}}$, if $r \equiv 10 \pmod{12}$,
(xii) $0$, if $r \equiv 11 \pmod{12}$.

In summary, we have proven:

**Proposition 3.4.2.** Let $E/\mathbb{Q}_3$ be an elliptic curve with good supersingular reduction at 3 and trace of Frobenius $a_3 = \pm 3$. Then for any polynomial $g(T) = b_1 T + b_2 T^2 \in \mathbb{Z}_3[T]$, the power series

$$f_g(T) = \sum_{r=0}^{\infty} \frac{\delta_r g(T^{3^r})}{3^{r/2}}$$

is the logarithm of a formal group law that is strictly isomorphic to $\widehat{E}(X,Y)$ over $\mathbb{Z}_3$, where

$$\delta_r = \begin{cases} 0, & \text{if } r \equiv 5,11 \pmod{12}, \\ 1, & \text{if } r \equiv 0,4 \pmod{12}, \\ -1, & \text{if } r \equiv 6,10 \pmod{12}, \\ \text{sign}(a_3)\sqrt{3}, & \text{if } r \equiv 1,3 \pmod{12}, \\ -\text{sign}(a_3)\sqrt{3}, & \text{if } r \equiv 7,9 \pmod{12}, \\ 2, & \text{if } r \equiv 2 \pmod{12}, \\ -2, & \text{if } r \equiv 8 \pmod{12}. \end{cases}$$

Now we consider the case that $E$ has supersingular reduction at $p = 2$ and $a_2 = \pm 2$. The coefficients $d_n$ are given by

$$d_n = \begin{cases} b_1 \frac{(2+\sqrt{-4})^{r+1} - (2-\sqrt{-4})^{r+1}}{2^{r+1} \cdot 2^r \cdot \sqrt{-4}}, & \text{if } n = 2^r \text{ for some } r \geq 0, \\ 0, & \text{else.} \end{cases}$$

Note that

$$\begin{aligned} b_1 \frac{(2+\sqrt{-4})^{r+1} - (2-\sqrt{-4})^{r+1}}{2^{r+1} \cdot 2^r \cdot \sqrt{-4}} &= -\frac{b_1 i}{2^{(r+1)/2}} \left[ \left( \frac{1+i}{\sqrt{2}} \right)^{r+1} - \left( \frac{1-i}{\sqrt{2}} \right)^{r+1} \right] \\ &= -\frac{b_1 i}{2^{(r+1)/2}} \cdot \begin{cases} (\zeta_8^{r+1} - \zeta_8^{7r+7}), & \text{if } a_2 = 2, \\ (\zeta_8^{3r+3} - \zeta_8^{5r+5}), & \text{if } a_2 = -2, \end{cases} \end{aligned}$$

where $\zeta_8$ is the primitive eighth root of unity $\zeta_8 = \dfrac{1+i}{\sqrt{2}}$. The value of this expression depends on the congruence class of $r$ modulo 8; testing each possibility, we see that $-\dfrac{b_1 i}{2^{(r+1)/2}}(\zeta_8^{r+1} - \zeta_8^{7r+7})$ simplifies to

| $a_2 = 2$ | $a_2 = -2$ |
|---|---|
| (i) $\frac{b_1}{2^{r/2}}$, if $r \equiv 0 \pmod 8$, | (i) $\frac{b_1}{2^{r/2}}$, if $r \equiv 0 \pmod 8$, |
| (ii) $\frac{\sqrt{2}b_1}{2^{r/2}}$, if $r \equiv 1 \pmod 8$, | (ii) $-\frac{\sqrt{2}b_1}{2^{r/2}}$, if $r \equiv 1 \pmod 8$, |
| (iii) $\frac{b_1}{2^{r/2}}$, if $r \equiv 2 \pmod 8$, | (iii) $\frac{b_1}{2^{r/2}}$, if $r \equiv 2 \pmod 8$, |
| (iv) $0$, if $r \equiv 3 \pmod 8$, | (iv) $0$, if $r \equiv 3 \pmod 8$, |
| (v) $-\frac{b_1}{2^{r/2}}$, if $r \equiv 4 \pmod 8$, | (v) $-\frac{b_1}{2^{r/2}}$, if $r \equiv 4 \pmod 8$, |
| (vi) $-\frac{\sqrt{2}b_1}{2^{r/2}}$, if $r \equiv 5 \pmod 8$, | (vi) $\frac{\sqrt{2}b_1}{2^{r/2}}$, if $r \equiv 5 \pmod 8$, |
| (vii) $-\frac{b_1}{2^{r/2}}$, if $r \equiv 6 \pmod 8$, | (vii) $-\frac{b_1}{2^{r/2}}$, if $r \equiv 6 \pmod 8$, |
| (viii) $0$, if $r \equiv 7 \pmod 8$. | (viii) $0$, if $r \equiv 7 \pmod 8$. |

All of these cases have the form $\frac{\lambda_r b_1}{2^{r/2}}$, where $\lambda_r = 0, \pm 1$, or $\pm\sqrt{2}$, depending on the congruence class of $r$ and the sign of $a_2$. We conclude that:

**Proposition 3.4.3.** Let $E/\mathbb{Q}_2$ be an elliptic curve with good supersingular reduction at 2 and trace of Frobenius $a_2 = \pm 2$. Then, for any $b_1 \in \mathbb{Z}_2$, the power series

$$f(T) = \sum_{r=0}^{\infty} \frac{\lambda_r b_1 T^{2^r}}{2^{r/2}}$$

is the logarithm of a formal group law that is strictly isomorphic to $\widehat{E}(X, Y)$ over $\mathbb{Z}_2$, where

$$\lambda_r = \begin{cases} 0, & \text{if } r \equiv 3, 7 \pmod 8, \\ 1, & \text{if } r \equiv 0, 2 \pmod 8, \\ -1, & \text{if } r \equiv 4, 6 \pmod 8, \\ \text{sign}(a_2)\sqrt{2}, & \text{if } r \equiv 1 \pmod 8, \\ -\text{sign}(a_2)\sqrt{2}, & \text{if } r \equiv 5 \pmod 8. \end{cases}$$

## 3.5 Canonical Systems of Points Revisited

To conclude this chapter, we show how the formal logarithms derived in the previous section can be used to construct canonical systems of points (see §2.4). Fix an odd prime $p$, and for each $n \geq 1$, choose a primitive $p^n$th root of unity $\zeta_{p^n}$ such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. Denote the $n$th layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$ by $K_n = \mathbb{Q}_p(\zeta_{p^{n+1}})$ and its Galois group by $G_n = \mathrm{Gal}(K_n/\mathbb{Q}_p)$. Also put $\mathfrak{m}_{-1} = p\mathbb{Z}_p$ and let $\mathfrak{m}_n$ be the maximal ideal of $\mathbb{Z}_p[\zeta_{p^{n+1}}]$ for all $n \geq 0$.

Let

$$f(T) = \sum_{r=0}^{\infty} \frac{(-1)^r T^{p^{2r}}}{p^r},$$

so that by Proposition 3.4.1, $F(X,Y) = f^{-1}(f(X)+f(Y))$ is a formal group law over $\mathbb{Z}_p$ that is strictly isomorphic to $\widehat{E}(X,Y)$, the formal group law associated with an elliptic curve of supersingular reduction at $p$ and $a_p = 0$. Denote the corresponding formal group over the ideal $\mathfrak{m}_n$ by $\mathcal{F}(\mathfrak{m}_n)$. Using the fact that the logarithm $f : \mathcal{F}(\mathfrak{m}_n) \to \mathfrak{m}_n$ is a bijection, we define a system of points $(d_n)_{n \geq -2}$ as follows:

$$f(d_{-2}) = \frac{2p}{p+1}, \qquad f(d_{-1}) = \frac{p}{p+1},$$

and

$$f(d_n) = \frac{p}{p+1} + \sum_{r=0}^{\left[\frac{n+1}{2}\right]} \frac{(-1)^r}{p^r}(\zeta_{p^{n+1-2r}} - 1) \text{ for } n \geq 0.$$

**Proposition 3.5.1.** (i) $\mathrm{Tr}_{0/-1}(d_0) = -2d_{-1}$.

(ii) $\mathrm{Tr}_{n+1/n}(d_{n+1}) = -d_{n-1}$ for all $n \geq 0$.

(iii) The points $d_n^\sigma$ ($\sigma \in G_n$) generate $\mathcal{F}(\mathfrak{m}_n)/\mathcal{F}(\mathfrak{m}_{n-1})$ as a $\mathbb{Z}_p$-module for all $n \geq 0$.

*Proof.* Let

$$k(T) = \sum_{r=0}^{\infty} \frac{(-1)^r[(1+T)^{p^{2r}} - 1]}{p^r}$$

and $(c_n)_{n\geq -2}$ be the system of points defined in §2.4. Then $f(d_n) = k(c_n)$ for all $n \geq -2$, so the result follows immediately from Proposition 2.4.2. □

The situation is slightly different when the trace is nonzero. First we make an observation about the sequences $(\delta_r)$ and $(\lambda_r)$, defined in the previous section:

**Lemma 3.5.2.** (i) $\sqrt{3}\delta_{r+1} = a_3\delta_r - \sqrt{3}\delta_{r-1}$ for all $r \geq 1$.

(ii) $\sqrt{2}\lambda_{r+1} = a_2\lambda_r - \sqrt{2}\lambda_{r-1}$ for all $r \geq 1$.

*Proof.* These are easily confirmed by direct computation. □

Consider the power series

$$k_3(T) = \sum_{r=0}^{\infty} \frac{\delta_r[(1+T)^{3^r} - 1]}{3^{r/2}}.$$

By Honda theory, this is the logarithm of a formal group law $F_3(X, Y)$ over $\mathbb{Z}_3$ that is strictly isomorphic to $\widehat{E}(X, Y)$ when $E$ is an elliptic curve of supersingular reduction at 3 and $a_3 = \pm 3$. Similarly,

$$k_2(T) = \sum_{r=0}^{\infty} \frac{\lambda_r[(1+T)^{2^r} - 1]}{2^{r/2}}$$

is the logarithm of a formal group law $F_2(X, Y)$ over $\mathbb{Z}_2$ that is strictly isomorphic to $\widehat{E}(X, Y)$ when $E$ has supersingular reduction at 2 and $a_2 = \pm 2$. By an extension of the argument in (Kobayashi 2003), there exist canonical systems of points generating $\mathcal{F}_3(\mathfrak{m}_n)/\mathcal{F}_3(\mathfrak{m}_{n-1})$ and $\mathcal{F}_2(\mathfrak{m}_n)/\mathcal{F}_2(\mathfrak{m}_{n-1})$ as $\mathbb{Z}_p[G_n]$-modules. However, the computations involving the trace map $\mathrm{Tr}_{n+1/n}$ are slightly altered.

For $p = 2$ or 3, set $c_{-2} = [2]\epsilon$, $c_{-1} = \epsilon$, and

$$c_n = \epsilon[+]_{\mathcal{F}_p}(\zeta_{p^{n+1}} - 1) \qquad \text{for } n \geq 0,$$

where $\epsilon$ is chosen so that $k_p(\epsilon) = \dfrac{p}{p + 1 - a_p}$. Then:

**Proposition 3.5.3.** (i) $\mathrm{Tr}_{0/-1}(c_0) = (a_p - 2)c_{-1}$.

(ii) $\mathrm{Tr}_{n+1/n}(c_{n+1}) = a_p c_n - c_{n-1}$ for all $n \geq 0$.

*Proof.* We will prove (ii) when $p = 3$; all the other cases rely on a similar strategy. Since the logarithm $k_3$ is a bijection between $\mathcal{F}_3(\mathfrak{m}_n)$ and $\mathfrak{m}_n$, it suffices to show $\mathrm{Tr}_{n+1/n}(k_3(c_{n+1})) = a_3 k_3(c_n) - k_3(c_{n-1})$. Indeed,

$$\begin{aligned}
\mathrm{Tr}_{n+1/n}(k_3(c_{n+1})) &= \mathrm{Tr}_{n+1/n}\left(\frac{3}{4-a_3} + \sum_{r=0}^{n+2} \frac{\delta_r}{3^{r/2}}(\zeta_{3^{n+2-r}} - 1)\right) \\
&= \mathrm{Tr}_{n+1/n}\left(\frac{3}{4-a_3}\right) + \mathrm{Tr}_{n+1/n}(\zeta_3 - 1) + \mathrm{Tr}_{n+1/n}\left(\sum_{r=1}^{n+2} \frac{\delta_r}{3^{r/2}}(\zeta_{3^{n+2-r}} - 1)\right) \\
&= \frac{9}{4-a_3} - 3 + 3\sum_{r=1}^{n+2} \frac{\delta_r}{3^{r/2}}(\zeta_{3^{n+2-r}} - 1) \\
&= \frac{3a_3 - 3}{4-a_3} + \sum_{r=1}^{\infty} \frac{\sqrt{3}\delta_r}{3^{(r-1)/2}}(\zeta_{3^{n+2-r}} - 1).
\end{aligned}$$

Applying Lemma 3.5.2 and re-indexing,

$$\begin{aligned}
\mathrm{Tr}_{n+1/n}(k_3(c_{n+1})) &= \frac{3a_3 - 3}{4-a_3} + \sum_{r=0}^{n+1} \frac{a_3\delta_r - \sqrt{3}\delta_{r-1}}{3^{r/2}}(\zeta_{3^{n+1-r}} - 1) \\
&= \frac{3a_3 - 3}{4-a_3} + a_3 \sum_{r=0}^{n+1} \frac{\delta_r}{3^{r/2}}(\zeta_{3^{n+1-r}} - 1) - \sum_{r=0}^{n+1} \frac{\delta_r}{3^{r/2}}(\zeta_{3^{n-r}} - 1) \\
&= \frac{3a_3 - 3}{4-a_3} + a_3\left(k_3(c_n) - \frac{3}{4-a_3}\right) - \left(k_3(c_{n-1}) - \frac{3}{4-a_3}\right) \\
&= a_3 k_3(c_n) - k_3(c_{n-1}).
\end{aligned}$$

□

Notice that this result is compatible with Proposition 2.4.2 when $a_p = 0$.

If instead we use the formal logarithms

$$f_3(T) = \sum_{r=0}^{\infty} \frac{\delta_r T^{3^r}}{3^{r/2}} \qquad \text{and} \qquad f_2(T) = \sum_{r=0}^{\infty} \frac{\lambda_r T^{2r}}{2^{r/2}},$$

then we would select as our system of points the $(d_n)_{n\geq -2}$ satisfying

$$f_p(d_{-2}) = \frac{2p}{p+1-a_p}, \qquad f_p(d_{-1}) = \frac{p}{p+1-a_p} \qquad (p = 2 \text{ or } 3),$$

and

$$f_p(d_n) = \frac{p}{p+1-a_p} + \begin{cases} \sum_{r=0}^{n+1} \frac{\delta_r}{3^{r/2}}(\zeta_{3^{n+1-r}} - 1), & \text{if } p = 3, \\ \sum_{r=0}^{n+1} \frac{\lambda_r}{2^{r/2}}(\zeta_{2^{n+1-r}} - 1), & \text{if } p = 2. \end{cases}$$

By construction, the system of points $(d_n)$ will also satisfy the conditions of Proposition 3.5.3 and generate the corresponding quotient of formal groups $\mathcal{F}_p(\mathfrak{m}_n)/\mathcal{F}_p(\mathfrak{m}_{n-1})$ as a $\mathbb{Z}_p[G_n]$-module when $p = 2$ or 3.

# Chapter 4

# FORMAL MODULES OF ELLIPTIC CURVES

## 4.1 Motivation

Regardless of whether we use Honda theory or the Functional Equation Lemma to construct our canonical system of points, one limitation is the requirement that our elliptic curve $E$ should be defined over the field $\mathbb{Q}$. It is for this reason that, in their study of the growth of the signed Selmer groups, both (Lei and Sujatha 2020) and (Kitajima and Otsuki 2016) impose the following condition: If $p$ is a fixed rational prime and $E$ is an elliptic curve define over a number field $K$, then the completion $K_v$ of $K$ at any prime $v$ of $K$ lying over $p$ for which $E$ has good supersingular reduction is $K_v = \mathbb{Q}_p$. The difficulty arises in the proof of Theorem 2.3.3, which establishes that the formal group law over $\mathbb{Z}$ associated with the minimal model of $E/\mathbb{Q}$ is strictly isomorphic to that generated by the logarithm $f_L(T)$, where $f_L(T)$ denotes the power series corresponding to the $L$-function of $E/\mathbb{Q}$. The proof reduces to the case of formal group laws over finite fields in two steps:

(i) Two formal group laws over $\mathbb{Z}$ are strictly isomorphic over $\mathbb{Z}$ if and only if they are strictly isomorphic over $\mathbb{Z}_p$ for all primes $p$. (Local-Global Principle, Theorem 2.1.3)

(ii) Two formal group laws over $\mathbb{Z}_p$ are strictly isomorphic over $\mathbb{Z}_p$ if and only if their reductions modulo $p$ are isomorphic over $\mathbb{F}_p$. (Theorem 2.1.4)

Step (i) still holds when we replace $\mathbb{Z}$ with the ring of integers of an arbitrary number field $K$ and the $\mathbb{Z}_p$'s with the rings of integers of the completions of $K$ at each

of the non-Archimedean primes. Step (ii), on the other hand, fails when we consider formal group laws defined over integral closures of $\mathbb{Z}_p$ in certain finite extensions of $\mathbb{Q}_p$. However, it is possible to salvage Theorem 2.1.4 if we pass from formal group laws to formal modules.

## 4.2 Definitions and Important Properties

Let $R$ be a ring and $A$ an $R$-algebra. If $F(X,Y)$ is a formal group law over $A$, let $\mathrm{End}_A(F(X,Y))$ denote the ring of endomorphisms of $F(X,Y)$ over $A$ (by the remarks following Definition 2.1.2, this ring contains an isomorphic copy of $\mathbb{Z}$ via the map $n \mapsto [n]$). Also let $J : \mathrm{End}_A(F(X,Y)) \to A$ be the ring homomorphism that sends each $\alpha(T) \in \mathrm{End}_A(F(X,Y))$ to the element $a \in A$ such that $\alpha(T) \equiv aT \pmod{\deg 2}$.

**Definition 4.2.1.** Let $R$ be a ring. A *(one-dimensional) formal $R$-module over an $R$-algebra $A$* is a pair $(F(X,Y), \rho_F)$, where $F(X,Y)$ is a (one-dimensional) commutative formal group law over $A$ and $\rho_F : R \to \mathrm{End}_A(F(X,Y))$ is a ring homomorphism that makes the following diagram commute:

$$\begin{array}{ccc} R & \xrightarrow{\rho_F} & \mathrm{End}_A(F(X,Y)) \\ & \searrow & \downarrow J \\ & & A \end{array}$$

Allowing $\rho_F : \mathbb{Z} \to \mathrm{End}_A(F(X,Y))$ to be the map $\rho_F(n) = [n]$, we see that every commutative formal group law over $A$ gives rise to a formal $\mathbb{Z}$-module over $A$.

**Definition 4.2.2.** Let $R$ be a ring and $(F(X,Y), \rho_F)$, $(G(X,Y), \rho_G)$ be two formal $R$-modules over the $R$-algebra $A$. A *homomorphism from $(F(X,Y), \rho_F)$ to $(G(X,Y), \rho_G)$ over $A$* is a homomorphism $\alpha(T) : F(X,Y) \to G(X,Y)$ of formal group laws over $A$

such that

$$\alpha \circ \rho_F(a) = \rho_G(a) \circ \alpha \qquad (\forall a \in R).$$

A (strict) isomorphism over $A$ is defined similarly.

If it happens that $A$ has characteristic 0, then the homomorphisms between $R$-modules over $A$ are simply the homomorphisms over $A$ of the underlying formal group laws:

**Proposition 4.2.3.** Let $R$ be a ring and $A$ an $R$-algebra of characteristic 0.

(i) Given a formal group law $F(X,Y)$ over $A$, there exists at most one ring homomorphism $\rho_F : R \to \mathrm{End}_A(F(X,Y))$ such that $(F(X,Y), \rho_F)$ is a formal $R$-module over $A$.

(ii) If $(F(X,Y), \rho_F)$ and $(G(X,Y), \rho_G)$ are two formal $R$-modules over $A$, then $\alpha(T) : F(X,Y) \to G(X,Y)$ is a homomorphism of formal group laws over $A$ if and only if it is a homomorphism of formal $R$-modules over $A$.

*Proof.* (i) Since $A$ has characteristic 0, the formal group law $F(X,Y)$ has a logarithm, say $f(T)$. If $K$ denotes the quotient field of $A$, then $f(T) : F(X,Y) \to \widehat{\mathbb{G}}_a(X,Y)$ is a strict isomorphism. The endomorphisms of $\widehat{\mathbb{G}}_a(X,Y)$ over $K$ are the power series $\alpha(T) \in K[[T]]$ with $\alpha(\widehat{\mathbb{G}}_a(X,Y)) = \widehat{\mathbb{G}}_a(\alpha(X), \alpha(Y))$, or equivalently $\alpha(X+Y) = \alpha(X) + \alpha(Y)$; clearly this only occurs if $\alpha(T) = aT$ for some $a \in K$. It follows that the endomorphisms of $F(X,Y)$ over $A$ take the form $f^{-1}(af(T))$ for some $a \in A$. Thus the only possible choice of $\rho_F : R \to \mathrm{End}_A(F(X,Y))$ is $\rho_F(r) = f^{-1}(rf(T))$.

(ii) Let $\alpha(T) : F(X,Y) \to G(X,Y)$ be a homomorphism of formal group laws over $A$. Since $A$ has characteristic 0, $F(X,Y)$ and $G(X,Y)$ have logarithms $f(T)$

and $g(T)$, respectively. By a similar logic as above, $\alpha(T)$ must have the form $\alpha(T) = g^{-1}(af(T))$ for some $a \in A$. It follows from (i) that

$$\begin{aligned}(\alpha \circ \rho_F(r))(T) &= g^{-1}(af(f^{-1}(rf(T)))) \\ &= g^{-1}(arf(T)) \\ &= g^{-1}(rg(g^{-1}(af(T)))) \\ &= (\rho_G(r) \circ \alpha)(T).\end{aligned}$$

So $\alpha$ is a homomorphism of the formal $R$-modules $(F(X,Y), \rho_F)$ and $(G(X,Y), \rho_G)$ over $A$. The reverse implication is true by definition.

□

**Corollary 4.2.4.** Let $R$ be a ring and $A$ an $R$-algebra of characteristic 0. Then two formal $R$-modules $(F(X,Y), \rho_F)$ and $(G(X,Y), \rho_G)$ over $A$ are strictly isomorphic if and only if the underlying formal groups $F(X,Y)$ and $G(X,Y)$ are strictly isomorphic over $A$.

For example, given any ring $R$ and $R$-algebra $A$, we define the additive formal $R$-module over $A$ to be the pair $(\widehat{\mathbb{G}}_a(X,Y), \rho_{\widehat{\mathbb{G}}_a})$, where $\widehat{\mathbb{G}}_a(X,Y) = X + Y$ is the additive formal group law over $A$ and $\rho_{\widehat{\mathbb{G}}_a}(r)(T) = rT$ for any $r \in R$. By the above corollary, any formal $R$-module over a field $K$ of characteristic 0 is strictly isomorphic to $(\widehat{\mathbb{G}}_a(X,Y), \rho_{\widehat{\mathbb{G}}_a})$. In fact, a similar result holds for fields of positive characteristic:

**Proposition 4.2.5.** Let $K$ be a field of characteristic $p > 0$. Then every formal $K$-module over a $K$-algebra $B$ is strictly isomorphic to $(\widehat{\mathbb{G}}_a(X,Y), \rho_{\widehat{\mathbb{G}}_a})$.

*Proof.* See (Hazewinkel 2012), Theorem 21.6.2. □

Let $K$ be a local field of characteristic 0 with ring of integers $\mathcal{O}_K$ and residue field $k$ of characteristic $p > 0$. For a prime $\nu$ of $K$, let $K_\nu$ denote the completion of $K$ at

$\nu$, and $\mathcal{O}_\nu$ its ring of integers. If we consider a formal $R$-module over $\mathcal{O}_K$, where $R$ is selected so that $\mathcal{O}_K$ is an $R$-algebra, then combining Corollary 4.2.4 with Theorem 2.1.3 yields:

**Theorem 4.2.6** (Local-Global Principle)**.** If $(F(X,Y),\rho_F)$ and $(G(X,Y),\rho_G)$ are formal $R$-modules over $\mathcal{O}_K$, then they are strictly isomorphic over $\mathcal{O}_K$ if and only if they are strictly isomorphic as $R$-modules over $\mathcal{O}_\nu$ for all non-Archimedean primes $\nu$ of $K$.

The following is analogous to Theorem 2.1.4:

**Theorem 4.2.7.** Two formal $\mathcal{O}_K$-modules over $\mathcal{O}_K$ are strictly isomorphic if and only if their reductions modulo $\mathfrak{m}_K$ are strictly isomorphic as formal $\mathcal{O}_K$-modules over $k$.

So we are primarily interested in studying the isomorphism classes of formal $\mathcal{O}_K$-modules over finite fields.

## 4.3 Classifying Formal Modules over Finite Fields

Throughout this section, $\mathcal{O}_K$ will denote the ring of integers of a finite extension $K$ of $\mathbb{Q}_p$, with maximal ideal $\mathfrak{m}_K$, uniformizer $\pi$, and residue field $k = \mathcal{O}_K/\mathfrak{m}_K$ of order $q$. The behavior of formal $\mathcal{O}_K$-modules over $k$ has much in common with that of formal group laws over $\mathbb{F}_p$. We extend the notion of height to formal $\mathcal{O}_K$-modules as follows:

**Definition 4.3.1.** Let $(F(X,Y),\rho_F)$ be a formal $\mathcal{O}_K$-module over $k$. The *$\mathcal{O}_K$-height of* $(F(X,Y),\rho_F)$ is the smallest positive integer $h$ such that

$$\rho_F(\pi)(T) \equiv 0 \pmod{\deg p^h},$$

assuming $\rho_F(\pi)$ is nonzero. If $\rho_F(\pi) = 0$, we say that $(F(X,Y), \rho_F)$ has $\mathcal{O}_K$-*height* $\infty$.

Note that if $\mathcal{O}_K = \mathbb{Z}_p$, then

$$\rho_F(\pi)(T) = \log_F^{-1}(p\log_F(T)) = [p](T),$$

so the $\mathbb{Z}_p$-height of a formal $\mathbb{Z}_p$-module over $\mathbb{F}_p$ is the same as the height of the underlying formal group law over $\mathbb{F}_p$.

We will need some facts from the theory of Brauer groups. Most of the information here comes from (Serre 1979), Chapter XII, §2. Let $D_n$ denote the *central division algebra over $K$ with rank $n^2$*, i.e., the division algebra of rank $n^2$ over $K$ whose center is precisely $K$. Let the finite extension $K'/K$ be a splitting field for $D_n$, so that $D_n \otimes_K K' \cong M_m(K')$, the $K'$-algebra of $(m \times m)$-matrices for some positive integer $m$. Denote this isomorphism by $\varphi$. The *reduced norm* on $D_n$ is the map $\mathrm{Nrd}_{D_n/K} : D_n \to K$ given by

$$\mathrm{Nrd}_{D_n/K}(a) = \det(\varphi(a \otimes 1)).$$

If $v$ is the normalized valuation on the field $K$, define $v' : D_n^\times \to \mathbb{Z}$ by $v'(x) = v(\mathrm{Nrd}_{D_n/K}(x))$, The image of $D_n^\times$ under $v'$ is contained in the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$; thus we may extend $v$ to a normalized valuation $w : D_n^\times \to \mathbb{Z}$ by setting

$$w(x) = \frac{1}{n}v'(x).$$

The *ring of integers* $\mathcal{O}_{D_n}$ of the central division algebra $D_n$ is the set

$$\mathcal{O}_{D_n} = \{x \in D_n : w(x) \geq 0\}.$$

**Proposition 4.3.2.** Let $D_n$ be a central division algebra of rank $n^2$ over a field $K$. There is a maximal subfield of $D_n$ that is unramified over $K$.

Now we return to the question of classifying formal $\mathcal{O}_K$-modules over $k$. The following construction and theorem are adapted from (Hazewinkel 2012), §24.5.

By class field theory, there is a maximal unramified extension $K^{\text{un}}$ of the field $K$. Let $(F(X,Y),\rho_F)$ be a formal $\mathcal{O}_K$-module over $k$ of $\mathcal{O}_K$-height $h$, and let $\bar{k}$ be the algebraic closure of $k$. Denote the ring of formal $\mathcal{O}_K$-module endomorphisms of $(F(X,Y),\rho_F)$ over $\bar{k}$ by $\mathcal{O}_K\text{-End}(F(X,Y))$. Consider the function $\sigma(T)=T^q$. We note that since $F(X,Y)$ and $\rho_f(a)$ $(a\in R)$ both have coefficients in $\mathbb{F}_q$,

$$\sigma(F(X,Y))=(F(X,Y))^q\equiv F(X^q,y^q)\equiv F(\sigma(X),\sigma(Y)) \pmod{p}$$

and

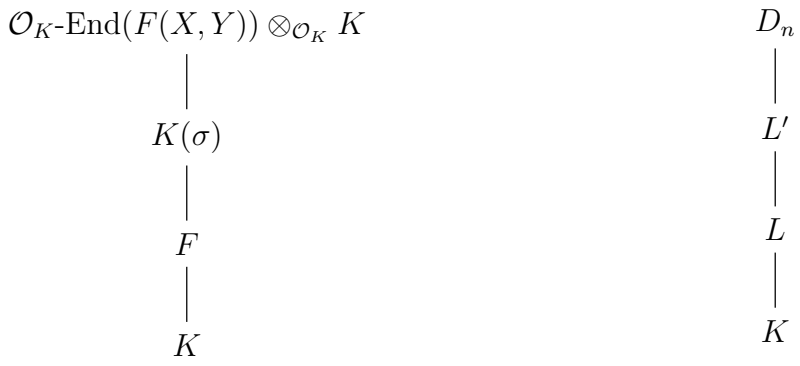
$$(\sigma\circ\rho_F(a))(T)=(\rho_F(a)(T))^q\equiv\rho_F(a)(T^q)\equiv(\rho_F(a)\circ\sigma)(T) \pmod{p}$$

for all $a\in\mathcal{O}_K$. Thus $\sigma\in\mathcal{O}_K\text{-End}(F(X,Y))$; we call $\sigma$ the *Frobenius formal $\mathcal{O}_K$-module endomorphism of* $(F(X,Y),\rho_F)$.

**Lemma 4.3.3.** $\mathcal{O}_K\text{-End}(F(X,Y))\cong\mathcal{O}_{D_n}$, the ring of integers of the central division algebra of rank $n^2$ over $K$.

*Proof.* The argument involves constructing a 'universal' formal $\mathcal{O}_K$-module to which $F(X,Y)$ is strictly isomorphic over $\bar{k}$; see (Hazewinkel 2012), Theorems 20.2.13 and 21.9.1. □

It follows that $\mathcal{O}_K\text{-End}(F(X,Y))\otimes_{\mathcal{O}_K}K$ is isomorphic to the division algebra $D_n$. The Frobenius endomorphism $\sigma$ generates a subfield $K(\sigma)$ of $\mathcal{O}_K\text{-End}(F(X,Y))\otimes_{\mathcal{O}_K}K$, which in turn corresponds to a subfield $L'$ of $D_n$ over $K$. By Proposition 4.3.2, there is a maximal unramified subextension $L/K$ of $L'$. Let $F$ be the corresponding unramified subextension $F/K$ of $K(\sigma)$, and $\mathcal{O}_F$ its ring of integers. In short, we are identifying the division algebras/fields in the following towers:

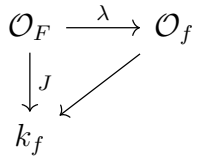



Define $\Phi(T) \in \mathcal{O}_F[T]$ to be the minimal polynomial of $\sigma$ over $F$. Also let $\mathcal{O}_K$-End$_k(F(X,Y))$ be the ring of formal $\mathcal{O}_K$-module endomorphisms of $F(X,Y)$ over $k$ (as opposed to $\bar{k}$).

**Lemma 4.3.4.** $\mathcal{O}_K$-End$_k(F(X,Y)) = \{\alpha \in \mathcal{O}_K\text{-End}(F(X,Y)) : \alpha \circ \sigma = \sigma \circ \alpha\}$.

*Proof.* The forward containment is obvious. For the reverse, let $\alpha(T)$ be a formal $\mathcal{O}_K$-module endomorphism of $F(X,Y)$ over $\bar{k}$. Then $\alpha(T) \in \mathcal{O}_K$-End$_k(F(X,Y))$ precisely when the coefficients $a_i$ of $\alpha(T)$ are elements of $k$. This occurs if and only if $a_i^q \equiv a_i \pmod{p}$ for all $i$, or equivalently, $\alpha \circ \sigma = \sigma \circ \alpha$. □

As a consequence of Lemma 4.3.4, $\mathcal{O}_F \subset \mathcal{O}_K$-End$_k(F(X,Y))$, and we can restrict the map $J : \mathcal{O}_K$-End$_k(F(X,Y)) \to k$ to $\mathcal{O}_F$. (Recall that $J$ sends each endomorphism $\alpha(T)$ to the coefficient of $T$.) Let $f$ be the residue field degree of the extension $K(\sigma)/K$ and $K_f/K$ the unique unramified subextension of $K^{\text{un}}$ of degree $f$; let $\mathcal{O}_f$ be its ring of integers and $k_f$ its residue field. There exists a unique isomorphism $\lambda$ that makes the following diagram commute:



(The map $\mathcal{O}_f \to k_f$ is the restriction of the projection map $\mathcal{O}^{\text{un}} \to \bar{k}$, where $\mathcal{O}^{\text{un}}$ is the ring of integers of the maximal unramified extension of $K$.)

**Definition 4.3.5.** The *characteristic $\mathcal{O}_K$-polynomial $\Psi(T)$ of the formal $\mathcal{O}_K$-module* $(F(X,Y), \rho_F)$ is the polynomial obtained by applying $\lambda$ to the coefficients of $\Phi(T)$.

**Theorem 4.3.6.** (i) $\Psi(T)$ is an Eisenstein polynomial over $\mathcal{O}_K$ of degree $h$.

(ii) Two formal $\mathcal{O}_K$-modules are strictly isomorphic over $\mathcal{O}_K$ if and only if the corresponding reduced formal modules over $k$ have the same characteristic $\mathcal{O}_K$-polynomial. In other words, the formal $\mathcal{O}_K$-modules over $\mathcal{O}_K$ of height $h$ are classified by Eisenstein polynomials over $\mathcal{O}_K$ of degree $h$.

Note that if $\mathcal{O}_K = \mathbb{Z}_p$, Theorem 4.3.6 reduces to the more familiar claim that formal group laws over $\mathbb{F}_p$ are classified by Eisenstein polynomials over $\mathbb{Z}_p$.

## 4.4 Formal Modules Associated with Elliptic Curves

Let $K$, $\mathcal{O}_K$, $\mathfrak{m}_K$, $k$, and $\pi$ be as in the previous section. Suppose $E$ is an elliptic curve over $K$ with good reduction and trace of Frobenius $a$. Also let $\widehat{E}(X,Y)$ be the formal group law over $\mathcal{O}_K$ associated with the minimal model of $E$.

**Definition 4.4.1.** The *formal $\mathcal{O}_K$-module associated with $E$* is the formal $\mathcal{O}_K$-module $(\widehat{E}(X,Y), \rho_{\widehat{E}})$ over $\mathcal{O}_K$, where $\rho_{\widehat{E}} : \mathcal{O}_K \to \text{End}_{\mathcal{O}_K}(\widehat{E}(X,Y))$ is defined by

$$\rho_E(r)(T) = \log_{\widehat{E}}^{-1}(r\log_{\widehat{E}}(T)) \qquad (r \in \mathcal{O}_K).$$

We can now give a partial description of the isomorphism classes of formal $\mathcal{O}_K$-modules associated with elliptic curves:

**Theorem 4.4.2.** There exist uniformizers $\pi_{\mathrm{ss}}, \pi_{\mathrm{ord}}$ of $\mathcal{O}_K$ and an element $\alpha \in \mathfrak{m}_K$ such that the formal $\mathcal{O}_K$-module $(\widehat{E}(X,Y), \rho_{\widehat{E}})$ has characteristic $\mathcal{O}_K$-polynomial

(i) $T^2 + \alpha T + \pi_{\mathrm{ss}}$, if $E$ has supersingular reduction;

(ii) $T + \pi_{\mathrm{ord}}$, if $E$ has ordinary reduction.

*Proof.* By general facts about elliptic curves, the Frobenius endomorphism of $E$ satisfies a monic quadratic polynomial over $\mathrm{End}(E)$; thus, by Theorem 4.3.6, the characteristic $\mathcal{O}_K$-polynomial of $(\widehat{E}(X,Y), \rho_{\widehat{E}})$ is a monic Eisenstein polynomial over $\mathcal{O}_K$ of degree one or two. Note that the reduction is supersingular if and only if the endomorphism ring $\mathcal{O}_K$-$\mathrm{End}(\widehat{E}(X,Y), \rho_{\widehat{E}})$ is an order in a quaternion algebra, which occurs precisely when the division algebra $D_h$ has rank 4 over $K$; i.e., when $(\widehat{E}(X,Y), \rho_{\widehat{E}})$ has $\mathcal{O}_K$-height 2. □

## 4.5 Future Work

Giving explicit descriptions of the elements $\alpha$, $\pi_{\mathrm{ss}}$, and $\pi_{\mathrm{ord}}$ in Theorem 4.4.2 will involve analyzing the behavior of the map $\lambda$ used in the definition of the characteristic $\mathcal{O}_K$-polynomial. It would be interesting to try to develop a variant of Proposition 3.3.2 for formal $\mathcal{O}_K$-modules; however, it is unclear how the $L$-series of $E/K$ would have to be modified to produce a logarithm whose corresponding formal $\mathcal{O}_K$-module would satisfy the same type of characteristic $\mathcal{O}_K$-polynomial as $(\widehat{E}(X,Y), \rho_{\widehat{E}})$.

Let $K$ be a number field, $v$ a prime of $K$, and $E/K$ an elliptic curve with good supersingular reduction at $v$. In order to generalize the construction of the canonical system of points in the case the completion $K_v$ is a non-trivial extension of $\mathbb{Q}_p$, it would be necessary to identify a formal logarithm $f(T)$ such that $F(X,Y) = f^{-1}(f(X) + f(Y))$ is the underlying formal group law of a formal $\mathcal{O}_{K_v}$-module over

$\mathcal{O}_{K_v}$ with characteristic $\mathcal{O}_{K_v}$-polynomial equal to $T^2 + \alpha T + \pi_{\mathrm{ss}}$. One would then have to find generators for the $\mathcal{O}_K$-modules $\mathcal{F}(\mathfrak{m}_{n+1})/\mathcal{F}(\mathfrak{m}_n)$, where the $\mathfrak{m}_n$'s are the maximal ideals in the layers of the cyclotomic $\mathbb{Z}_p$-extension of $K$. While the classification of formal $\mathcal{O}_K$-modules over $\mathcal{O}_K$ presents a clear parallel with that of formal group laws over $\mathbb{F}_p$, more research is needed to determine whether this approach is feasible.

REFERENCES


Coates, J. and Sujatha, R. 2005. "Fine Selmer Groups of Elliptic Curves over $p$-adic Lie Extensions." *Math. Ann.* 331:809–839.

———. 2010. *Galois Cohomology of Elliptic Curves.* Tata Institute of Fundamental Research.

Diamond, Fred and Shurman, Jerry. 2016. *A First Course in Modular Forms.* Springer.

Hamidi, Parham and Ray, Jishnu. 2020. "Conjecture A and $\mu$-Invariant for Selmer Groups of Supersingular Elliptic Curves." doi:10.48550/ARXIV.2006.14134.

Hazewinkel, Michiel. 1977. "On Norm Maps for One Dimensional Formal Groups III." *Duke Mathematical Journal* 44 (2): 305–314.

———. 2012. *Formal Groups and Applications.* AMS Chelsea Publishing.

Honda, Taira. 1970. "On the Theory of Commutative Formal Groups." *J. Math Soc. Japan* 22 (2): 213–246.

Iovita, Adrian and Pollack, Robert. 2006. "Iwasawa Theory of Elliptic Curves at Supersingular Primes over $\mathbb{Z}_p$-Extensions of Number Fields." *J. reine angew.* 598:71–103.

Jürgen Neukirch, Alexander Schmidt and Wingberg, Kay. 2000. *Cohomology of Number Fields.* Springer.

Kato, Kazuya. 2004. "$p$-adic Hodge Theory and Values of Zeta Functions of Modular Forms." *Astérisque* 295:117–290.

Kitajima, Takahiro and Otsuki, Rei. 2016. *On the Plus and Minus Selmer Groups for Elliptic Curves at Supersingular Primes.* doi:10.48550/ARXIV.1607.03612.

Knapp, Anthony W. 1992. *Elliptic Curves.* Princeton University Press.

Kobayashi, Shin-ichi. 2003. "Iwasawa Theory for Elliptic Curves at Supersingular Primes." *Inventiones math.* 152:1–36.

Kolyvagin, V.A. and Logachev, D. Yu. 1990. "Finiteness of the Shafarevich-Tate Group and the Group of Rational Points for Some Modular Abelian Varieties." *Leningrad Math. J.* 1 (5): 1229–1253.

Kummer, E. E. 1852. "Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen." *Journal für die reine und angewandte Mathematik* 44:93–146.

Lazard, Michel. 1955. "Sur les groupes de Lie formels à un paramètre." *Bulletin de la S.M.F.* 83:251–274.

Lei, Antonio and Sujatha, Ramdorai. 2020. "On Selmer Groups in the Supersingular Reduction Case." *Tokyo Journal of Mathematics* 43, no. 2 (December). doi:10.3836/tjm/1502179319.

Mazur, Barry. 1972. "Rational Points of Abelian Varieties with Values in Towers of Number Fields." *Inventiones math.,* no. 18: 183–266.

Schneider, Peter. 1985. "$p$-adic Height Pairings II." *Inventiones math.* 79:329–374.

Serre, Jean-Pierre. 1979. *Local Fields.* Springer.

———. 1997. *Galois Cohomology.* Springer.

Silverman, Joseph H. 2009. *The Arithmetic of Elliptic Curves.* Springer.

Washington, Lawrence C. 1997. *Introduction to Cyclotomic Fields.* Springer.