IWASAWA INVARIANTS OF ELLIPTIC CURVES AND p-ADIC MEASURES

A Thesis Submitted

in Partial Fulfilment of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

by

Rupam Barman

(Roll Number: 06612301)

to the

DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI

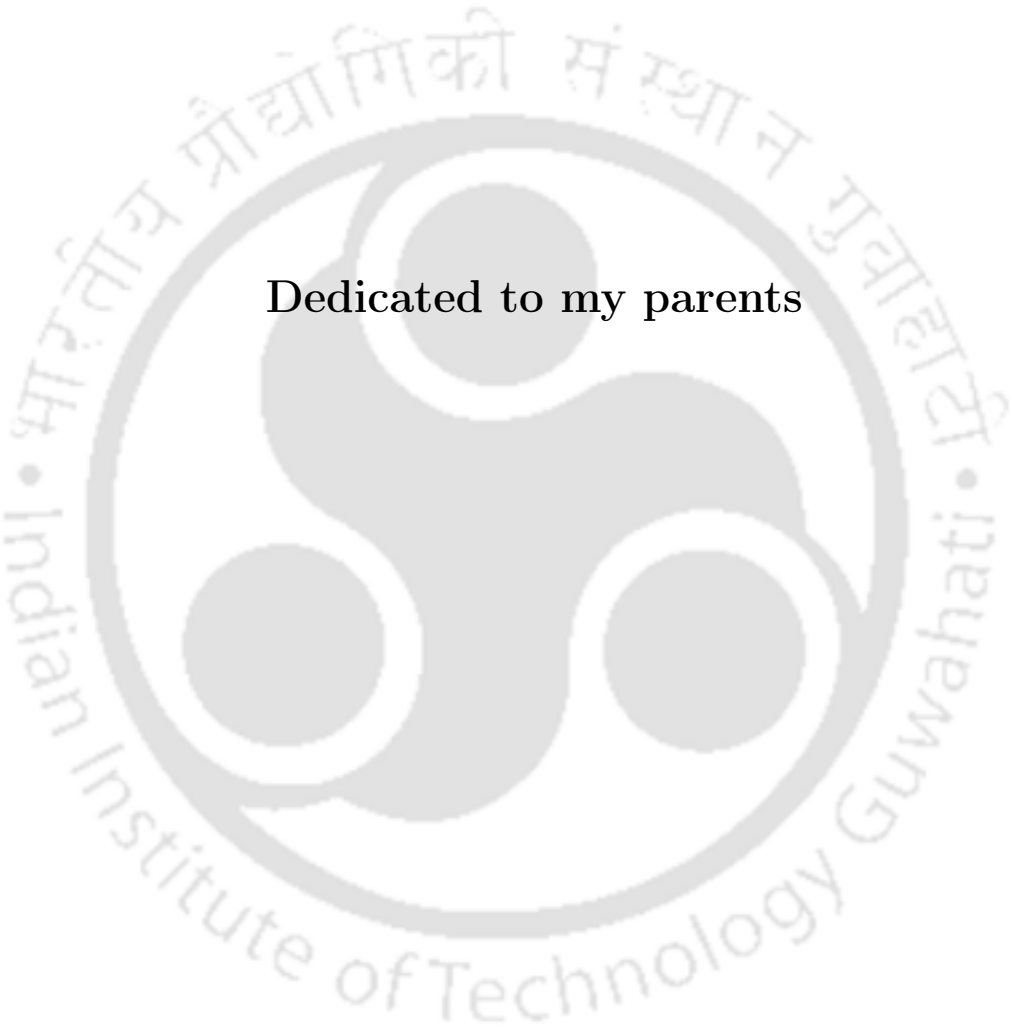
January, 2010

CERTIFICATE

It is certified that the work contained in the thesis entitled "**Iwasawa Invariants of Elliptic Curves and p-adic Measures**" by **Rupam Barman** (Roll Number: 06612301) has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

Dr. Anupam Saikia
Assistant Professor
Department of Mathematics
IIT Guwahati

April, 2010



Dedicated to my parents

Acknowledgements

I am very grateful to my supervisor Dr. Anupam Saikia for his guidance and many stimulating discussions throughout my PhD years. This work would not have been possible without his help.

I would like to thank Prof. R. Sujatha for her continuous support throughout my PhD years. I am very grateful to her for giving me an opportunity to visit Tata Institute of Fundamental Research Mumbai during July-August 2008 for a period of two months and suggesting the problem of Chapter 4. I also gratefully acknowledge the financial support and hospitality of the same institute during that period.

I am also indebted to Dr. Aribam Chandrakant Sharma for his support and for many fruitful discussions during my stay at TIFR.

I would like to thank Prof. William Stein for writing a SAGE code for me. I am also very much thankful to Prof. John H. Coates, Prof. Barry Mazur, Dr. Christian Wuthrich, Dr. John Cremona and Dr. Robert Pollack for their valuable suggestions during my PhD years.

I am indeed grateful to Tezpur University for giving me study leave for a period of one year to carry my PhD work at IIT Guwahati. I thank all my colleagues of the Department of Mathematical Sciences for their encouragement. My special thanks to Prof. Nayandeep Deka Baruah for his continuous support during my PhD years.

I gratefully acknowledge the financial support received from National Board for Higher Mathematics for a period of three years under teacher fellowship.

Finally, I thank my parents, my wife and my daughter TORA for their support.

April, 2010 **Rupam Barman**

Abstract

The central theme of our work is to investigate Iwasawa invariants associated with elliptic curves and p-adic measures. Iwasawa μ- and λ-invariants of an elliptic curve contain valuable information about the curve. On the other hand, p-adic L-functions over $\mathbb{Q}$ arise as Γ-transforms of certain p-adic measures, hence there is considerable interest in Iwasawa invariants of such measures and their Γ-transforms.

Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$. Let p be an odd prime where E_1 and E_2 have good ordinary reduction. Assume that $E_1[p^i] \cong E_2[p^i]$ as Galois modules for $i = \mu(E_1)+1$. Also assume that both $E_1(\mathbb{Q})[p]$ and $E_2(\mathbb{Q})[p]$ are trivial. Under the above assumptions we prove that $\mu(E_1) = \mu(E_2)$. Also, if $E_1[p^i] \cong E_2[p^i]$ as Galois modules for $i = \mu(E_1)$, then $\mu(E_1) \leq \mu(E_2)$. This result is an extension of earlier works of Greenberg and Vatsal, who studied this problem for elliptic curves with μ-invariants zero. We also illustrate our results through some numerical examples.

We find a generalization of an existing result of Satoh, Kida and Childress that deals with p-adic measures on $\mathbb{Z}_p$ to p-adic measures on $\mathbb{Z}_p^n$ for any n. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$, where p is a fixed odd prime. If α is a $\mathcal{O}$-valued measure on $\mathbb{Z}_p^n$, then it gives a power series in n variables with coefficients in $\mathcal{O}$. Analogous to the case $n = 1$, we define Iwasawa invariants of such a power series for any n. Given a $\mathcal{O}$-valued measure α on $\mathbb{Z}_p^n$, one obtains a new measure $\beta = \sum_{\eta_1 \in V} \cdots \sum_{\eta_n \in V} (\alpha \circ (\eta_1, \cdots, \eta_n))|_{U^n}$ on U^n while defining the Γ-transform of α. Extending by 0, β gives a measure on $\mathbb{Z}_p^n$. We obtain a relation between the Iwasawa invariants of the power series associated to β and the Γ-transform for any $n \geq 1$. We prove the relation by deriving certain p-adic properties of Mahler coefficients of the continuous functions $f_m(x) = \binom{u^x}{m}$ and $f_{m_1,\cdots,m_n}(x_1, \cdots, x_n) = \binom{u^{x_1}}{m_1} \cdots \binom{u^{x_n}}{m_n}$, where u is a topological generator of $1 + p\mathbb{Z}_p$.

In case of $n = 1$, Childress showed how the coefficients of the power series associated to a p-adic measure α on $\mathbb{Z}_p$ are related to the coefficients of the measure β. She proved congruences modulo p amongst these coefficients. Finally, using these congruences she related the coefficients of α to the λ-invariant of the Iwasawa series of the Γ-transform of α. Following her approach, one can generalize the congruences modulo p amongst the coefficients of a p-adic measure α on $\mathbb{Z}_p^n$ and the coefficients of the associated measure β. We relate the coefficients of a p-adic measure α on $\mathbb{Z}_p^2$ to the λ-invariant of the Iwasawa series of the Γ-transform of α. One can produce similar results for any α defined on $\mathbb{Z}_p^n$, but the number of coefficients of the power series associated with α which are involved increases with n.

Contents

Chapter 1

Introduction

The striking feature of Iwasawa theory is that deep information about the arithmetic of a finite extension F of $\mathbb{Q}$ can be obtained by studying the arithmetic of certain infinite Galois tower of number fields lying above F. The typical example is the classical theory of cyclotomic fields. Let μ_m denote the group of m-th roots of unity. Let p be a prime number and define

$$P = \mathbb{Q}(\mu_p), \qquad P_n = \mathbb{Q}(\mu_{p^{n+1}}), \qquad P_\infty = \bigcup_{n \geq 0} P_n = \mathbb{Q}(\mu_{p^\infty}).$$

Number theorists have studied the field P since the time of Kummer, but it was Iwasawa who realized the importance of the infinite tower above P. This infinite tower of fields is referred to as the cyclotomic tower. Many aspects of Iwasawa's theory are not special to the cyclotomic tower. They have already been successfully applied in the arithmetic theory of elliptic curves with complex multiplication. One significant result in this direction is the proof of a version of the Birch and Swinnerton-Dyer by Coates and Wiles in [6]. They worked with the tower of fields generated by the torsion points of an elliptic curve. More generally, one can apply these ideas to certain infinite tower of fields which are

known as $\mathbb{Z}_p$-extensions (see section 1.1.1).

Iwasawa theory occupies a unique place in the study of elliptic curves (see [17–20]). One of the most important questions about the arithmetic of an elliptic curve defined over a number field is the rank of the Mordell-Weil group. Suppose E is an elliptic curve defined over the number field F. The rational points on E over F form an abelian group known as the Mordell-Weil group and is denoted by $E(F)$. The Mordell-Weil group is finitely generated as a $\mathbb{Z}$-module. It is possible to describe quite precisely the torsion subgroup. In fact, if E is defined over $\mathbb{Q}$, then its torsion part is completely known due to a theorem of Mazur. However, it is far more difficult to determine its free part. By studying the Selmer groups, valuable information about the Mordell-Weil group can be gained. In particular, an upper bound for the Mordell-Weil rank can be obtained. By investigating elements of the Selmer groups, one can hope to find the generators of the free part of the Mordell-Weil group. This procedure is known as the method of descent. The Selmer groups are defined in terms of Galois cohomology (for details, see chapter 2). Let p be a prime number. The underlying idea of Iwasawa theory is to study first the arithmetic of E over a certain infinite Galois extension F_∞ of F, and then to exploit the natural action of the Galois group of F_∞ over F on the basic arithmetic objects to derive information about E over the original base field F. Suppose that p is a prime where E has good ordinary reduction. If K is an algebraic extension of $\mathbb{Q}$, then the Selmer group for E over K is a certain subgroup of $H^1(G_K, E(\overline{\mathbb{Q}})_{\text{tors}})$, where $G_K = \text{Gal}(\overline{\mathbb{Q}}/K)$. The Selmer group $\text{Sel}_E(K)$ fits into an exact sequence

$$0 \to E(K) \otimes \mathbb{Q}/\mathbb{Z} \to \text{Sel}_E(K) \to Ш_E(K) \to 0,$$

where $Ш_E(K)$ denotes the Shafarevich-Tate group for E over K (see [11, 19]).

Let $K = \mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Then $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ acts on $\mathrm{Sel}_E(\mathbb{Q}_\infty)$. Its p-primary subgroup $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ can be regarded as a Λ-module, where $\Lambda = \mathbb{Z}_p[[T]]$ is the completed group algebra for Γ over $\mathbb{Z}_p$. Kato has proven that $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ is Λ-cotorsion, as Mazur conjectured in [5]. That is, the Pontryagin dual $X_E(\mathbb{Q}_\infty)$ of $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ is a torsion Λ-module. It is also known that $X_E(\mathbb{Q}_\infty)$ is finitely generated Λ-module. The classification of finitely generated Λ-modules (see section 1.1.3) asserts that one has a pseudo-isomorphism

$$X_E(\mathbb{Q}_\infty) \sim \Big(\bigoplus_{i=1}^{n} \Lambda/(f_i(T))^{a_i}\Big) \bigoplus \Big(\bigoplus_{j=1}^{m} \Lambda/(p^{\mu_j})\Big). \tag{1.1}$$

The $f_i(T)$'s are irreducible distinguished polynomials in Λ. The a_i's and μ_j's are positive integers. One can then define the algebraic Iwasawa invariants of $E/\mathbb{Q}$ at the prime p by

$$\mu(E) = \sum_{j=1}^{m} \mu_j \quad \text{and} \quad \lambda(E) = \sum_{i=1}^{n} a_i \deg(f_i(T)).$$

Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$. Let p be an odd prime where E_1 and E_2 have good ordinary reduction. In [21], Greenberg and Vatsal studied vanishing of the μ-invariants of both the curves in terms of the Galois module structure of the p-torsion points on the curves. In this thesis, we extend their results for curves with non-zero μ-invariants. We illustrate our results through some numerical examples.

In [24], Sinnott gave an elegant new proof of the theorem of Ferrero and Washington that the Iwasawa μ-invariant is zero for the cyclotomic $\mathbb{Z}_p$-extension of any abelian number field. Sinnott showed how to compute the μ-invariant of the Γ-transform of a rational function. Since the p-adic L-functions over $\mathbb{Q}$ arise as such Γ-transforms, he obtained a new proof of the theorem of Ferrero and

Washington (see [4]). Following his approach, Rosenberg also found a new proof of the same theorem. In addition, he gave an upper bound on the corresponding λ-invariant (see [23]). For a more complete discussion on p-adic measure theory, p-adic L-function, and the relation between Iwasawa's μ-invariant and p-adic L-functions, see [12, 22].

Let us fix an odd prime p. We write $\mathbb{Z}_p^\times = V \times U$ where V is the group of $(p-1)$st roots of unity in $\mathbb{Z}_p$ and $U = 1 + p\mathbb{Z}_p$. Let u be a topological generator of U. The projections from $\mathbb{Z}_p^\times$ onto V and U are denoted by ω and $<>$ respectively. We have an isomorphism $\phi : \mathbb{Z}_p \to U$ given by $\phi(y) = u^y$. Let $\mathcal{O}$ be the ring of integers of some finite extension K of $\mathbb{Q}_p$ with a local parameter π. Let Λ denote the $\mathcal{O}$-valued measures on $\mathbb{Z}_p$. It is well-known, (see e.g. [14, 24]), that Λ is a ring under convolution, and is isomorphic to the formal power series ring $\mathcal{O}[[T-1]]$. Thus, for given $\alpha \in \Lambda$, we get a power series $\widehat{\alpha}(T) \in \mathcal{O}[[T-1]]$. For a power series $f(T) \in \mathcal{O}[[T-1]]$, we can define the Iwasawa μ-invariant of f, denoted by $\mu(f)$, as the largest non-negative integer n such that π^n divides all the coefficients of f. If $f(T) = a_0 + a_1 T + a_2 T^2 + \cdots$, then Iwasawa λ-invariant of f, denoted by $\lambda(f)$, is defined as the smallest non-negative integer m such that $\pi^{-\mu(f)} a_m$ is a unit in $\mathcal{O}$. The Γ-transform of a measure α is defined as a function of the p-adic variable s given by

$$\Gamma_\alpha(s) = \int_{\mathbb{Z}_p^\times} < x >^s \, d\alpha(x).$$

Given a $\mathcal{O}$-valued measure α on $\mathbb{Z}_p$, one obtains a new measure $\beta = \sum_{\eta \in V} (\alpha \circ \eta)|_U$ on U while defining the Γ-transform of α. Extending by 0, β gives a measure on $\mathbb{Z}_p$. It was Kida who first obtained a relation between the Iwasawa invariants of the power series associated to β and the Γ-transform of α with a fixed topological generator of U (see [25]). Later, Nancy Childress in her paper [14]

proved that relation for any topological generator of U, but under the conditions that $\lambda(G(T)) \leq p$. She remarked that it would be interesting to know whether her methods can be extended for larger $\lambda(G(T))$. Satoh obtained the same result without any condition on $\lambda(G(T))$, but his approach was based on certain properties of Stirling numbers (see [10]). In this thesis, we obtain a relation between the λ-invariant of a p-adic measure and its Γ-transform with an arbitrary topological generator exploiting certain combinatorial identities. Through our approach we also derive certain p-adic properties of Mahler coefficients of the continuous functions $f_m(x) = \binom{u^x}{m}$ and $f_{m_1,\cdots,m_n}(x_1,\cdots,x_n) = \binom{u^{x_1}}{m_1}\cdots\binom{u^{x_n}}{m_n}$. Let $n \geq 1$. It is well known that $\mathcal{O}$-valued measures on $\mathbb{Z}_p^n$ is isomorphic to the formal power series ring $\mathcal{O}[[T_1-1,\cdots,T_n-1]]$. Then one can define Γ-transform of a measure on $\mathbb{Z}_p^n$. Using our method, we obtain a new relation between the λ-invariant of a measure on $\mathbb{Z}_p^n$ and its Γ-transform with an arbitrary topological generator of U for any $n \geq 1$. Finally, we relate the coefficients of a measure α on $\mathbb{Z}_p^2$ to the λ-invariant of the Iwasawa series of the Γ-transform of α. One can produce similar results for any measure α on $\mathbb{Z}_p^n$, but the number of coefficients of $\widehat{\alpha}(T_1-1,\cdots,T_n-1)$ which are involved increases with n.

1.1 Basic Background: Iwasawa Theory

1.1.1 $\mathbb{Z}_p$-extensions

For any finite field extension $F/\mathbb{Q}$, there exists an integer $n \geq 0$ such that multiplicative group μ_{p^n} of the p^n-th roots of 1 is contained in F but $\mu_{p^{n+1}} \nsubseteq F$. Hence $\mathrm{Gal}(F(\mu_{p^\infty})/F)$ is isomorphic to a subgroup of $\mathbb{Z}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ of finite index. The *cyclotomic $\mathbb{Z}_p$-extension* of F is the unique subfield F_∞ of

$F(\mu_{p^\infty})$ with $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$.

In general, a field F_∞ is called a $\mathbb{Z}_p$-*extension* of F if F_∞ is a Galois extension of F whose Galois group is a topological group isomorphic to the additive group of $\mathbb{Z}_p$. That is, F_∞ is the union of a tower of number fields:

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n \subset \cdots \subset F_\infty = \bigcup_{n \geq 0} F_n \tag{1.2}$$

such that $\mathrm{Gal}(F_{n+1}/F_n) \cong \mathbb{Z}/p\mathbb{Z}$ and $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$. An important property of any $\mathbb{Z}_p$-extension of a number field F is that if v is a prime of F not dividing p, then v is unramified in F_∞/F.

1.1.2 The Iwasawa Algebra and Its Modules

Let F_∞/F be a $\mathbb{Z}_p$-extension of a number field F. We denote the Galois group of F_∞ over F by Γ and the subgroup of Γ which fixes F_n by Γ_n. Here, Γ is isomorphic to $\mathbb{Z}_p$ and Γ/Γ_n is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. Let $\mathbb{Z}_p[\Gamma/\Gamma_n]$ be the group ring of the cyclic group Γ/Γ_n with coefficients in $\mathbb{Z}_p$. For $m \geq n$, there is a natural surjective map from $\mathbb{Z}_p[\Gamma/\Gamma_m]$ to $\mathbb{Z}_p[\Gamma/\Gamma_n]$. The *Iwasawa Algebra* of Γ is defined as

$$\Lambda = \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma_n] \tag{1.3}$$

where the inverse limit is with respect to these canonical maps. The Iwasawa algebra is particularly useful as it has both an algebraic and an analytic interpretation. Analytically, elements of Λ can be interpreted as $\mathbb{Z}_p$-valued measures on Γ. The algebraic interpretation is that one can naturally extend the continuous action of Γ on any compact $\mathbb{Z}_p$-module X to an action of the whole Iwasawa algebra Λ. The important arithmetic objects like the class groups of global fields or the local units naturally form an inverse system and the inverse

limits have the natural structure of a compact Λ-module. Serre pointed out that Λ is topologically isomorphic as a ring to $\mathbb{Z}_p[[T]]$, the ring of formal power series in an indeterminate T with coefficients in $\mathbb{Z}_p$. This isomorphism is given by

$$\gamma \mapsto 1 + T,$$

where γ is a topological generator of $\mathrm{Gal}(F_\infty/F) = \Gamma$ (that is, an element of Γ such that $\gamma|F_1$ is not trivial). Note that this isomorphism depends on the choice of γ and hence non-canonical.

1.1.3 Structure of Λ-Modules

The rich structure theory for such $\mathbb{Z}_p[[T]]$-modules can be exploited to study certain important compact Λ-modules. This leads us to a deeper understanding of the arithmetic. $\mathbb{Z}_p[[T]]$ is a Noetherian local ring with unique maximal ideal $\mathfrak{m} = (p, T)$ of index p. Under the $\mathfrak{m}$-adic topology, $\mathbb{Z}_p[[T]]$ is a compact topological ring. Even though $\mathbb{Z}_p[[T]]$ is not a principal ideal domains, modules over $\mathbb{Z}_p[[T]]$ behave in a very similar way to modules over a PID. The following theorem tells us that we have an analgoue of division algorithm in $\Lambda = \mathbb{Z}_p[[T]]$.

Theorem 1.1.1. ([19]) *Suppose that $g(T) \in \Lambda$, but $g(T) \notin p\Lambda$. If $g(T) = \sum_{i=0}^{\infty} b_i T^i$, let d be the smallest integer such that $b_d \in \mathbb{Z}_p^\times$. Let $f(T)$ be any element of Λ. Then there exists a polynomial $r(T) \in \mathbb{Z}_p[T]$ of degree less than d, and an element $h(T) \in \Lambda$ such that*

$$f(T) = g(T)h(T) + r(T).$$

Furthermore, $h(T)$ and $r(T)$ are uniquely determined by $f(T)$ and $g(T)$.

From the above theorem, we easily get the following corollary.

Corollary 1.1.1. *Let $g(T)$ be as in the above theorem. Then $\Lambda/(g(T))$ is isomorphic to $\mathbb{Z}_p^d$ as a $\mathbb{Z}_p$-module.*

Definition 1.1.1. *A polynomial $\sum_{i=0}^{d} c_i T^i \in \mathbb{Z}_p[T]$ is called a* ***distinguished polynomial*** *if $c_d = 1$ and $c_i \in p\mathbb{Z}_p$ for every $i < d$.*

Theorem 1.1.2. *(**p-adic Weierstrass Preparation Theorem**,* [12, 19]*) Let $g(T)$ be a nonzero element of Λ. Then we can write $g(T)$ uniquely in the form*

$$g(T) = p^m u(T) g_0(T)$$

where $m \geq 0, u(T) \in \Lambda^\times$, and $g_0(T)$ is a distinguished polynomial. Also, $g(T)$ is an irreducible element of Λ if and only if either $m = 1$ and $g_0(T) = 1$ or $m = 0$ and $g_0(T)$ is irreducible as an element of $\mathbb{Z}_p[T]$.

Remark 1.1.1. *From Theorem 1.1.2 it is easy to see that up to multiplication by elements of $\Lambda^\times$, the irreducible elements of Λ are either p or any distinguished polynomial in $\mathbb{Z}_p[T]$ which is irreducible over $\mathbb{Z}_p$.*

Remark 1.1.2. *It follows easily from Theorem 1.1.2 that any non-zero element in $\mathbb{Z}_p[[T]]$ can have only finitely many zeroes.*

The following definition is crucial in the study of Λ-modules.

Definition 1.1.2. *Let R be a ring and M, N be R-modules. An R-module homomorphism $\phi : M \to N$ is called pseudo isomorphism if $ker(\phi)$ and $coker(\phi)$ are finite. If M and N are pseudo isomorphic, then it is denoted by $M \sim N$.*

The following theorem classifies finitely generated Λ-modules up to pseudo isomorphism. Proof of this theorem can be found in [12, 19].

Theorem 1.1.3. *(**Structure Theorem of finitely generated** Λ**-modules**) If X is a finitely generated Λ-module, then there exists a Λ-module pseudo isomorphism*

$$X \sim \Lambda^r \bigoplus \Big(\bigoplus_{i=1}^{s} \Lambda/(f_i(T))^{e_i}\Lambda \Big) \bigoplus \Big(\bigoplus_{j=1}^{t} \Lambda/p^{m_j}\Lambda \Big),$$

where all integers $r, e_i, m_j \geq 0$, and all $f_i(T)$ are irreducible distinguished polynomials in $\mathbb{Z}_p[T]$.

Remark 1.1.3. *If X is a finitely generated torsion Λ-module, then in the above theorem we have $r = 0$.*

Definition 1.1.3. *Let X be a finitely generated torsion Λ-module. Then from Theorem 1.1.3, we have*

$$X \sim \Big(\bigoplus_{i=1}^{s} \Lambda/(f_i(T))^{e_i}\Lambda \Big) \bigoplus \Big(\bigoplus_{j=1}^{t} \Lambda/p^{m_j}\Lambda \Big).$$

The characteristic polynomial for X is defined as

$$f_X(T) = \prod_{j=1}^{t} p^{m_j} \prod_{i=1}^{s} f_i(T)^{e_i}. \tag{1.4}$$

1.1.4 Iwasawa Invariants

Let $\mathcal{O}$ be the ring of integers in a finite extension of $\mathbb{Q}_p$ with a local parameter π. For any non-zero $x = \pi^n u$ with $u \in \mathcal{O}^\times$, we have $\mathrm{ord}(x) = n$.

Definition 1.1.4. *The Iwasawa μ- and λ- invariants of a power series*

$$F(T) = \sum_{n=0}^{\infty} a_n T^n \in \mathcal{O}[[T]]$$

are defined by

$$\mu(F(T)) = min\{ord(a_n) : n \geq 0\}$$

$$\lambda(F(T)) = min\{n : ord(a_n) = \mu(F(T))\}.$$

Remark 1.1.4. *Let $f(T) = \sum_{i=0}^{\infty} c_i T^i$ be a non zero element of Λ. Then $f(T) \in \Lambda^\times$ if and only if $\mu(f) = \lambda(f) = 0$.*

Definition 1.1.5. *Let X be a finitely generated torsion Λ-module. Let $f_X(T)$ be the characteristic polynomial of X. Then the Iwasawa μ and λ-invariants of X are defined as*

$$\mu(X) = \mu(f_X(T)) \quad \text{and} \quad \lambda(X) = \lambda(f_X(T)).$$

Remark 1.1.5. *The Iwasawa invariants of the characteristic polynomial f_X given in* (1.4) *are:*

$$\mu(f_X) = \sum_{j=1}^{t} m_j \qquad \text{and} \qquad \lambda(f_X) = \sum_{i=1}^{s} e_i deg(f_i(T)).$$

By definition, there are also called the Iwasawa invariants of the finitely generated torsion Λ-module X.

We now give an equivalent description of the Iwasawa invariants. Suppose that X is a finitely generated, torsion Λ-module, where $\Lambda = \mathbb{Z}_p[[T]]$. If I is any ideal of Λ, we use the following notation

$$X[I] = \{x \in X : \alpha x = 0 \text{ for all } \alpha \in I\}.$$

Let $\mathfrak{m} = (p, T)$ be the maximal ideal of Λ and let $Z = \bigcup_{n \geq 0} X[\mathfrak{m}^n]$. Since Λ is Noetherian and X is finitely generated Λ-module, so X is also Noetherian. Hence, it follows that $Z = X[\mathfrak{m}^t]$ for some $t > 0$ and that Z is finite. It is clear that any finite Λ-submodule of X is contained in Z and so we refer to Z as the maximal, finite Λ-submodule of X.

Let $Y = \bigcup_{n \geq 0} X[p^n]$, which is just the $\mathbb{Z}_p$-torsion submodule of X. Just as above, we see that $Y = X[p^t]$ for some $t > 0$. We have $Z \subseteq Y$ and the

quotient X/Y is a finitely generated, torsion Λ-module and is torsion free as a $\mathbb{Z}_p$-module. We summarize the above observations in the following proposition (see [17, 19]).

Proposition 1.1.1. *Suppose that X is a finitely generated, torsion Λ-module. Then there are uniquely determined Λ-submodules Z and Y of X with the following properties:*

1. *Z is finite and X/Z has no nonzero, finite Λ-submodules.*
2. *Y is annihilated by a power of p and X/Y is a free $\mathbb{Z}_p$-module of finite rank.*

Now we give equivalent definitions of Iwasawa invariants associated with X (see [17, 19]). The $\mathbb{Z}_p$-rank of X/Y is equal to $\dim_{\mathbb{Q}_p}(V)$, where V is the $\mathbb{Q}_p$-vector space $X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Definition 1.1.6. *The λ-invariant of X is defined as*

$$\lambda(X) = rank_{\mathbb{Z}_p}(X/Y) = dim_{\mathbb{Q}_p}(V).$$

We have $Y = X[p^t]$ for some $t > 0$. For each i such that $0 < i \leq t$, the Λ-module $X[p^i]/X[p^{i-1}]$ has exponent p and can be considered as an $\mathbb{F}_p[[T]]$-module. It is finitely generated and thus has finite rank.

Definition 1.1.7. *The μ-invariant of X is defined as*

$$\mu(X) = \sum_{i=1}^{t} rank_{\mathbb{F}_p[[T]]}(X[p^i]/X[p^{i-1}]).$$

Remark 1.1.6. *Let $r_i = rank_{\mathbb{F}_p[[T]]}(X[p^i]/X[p^{i-1}])$. Then $r_1 \geq \cdots \geq r_n \geq \cdots$.*

Lemma 1.1.1. *If X is finitely generated as a $\mathbb{Z}_p$-module, then $\mu(X) = 0$. To be precise, we have*

$$\mu(X) = 0 \Leftrightarrow Y \text{ is finite} \Leftrightarrow X[p] \text{ is finite} \Leftrightarrow X/pX \text{ is finite.}$$

We shall now give a proof of the equivalence of the above definitions of Iwasawa invariants in the following theorem. Note that for a module M which is finitely generated over $\mathbb{F}_p[[T]]$, the μ-invariant as a $\mathbb{Z}_p[[T]]$-module is the same as the $\mathbb{F}_p[[T]]$-rank. Indeed, if M is annihilated by p, then in the structure theorem (see Theorem 1.1.3) the only factors that can appear are copies of $\mathbb{Z}_p[[T]]/p\mathbb{Z}_p[[T]]$. The number of these copies is, by definition, the μ-invariant of M, which is also the $\mathbb{F}_p[[T]]$-rank. We use this important fact in the proof of the following theorem.

Theorem 1.1.4. *The Definition 1.1.5 and Definition 1.1.7 of μ-invariant of X are equivalent. Also, Definition 1.1.5 and Definition 1.1.6 of λ-invariant of X are equivalent.*

Proof. Let X be a finitely generated torsion $\Lambda = \mathbb{Z}_p[[T]]$-module. Let $Y = \bigcup_{n\geq 0} X[p^n]$, which is just the $\mathbb{Z}_p$-torsion submodule of X. We know that $Y = X[p^t]$ for some $t > 0$. From the structure theorem, it is clear that $\mu(X) = \mu(Y)$. We also have the following:

$$X[p] \subset X[p^2] \subset \cdots \subset X[p^{t-1}] \subset X[p^t].$$

Since μ-invariant is additive along the exact sequence

$$0 \longrightarrow X[p^r] \longrightarrow X[p^{r+1}] \longrightarrow X[p^{r+1}]/X[p^r] \longrightarrow 0$$

for any r, we have

$$\mu(X[p^{r+1}]/X[p^r]) = \mu(X[p^{r+1}]) - \mu(X[p^r]).$$

Now,

$$\begin{aligned}\mu(X) &= \mu(X[p^t]) \\ &= \mu(X[p^t]) - \mu(X[p^{t-1}]) + \mu(X[p^{t-1}]) - \mu(X[p^{t-2}]) + \mu(X[p^{t-2}]) - \cdots \\ &= \mu(X[p^t]/X[p^{t-1}]) + \mu(X[p^{t-1}]/X[p^{t-2}]) + \cdots + \mu(X[p]) \\ &= \sum_{i=1}^{t} \text{rank}_{\mathbb{F}_p[[T]]}(X[p^i]/X[p^{i-1}]).\end{aligned}$$

This proves the equivalence of the two definitions of μ-invariant.

Again, suppose that $f_X(T) = \prod_{j=1}^{t} p^{m_j} \prod_{i=1}^{s} f_i(T)^{e_i}$ is the characteristic polynomial of X. For every i, $f_i(T)^{e_i}$ is a distinguished polynomial. From Corollary 1.1.1, we have that $\Lambda/(f_i(T)^{e_i})$ is isomorphic to $\mathbb{Z}_p^{\deg(f_i(T)^{e_i})}$ as a $\mathbb{Z}_p$-module. This implies that

$$\text{rank}_{\mathbb{Z}_p}(X/Y) = \sum_{i=1}^{s} e_i \deg(f_i(T)) = \lambda(f_X(T)).$$

This proves that the Definition 1.1.5 and Definition 1.1.6 of λ-invariant of X are equivalent. This completes the proof of the theorem. □

Remark 1.1.7. *We shall prove an $\mathbb{F}_p[[T]]$-corank version of Definition 1.1.7 in the next chapter for Selmer group (see Theorem 2.3.2).*

Selmer groups are used to study the ranks of elliptic curves. In this thesis, we use the p-primary part of the Selmer group. Let K be any algebraic extension of $\mathbb{Q}$. Suppose that E is an elliptic curve defined over K. One of the principal ways in which one studies the Mordell-Weil group $E(K)$ is by using Galois cohomology (see [7, 9]). Fix $n \geq 2$. Then there is a natural injective homomorphism of $E(K)/nE(K)$ into $H^1(G_K, E[n])$ which is called the Kummer map. Here G_K is the absolute Galois group of K. If K is a finite extension of $\mathbb{Q}$, then $H^1(G_K, E[n])$ turns out to be an infinite group. But one can show that

the image of $E(K)/nE(K)$ under the Kummer map is contained in a certain finite subgroup of $H^1(G_K, E[n])$, called the n-Selmer group. In that way, one proves the weak Mordell-Weil theorem which asserts that $E(K)/nE(K)$ is finite if K is a number field.

Let L be a field of characteristic zero. Classical Kummer theory gives an isomorphism

$$L^\times/(L^\times)^n \to H^1(G_L, \mu_n)$$

for any $n \geq 1$, where μ_n denotes the group of n-th roots of unity in $\overline{L}$. Taking the direct limit, one obtains an isomorphism

$$\kappa : L^\times \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to H^1(G_L, (\overline{L}^\times)_{\text{tors}}).$$

Imitating Kummer theory for the multiplicative group $K^\times$, one can define the Kummer homomorphism

$$E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to H^1(G_K, E(\overline{K})_{\text{tors}})$$

as follows: Let $\alpha = P \otimes r \in E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$, where $P \in E(K)$ and $r = \frac{m}{n} + \mathbb{Z}$. Choose $Q \in E(\overline{K})$ such that $nQ = mP$. Define a 1-cocycle $\phi_\alpha : G_K \to E(\overline{K})_{\text{tors}}$ by $\phi_\alpha(g) = g(Q) - Q$ for all $g \in G_K$. Then $[\phi_\alpha]$ is well defined and one defines $\kappa(\alpha) = [\phi_\alpha]$. The following sequence (known as Kummer sequence) is exact:

$$0 \longrightarrow E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \xrightarrow{\kappa} H^1(G_K, E(\overline{K})_{\text{tors}}) \xrightarrow{\lambda} H^1(G_K, E(\overline{K})) \longrightarrow 0$$

We use the Kummer sequence for the completions K_v where v is any prime of K. In the following commutative diagram, the vertical maps are defined in obvious ways and the rows are exact.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)\otimes(\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\kappa} & H^1(G_K, E(\overline{K})_{\text{tors}}) & \xrightarrow{\lambda} & H^1(G_K, E(\overline{K})) & \longrightarrow & 0 \\
 & & \downarrow a_v & & \downarrow b_v & & \downarrow c_v & & \\
0 & \longrightarrow & E(K_v)\otimes(\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\kappa_v} & H^1(G_{K_v}, E(\overline{K_v})_{\text{tors}}) & \xrightarrow{\lambda_v} & H^1(G_{K_v}, E(\overline{K_v})) & \longrightarrow & 0
\end{array}$$

Definition 1.1.8. *The Selmer group $Sel_E(K)$ is defined as follows:*

$$Sel_E(K) = ker\Big(H^1(G_K, E(\overline{K})_{tors}) \to \prod_v (H^1(G_{K_v}, E(\overline{K_v})_{tors})/im(\kappa_v))\Big),$$

where v runs over all primes of K, archimedean and nonarchimedean.

Remark 1.1.8. *If K is a finite extension of $\mathbb{Q}$, then K_v is the completion of K at v. If K is an infinite algebraic extension of $\mathbb{Q}$, then K_v denotes the union of the completions at v of all finite extensions of $\mathbb{Q}$ contained in K. Thus K_v is always either $\mathbb{R}$ or $\mathbb{C}$ or an algebraic extension of $\mathbb{Q}_l$ for some rational prime l.*

Theorem 1.1.5. *(*Kato-Rohrlich*) If E is an elliptic curve defined over $\mathbb{Q}$ with good ordinary or multiplicative reduction at a prime p, and if F_∞ is the cyclotomic $\mathbb{Z}_p$-extension of an abelian extension $F/\mathbb{Q}$, then $Sel_E(F_\infty)_p$ is a cofinitely generated Λ-cotorsion module.*

That is, its dual X is a finitely generated torsion Λ-module and hence of the form:

$$X \sim \prod_{i=1}^{s} \Lambda/(f_i(T))^{e_i} \times \prod_{j=1}^{t} \Lambda/p^{m_j}.$$

The Iwasawa invariants of X are called the Iwasawa invariants of the elliptic curve E defined over F at the prime p.

1.2 Basic Background: p-adic Measures

The metric space $\mathbb{Z}_p$ has a basis of open sets consisting all sets of the form

$$a + p^n\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x - a|_p \leq \frac{1}{p^n}\}$$

for $a \in \mathbb{Z}_p$ and $n \in \mathbb{N}$. These sets are known as intervals. It is well known that $\mathbb{Z}_p$ is compact.

Definition 1.2.1. *A p-adic distribution μ on $\mathbb{Z}_p$ is a $\mathbb{Q}_p$-linear vector space homomorphism from the $\mathbb{Q}_p$-vector space of locally constant functions on $\mathbb{Z}_p$ to $\mathbb{Q}_p$. If $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is locally constant, instead of writing $\mu(f)$ for the value of μ at f, one usually writes $\int f\mu$.*

Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$. In $\mathbb{Z}_p$, any two open balls are either disjoint or one is contained in the other. Since $\mathbb{Z}_p$ is compact, therefore f is locally constant if and only if it is a finite linear combination with coefficients in $\mathbb{Q}_p$ of characteristic functions of compact open sets in $\mathbb{Z}_p$. Hence, we have the following equivalent definition of p-adic distribution. For details see [15].

Definition 1.2.2. *A p-adic distribution μ on $\mathbb{Z}_p$ is an additive map from the set of compact-opens in $\mathbb{Z}_p$ to $\mathbb{Q}_p$.*

Definition 1.2.3. *A p-adic distribution μ on $\mathbb{Z}_p$ is a measure if its values on compact open sets U are bounded by some constant $M \in \mathbb{R}$. That is, $|\mu(U)|_p \leq M$ for all compact open set U.*

Let U be open and compact subset of $\mathbb{Z}_p$. Define $H_U = \{\gamma \in \mathbb{Z}_p : \gamma + U = U\}$. Then H_U is a compact open subgroup of $\mathbb{Z}_p$. Hence $\mathbb{Z}_p$ is a union of disjoint cosets of H. Let $\mathbb{Z}_p = \cup_{i=1}^{n}(\sigma_i + H_U)$.

Definition 1.2.4. *Let μ and λ be two measures on $\mathbb{Z}_p$. Let U be any compact open subset of $\mathbb{Z}_p$. The convolution $\mu \circ \lambda$ of μ and λ is defined as*

$$(\mu \circ \lambda)(U) = \sum_{i=1}^{n} \lambda(U - \sigma_i)\mu(\sigma_i + H_U).$$

1.3 Organization

There are six chapters in this thesis. The Chapter 1 is introductory in nature which contains basic background on elliptic curves and p-adic measures.

Chapter 2 is devoted to the study of Iwasawa μ-invariants of elliptic curves. We obtain a result which is an extension of earlier work by Greenberg and Vatsal [21]. We illustrate our result through some numerical examples.

Chapter 3 deals with Mahler coefficients of certain continuous functions. More specifically, let u be a topological generator of $1+p\mathbb{Z}_p$. Then we consider the continuous functions $f_m : \mathbb{Z}_p \to \mathbb{Z}_p$ and $f_{m_1,\cdots,m_n} : \mathbb{Z}_p^n \to \mathbb{Z}_p$ defined by $f_m(x) = \binom{u^x}{m}$ and $f_{m_1,\cdots,m_n}(x_1,\cdots,x_n) = \binom{u^{x_1}}{m_1}\cdots\binom{u^{x_n}}{m_n}$, respectively. We obtain certain p-adic properties of the Mahler coefficients of these continuous functions.

Chapter 4 is devoted to p-adic measures on $\mathbb{Z}_p^n$ and their Γ-transforms. We give a generalization of an existing result of Satoh, Kida and Childress which deals with p-adic measures on $\mathbb{Z}_p$ to p-adic measures on $\mathbb{Z}_p^n$ for any n. We prove this result using the p-adic properties of Mahler coefficients discussed in Chapter 3.

In Chapter 5, we discuss some consequences of the results of Chapter 4. We relate the coefficients of a p-adic measure α on $\mathbb{Z}_p^2$ to the λ-invariant of the Iwasawa series of the Γ-transform of α. One can produce similar results for any p-adic measure α defined on $\mathbb{Z}_p^n$, but the number of coefficients of $\widehat{\alpha}(T_1-1,\cdots,T_n-1)$ which are involved increases with n.

Finally in Chapter 6, we mention a few related problems which will possibly provide scope for future research.

Chapter 2

Iwasawa μ-Invariants of Elliptic Curves

In this chapter, we prove some results on μ-invariants of elliptic curves defined over $\mathbb{Q}$. We illustrate our result through some numerical examples.

2.1 Introduction

Suppose that E is an elliptic curve defined over $\mathbb{Q}$, and p is a prime where E has good ordinary reduction. If K is an algebraic extension of $\mathbb{Q}$, then the Selmer group $\mathrm{Sel}_E(K)$ for E over K is a certain subgroup of $H^1(G_K, E(\overline{\mathbb{Q}})_{\mathrm{tors}})$, where $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. The Selmer group fits into an exact sequence

$$0 \to E(K) \otimes \mathbb{Q}/\mathbb{Z} \to \mathrm{Sel}_E(K) \to Ш_E(K) \to 0,$$

where $Ш_E(K)$ denotes the Shafarevich-Tate group for E over K (see [19]). Let $K = \mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Then $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ acts on $\mathrm{Sel}_E(\mathbb{Q}_\infty)$. Its p-primary subgroup $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ can be regarded as a Λ-module, where $\Lambda = \mathbb{Z}_p[[T]]$ is the completed group algebra for Γ over $\mathbb{Z}_p$. The Pontryagin

dual of $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ is defined as

$$X_E(\mathbb{Q}_\infty) := \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_E(\mathbb{Q}_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

We also denote the Pontryagin dual of $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ by $\widehat{\mathrm{Sel}_E(\mathbb{Q}_\infty)_p}$. It is known that $X_E(\mathbb{Q}_\infty)$ is a finitely generated Λ-module. Kato has proven that $X_E(\mathbb{Q}_\infty)$ is Λ-torsion, as Mazur conjectured in [5]. The classification of finitely generated Λ-modules asserts that one has a pseudo-isomorphism

$$X_E(\mathbb{Q}_\infty) \sim \Big(\bigoplus_{i=1}^{n} \Lambda/(f_i(T))^{a_i}\Big) \bigoplus \Big(\bigoplus_{j=1}^{m} \Lambda/(p^{\mu_j})\Big).$$

The $f_i(T)$'s are irreducible distinguished polynomials in Λ. The a_i's and μ_j's are positive integers. The characteristic polynomial for X is

$$f_X(T) = \prod_{j=1}^{m} p^{\mu_j} \prod_{i=1}^{n} f_i(T)^{a_i}.$$

Then the algebraic Iwasawa invariants of $E/\mathbb{Q}$ at the prime p are given by

$$\mu(E) = \mu(f_X(T)) = \sum_{j=1}^{m} \mu_j \quad \text{and} \quad \lambda(E) = \lambda(f_X(T)) = \sum_{i=1}^{n} a_i \deg(f_i(T)).$$

2.2 Selmer Groups

In this section, we define certain Selmer groups of elliptic curves. Let us first fix some notations. For any field extension K/F and any $\mathrm{Gal}(K/F)$-module X, $H^1(K/F, X)$ means $H^1(\mathrm{Gal}(K/F), X)$. Also, $H^1(K, Y)$ denotes $H^1(G_K, Y)$, where G_K is the absolute Galois group of K and Y is any G_K-module.

Let E be an elliptic curve defined over $\mathbb{Q}$. Let Σ denote any finite set of primes containing p, ∞, and the primes of bad reduction for E. The Selmer group $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ is defined as the kernel of the following "global-to-local" map

$$H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \prod_{l\in\Sigma} \mathcal{H}_l(\mathbb{Q}_\infty).$$

For each finite prime $l \in \Sigma$, the group $\mathcal{H}_l(\mathbb{Q}_\infty)$ is defined by

$$\mathcal{H}_l(\mathbb{Q}_\infty) = \prod_{\eta|l} H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty])/im(\kappa_\eta).$$

Here η runs over the finite set of places of $\mathbb{Q}_\infty$ over l, and $(\mathbb{Q}_\infty)_\eta$ denotes the union of the completions of the finite layers $\mathbb{Q}_n$ at η. Also, κ_η denotes the local Kummer map

$$\kappa_\eta : E((\mathbb{Q}_\infty)_\eta) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty]).$$

The following is a classical result. For a proof, see Theorem 2.4 in [19].

Theorem 2.2.1. *(i) Suppose that E is an elliptic curve defined over an algebraic extension K_v of $\mathbb{Q}_l$ where l is a prime, $l \neq p$. Then $E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$.*
(ii) Suppose that E is an elliptic curve defined over $K_v = \mathbb{C}$ or $K_v = \mathbb{R}$. Then $E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$.
Thus, whenever $v \nmid p$, we have $im(\kappa_v) = 0$.

Thus, if $l \neq p$ then Theorem 2.2.1 implies that $\mathcal{H}_l(\mathbb{Q}_\infty)$ is simply the product $\prod_{\eta|l} H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty])$.

Assume that E has good, ordinary reduction at p. Thus, the reduction of E at p is an elliptic curve $\widetilde{E}$ defined over $\mathbb{F}_p$ and $\widetilde{E}(\overline{\mathbb{F}_p})$ has elements of order p. We know that the reduction map $\pi : E[p^\infty] \to \widetilde{E}[p^\infty]$ is surjective. The Selmer group $S_{E[p^\infty]}(\mathbb{Q}_\infty)$ is defined as

$$S_{E[p^\infty]}(\mathbb{Q}_\infty) := \ker\Big(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \prod_{l\in\Sigma} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty])\Big), \tag{2.1}$$

where $\mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty])$ is defined as follows. If $l \neq p$,

$$\mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty]) = \prod_{\eta|l} H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty]).$$

The product is over the finite set of primes η of $\mathbb{Q}_\infty$ lying over l. There is a unique prime η_p of $\mathbb{Q}_\infty$ lying over p. Let I_{η_p} denote the inertia subgroup of $G_{(\mathbb{Q}_\infty)_{\eta_p}}$. We define

$$\mathcal{H}_p(\mathbb{Q}_\infty, E[p^\infty]) = H^1((\mathbb{Q}_\infty)_{\eta_p}, E[p^\infty])/L_{\eta_p}$$

where

$$L_{\eta_p} = \ker\Big(H^1((\mathbb{Q}_\infty)_{\eta_p}, E[p^\infty]) \to H^1(I_{\eta_p}, \widetilde{E}[p^\infty])\Big).$$

Let Σ_0 be any subset of Σ which does not contain p. We define the corresponding "non-primitive" Selmer group by

$$\mathrm{Sel}_E^{\Sigma_0}(\mathbb{Q}_\infty)_p = \ker\Big(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \prod_{l\in\Sigma-\Sigma_0} \mathcal{H}_l(\mathbb{Q}_\infty)\Big).$$

Remark 2.2.1. *It is clear that* $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p \subset \mathrm{Sel}_E^{\Sigma_0}(\mathbb{Q}_\infty)_p$.

We now define a Selmer group for $E[p^i]$ where $i \geq 1$ in the following way. Consider the exact sequence $0 \to \ker(\pi)[p^i] \to E[p^i] \xrightarrow{\pi} \widetilde{E}[p^i] \to 0$ of $G_{\mathbb{Q}_p}$-modules. For any subset Σ_0 of $\Sigma - \{p, \infty\}$, let

$$\mathrm{Sel}_{E[p^i]}^{\Sigma_0}(\mathbb{Q}_\infty) = \ker\Big(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^i]) \to \prod_{l\in\Sigma-\Sigma_0} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^i])\Big).$$

For $l \neq p$, we define $\mathcal{H}_l(\mathbb{Q}_\infty, E[p^i]) = \prod_{\eta|l} H^1(I_\eta, E[p^i])$ and for $l = p$, we define $\mathcal{H}_p(\mathbb{Q}_\infty, E[p^i]) = H^1(I_{\eta_p}, \widetilde{E}[p^i])$.

$\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ is the p-primary Selmer group of $\mathrm{Sel}_E(\mathbb{Q}_\infty)$. It is not difficult to see that $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p = S_{E[p^\infty]}(\mathbb{Q}_\infty)$. The non-primitive Selmer groups $\mathrm{Sel}_E^{\Sigma_0}(\mathbb{Q}_\infty)_p$ and $S_{E[p^\infty]}^{\Sigma_0}(\mathbb{Q}_\infty)$ are also equal. We use these equalities in the proof of the main result. For more details see [19] and [21].

The following result is proved in [21].

Theorem 2.2.2. *We have* $\mu\Big(\widehat{\mathrm{Sel}_E(\mathbb{Q}_\infty)_p}\Big) = \mu\Big(\widehat{\mathrm{Sel}_E^{\Sigma_0}(\mathbb{Q}_\infty)_p}\Big)$.

2.3 Main Results

Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$. Let p be an odd prime where E_1 and E_2 have good ordinary reduction. Assume that $E_1[p] \cong E_2[p]$ as Galois modules. In [21], Greenberg and Vatsal proved that $\mathrm{Sel}_{E_1}(\mathbb{Q}_\infty)[p]$ is finite if and only if $\mathrm{Sel}_{E_2}(\mathbb{Q}_\infty)[p]$ is finite. Consequently, if $\mathrm{Sel}_{E_1}(\mathbb{Q}_\infty)_p$ is Λ-cotorsion and $\mu(E_1) = 0$, then $\mathrm{Sel}_{E_2}(\mathbb{Q}_\infty)_p$ is Λ-cotorsion and $\mu(E_2) = 0$.

In this chapter, we prove the following main result.

Theorem 2.3.1. *Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$. Let p be an odd prime where E_1 and E_2 have good ordinary reduction. Assume that $E_1[p^i] \cong E_2[p^i]$ as Galois modules for $i = \mu(E_1) + 1$. Also assume that both $E_1(\mathbb{Q})[p]$ and $E_2(\mathbb{Q})[p]$ are trivial. Then $\mu(E_1) = \mu(E_2)$. If $E_1[p^i] \cong E_2[p^i]$ as Galois modules for $i = \mu(E_1)$, then $\mu(E_1) \leq \mu(E_2)$.*

Before giving the proof of the above result, we first prove the following results.

Theorem 2.3.2. *Let $S = \mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ and $\widehat{S} = X_E(\mathbb{Q}_\infty)$ be the Pontryagin dual. Let p be a prime where E has good ordinary reduction. Then*

$$\mu(X_E(\mathbb{Q}_\infty)) = \sum_{i=1}^{\infty} \mathrm{corank}_{\mathbb{F}_p[[T]]} \frac{S[p^i]}{S[p^{i-1}]}.$$

Proof. From Definition 1.1.7, we have

$$\mu(X_E(\mathbb{Q}_\infty)) = \sum_{i=1}^{\infty} \mathrm{rank}_{\mathbb{F}_p[[T]]}(X_E(\mathbb{Q}_\infty)[p^i]/X_E(\mathbb{Q}_\infty)[p^{i-1}]).$$

Since $p^{r+1}S \subseteq p^r S$, we have the following exact sequence

$$0 \to \frac{p^r S}{p^{r+1}S} \to \frac{S}{p^{r+1}S} \to \frac{S}{p^r S} \to 0.$$

Taking the Pontryagin dual, we have

$$0 \to \widehat{\left(\frac{S}{p^r S}\right)} \to \widehat{\left(\frac{S}{p^{r+1}S}\right)} \to \widehat{\left(\frac{p^r S}{p^{r+1}S}\right)} \to 0.$$

This implies that

$$\text{rank}_{\mathbb{F}_p[[T]]} \frac{\widehat{(S/p^{r+1}S)}}{\widehat{(S/p^r S)}} = \text{rank}_{\mathbb{F}_p[[T]]} \widehat{\left(\frac{p^r S}{p^{r+1}S}\right)} = \text{corank}_{\mathbb{F}_p[[T]]} \frac{p^r S}{p^{r+1}S}. \tag{2.2}$$

Again, for any module M, we have

$$\widehat{M}[p^r] \cong \widehat{\left(\frac{M}{p^r M}\right)}. \tag{2.3}$$

From (2.2) and (2.3), we have

$$\begin{aligned} \text{rank}_{\mathbb{F}_p[[T]]} \frac{X_E(\mathbb{Q}_\infty)[p^{r+1}]}{X_E(\mathbb{Q}_\infty)[p^r]} &= \text{rank}_{\mathbb{F}_p[[T]]} \frac{\widehat{S}[p^{r+1}]}{\widehat{S}[p^r]} \\ &= \text{rank}_{\mathbb{F}_p[[T]]} \frac{\widehat{(S/p^{r+1}S)}}{\widehat{(S/p^r S)}} \\ &= \text{corank}_{\mathbb{F}_p[[T]]} \frac{p^r S}{p^{r+1}S}. \end{aligned} \tag{2.4}$$

Now consider the following exact sequence of multiplication by p.

$$0 \to (p^{r-1}S)[p] \to (p^{r-1}S) \to (p^{r-1}S) \to \frac{p^{r-1}S}{p^r S} \to 0. \tag{2.5}$$

Also consider the map $\phi : S[p^r] \to (p^{r-1}S)[p]$ defined by $\phi(x) = p^{r-1}x$. This map is well-defined and clearly surjective. We find that $\ker \phi = S[p^{r-1}]$. Therefore

$$\frac{S[p^r]}{S[p^{r-1}]} \cong (p^{r-1}S)[p].$$

Using this isomorphism and taking dual of (2.5), we see that

$$\text{rank}_{\mathbb{F}_p[[T]]} \widehat{\left(\frac{p^{r-1}S}{p^r S}\right)} = \text{rank}_{\mathbb{F}_p[[T]]} \widehat{(p^{r-1}S)}[p] = \text{rank}_{\mathbb{F}_p[[T]]} \widehat{\left(\frac{S[p^r]}{S[p^{r-1}]}\right)}. \tag{2.6}$$

From (2.4) and (2.6), we get

$$\text{corank}_{\mathbb{F}_p[[T]]} \frac{S[p^r]}{S[p^{r-1}]} = \text{rank}_{\mathbb{F}_p[[T]]} \frac{X_E(\mathbb{Q}_\infty)[p^r]}{X_E(\mathbb{Q}_\infty)[p^{r-1}]},$$

and this completes the proof of the theorem. □

Since E has good reduction at p, $E[p^\infty]$ is unramified outside p (see Proposition 4.1 in [11]). Also, $\widetilde{E}[p^\infty]$ is unramified as a $G_{\mathbb{Q}_p}$-module. We prove the following result which is analogous to Proposition 2.8 of [21]. Also see [1].

Theorem 2.3.3. *Let p be an odd prime. Assume that Σ_0 is a subset of $\Sigma - \{p, \infty\}$. Assume that $E(\mathbb{Q})[p] = 0$ and $i \geq 1$. Then*

$$S^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)[p^i] \cong S^{\Sigma_0}_{E[p^i]}(\mathbb{Q}_\infty).$$

Proof. Since $H^0(\mathbb{Q}, E[p]) = E(\mathbb{Q})[p] = 0$ and $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is a pro-p group, we have $H^0(\mathbb{Q}_\infty, E[p^\infty]) = 0$. Consider the exact sequence

$$0 \to E[p^i] \to E[p^\infty] \xrightarrow{p^i} E[p^\infty] \to 0$$

of $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$- modules. Taking $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$ cohomology and using the fact that $H^0(\mathbb{Q}_\infty, E[p^\infty]) = 0$, we find the following isomorphism

$$H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^i]) \cong H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty])[p^i].$$

We now compare the local conditions defining $S^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)[p^i]$ and $S^{\Sigma_0}_{E[p^i]}(\mathbb{Q}_\infty)$. Suppose that σ is a 1-cocycle of $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$ with values in $E[p^i]$. Let $\eta|l$, where $l \neq p$ and $l \in \Sigma - \Sigma_0$. Then I_η acts trivially on $E[p^\infty]$. The map $H^1(I_\eta, E[p^i]) \to H^1(I_\eta, E[p^\infty])$ is injective because $H^0(I_\eta, E[p^\infty]) = E[p^\infty]$ is divisible. Thus, the local conditions at l defining $S^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)[p^i]$ and $S^{\Sigma_0}_{E[p^i]}(\mathbb{Q}_\infty)$ are equivalent. Also, the map

$$H^1(I_{\eta_p}, \widetilde{E}[p^i]) \to H^1(I_{\eta_p}, \widetilde{E}[p^\infty])$$

is injective because $H^0(I_\eta, \widetilde{E}[p^\infty]) = \widetilde{E}[p^\infty]$ is divisible. Hence the local conditions on σ defining the two Selmer groups are equivalent, and this completes the proof. □

We are now ready to prove the Theorem 2.3.1. Let Σ be a finite set of primes containing p, ∞, and all primes where either E_1 or E_2 has bad reduction. Let $\Sigma_0 = \Sigma - \{p, \infty\}$.

Proof of the Theorem 2.3.1: From Theorem 2.3.2 and Theorem 2.2.2, we have

$$\begin{aligned}
\mu(E_1) &= \mu(X_{E_1}(\mathbb{Q}_\infty)) \\
&= \sum_{i=1}^{\infty} \text{corank}_{\mathbb{F}_p[[T]]} \frac{\text{Sel}_{E_1}^{\Sigma_0}(\mathbb{Q}_\infty)_p[p^i]}{\text{Sel}_{E_1}^{\Sigma_0}(\mathbb{Q}_\infty)_p[p^{i-1}]} \\
&= \sum_{i=1}^{\mu(E_1)} \text{corank}_{\mathbb{F}_p[[T]]} \frac{S_{E_1[p^\infty]}^{\Sigma_0}(\mathbb{Q}_\infty)[p^i]}{S_{E_1[p^\infty]}^{\Sigma_0}(\mathbb{Q}_\infty)[p^{i-1}]} \\
&= \sum_{i=1}^{\mu(E_1)} \text{corank}_{\mathbb{F}_p[[T]]} \frac{S_{E_1[p^i]}^{\Sigma_0}(\mathbb{Q}_\infty)}{S_{E_1[p^{i-1}]}^{\Sigma_0}(\mathbb{Q}_\infty)} \\
&= \sum_{i=1}^{\mu(E_1)} \text{corank}_{\mathbb{F}_p[[T]]} \frac{S_{E_2[p^i]}^{\Sigma_0}(\mathbb{Q}_\infty)}{S_{E_2[p^{i-1}]}^{\Sigma_0}(\mathbb{Q}_\infty)} \qquad (2.7) \\
&= \sum_{i=1}^{\mu(E_1)} \text{corank}_{\mathbb{F}_p[[T]]} \frac{\text{Sel}_{E_2}^{\Sigma_0}(\mathbb{Q}_\infty)_p[p^i]}{\text{Sel}_{E_2}^{\Sigma_0}(\mathbb{Q}_\infty)_p[p^{i-1}]} \\
&\leq \mu(E_2).
\end{aligned}$$

To get the equality (2.7), we use Theorem 2.3.3 and the isomorphisms $E_1[p^i] \cong E_2[p^i]$ as Galois modules for $i = \mu(E_1)$. Also, we use the fact that $S_{E[p^i]}^{\Sigma_0}(\mathbb{Q}_\infty)$ is determined completely by the $G_\mathbb{Q}$-module $E[p^i]$. Again, if $E_1[p^i] \cong E_2[p^i]$ as Galois modules for $i = \mu(E_1) + 1$, then $\text{corank}_{\mathbb{F}_p[[T]]} \frac{\text{Sel}_{E_1[p^i]}^{\Sigma_0}(\mathbb{Q}_\infty)}{\text{Sel}_{E_1[p^{i-1}]}^{\Sigma_0}(\mathbb{Q}_\infty)} = 0$ implies $\text{corank}_{\mathbb{F}_p[[T]]} \frac{\text{Sel}_{E_2[p^i]}^{\Sigma_0}(\mathbb{Q}_\infty)}{\text{Sel}_{E_2[p^{i-1}]}^{\Sigma_0}(\mathbb{Q}_\infty)} = 0$ for $i = \mu(E_1) + 1$. Hence if $E_1[p^i] \cong E_2[p^i]$ as Galois modules for $i = \mu(E_1) + 1$, then $\mu(E_1) = \mu(E_2)$. □

2.4 Numerical Examples

In this section, we illustrate the Main Theorem through some examples. Let us consider the following elliptic curves:

$$E_1 : y^2 = x^3 - x^2 - 2858x - 10163, \qquad [4900a1] \tag{2.8}$$

$$E_2 : y^2 = x^3 - x^2 - 174358x - 27964663, \qquad [4900a2] \tag{2.9}$$

$$E_3 : y^2 = x^3 - x^2 - 24908x + 1522312, \qquad [4900b1] \tag{2.10}$$

$$E_4 : y^2 = x^3 - x^2 + 24092x + 6422312. \qquad [4900b2] \tag{2.11}$$

Here the labels in the square brackets denote the Cremona numbers of the curves (see [8]). These are curves of conductor 4900. We begin with some facts about these curves. There is a single 3-isogeny $\phi : E_1 \longrightarrow E_2$ and $\psi : E_3 \longrightarrow E_4$. These isogenies are defined over $\mathbb{Q}$. The exact formulas of ϕ and ψ are given below:

$$\phi(x,y) = \left(\frac{x^3 - 164x^2 + 41024x - 1612100}{x^2 - 164x + 6724}, \frac{x^3y - 246x^2y - 14128xy - 139768y}{x^3 - 246x^2 + 20172x - 551368} \right)$$

$$\psi(x,y) = \left(\frac{x^3 - 164x^2 - 3076x + 901600}{x^2 - 164x + 6724}, \frac{x^3y - 246x^2y + 29972xy - 1550968y}{x^3 - 246x^2 + 20172x - 551368} \right)$$

All the four curves have good ordinary reduction at 3. A computation using 3-division polynomials shows that there is no non-trivial rational 3-torsion point on these curves.

The Weierstrass equations of E_1, E_2, E_3, and E_4 are given by

$$WE_1 : y^2 = x^3 - 3704400x - 518616000, \tag{2.12}$$

$$WE_2 : y^2 = x^3 - 225968400x - 1307430936000, \tag{2.13}$$

$$WE_3 : y^2 = x^3 - 32281200x + 70637616000, \tag{2.14}$$

$$WE_4 : y^2 = x^3 + 31222800x + 300014064000. \tag{2.15}$$

Lemma 2.4.1. *Suppose that for an elliptic curve $E/\mathbb{Q}$, $\mathbb{Q}(E[3])$ denotes the field of 3-torsion points. Then $\mathbb{Q}(E_1[3]) = \mathbb{Q}(E_3[3])$ and $\mathbb{Q}(E_2[3]) = \mathbb{Q}(E_4[3])$. Moreover, these fields are of degree 12 over $\mathbb{Q}$. There is a 3-torsion point of E_1 and E_3 defined over $\mathbb{Q}(\sqrt{5})$, while E_2 and E_4 have a 3-torsion point defined over $\mathbb{Q}(i\sqrt{15})$.*

Proof. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$. Then its 3-division polynomial is $\psi(x) = 3x^4 + 6ax^2 + 12bx - a^2$. Let x_0, x_1 be two different roots of ψ, so that $\psi(x) = 3(x - x_0)(x^3 + x_0x^2 + (2a + x_0^2)x + 4b + 2ax_0 + x_0^3)$.

Let $y_1^2 = x_1^3 + ax_1 + b$. As x_1 is a root of the second factor of $\psi(x)$, we get

$$\begin{aligned} -y_1^2 &= x_0x_1^2 + (2a + x_0^2)x_1 + 4b + 2ax_0 + x_0^3 - ax_1 - b, \\ i.e., \quad -4y_1^2x_0 &= 4x_0^2x_1^2 + 4x_0^3x_1 + 4ax_0x_1 + 8ax_0^2 + 4x_0^4 - 3x_0^4 - 6ax_0^2 + a^2 \\ &= (x_0^2 + a + 2x_0x_1)^2 \\ y_1^2 &= \frac{-(x_0^2 + 2x_0x_1 + a)^2}{4x_0}, \end{aligned}$$

giving

$$y_1 = \pm\sqrt{-x_0}(x_1 + \frac{x_0^2 + a}{2x_0}).$$

Similarly,

$$y_0 = \pm\sqrt{-x_1}(x_0 + \frac{x_1^2 + a}{2x_1}).$$

Therefore, the field of the 3-torsion points is given by

$$\mathbb{Q}(x_0, \sqrt{-x_0}, x_1, \sqrt{-x_1}, x_2, \sqrt{-x_2}, x_3, \sqrt{-x_3}).$$

In other words,

$$\mathbb{Q}(E[3]) = \mathbb{Q}(\sqrt{-x_0}, \sqrt{-x_1}, \sqrt{-x_2}, \sqrt{-x_3}).$$

Hence $\mathbb{Q}(E[3])$ is the splitting field of

$$\psi(-X^2) = 3X^8 + 6aX^4 - 12bX^2 - a^2.$$

Let $\psi_i(-X^2)$ denote the above polynomial for $WE_i : i = 1, \cdots, 4$. We use this to compute the splitting fields of $\psi_i(-X^2)$, where $\psi_i(-X^2)$ denotes the above polynomial for $WE_i : i = 1, \cdots, 4$. Using MAGMA we compute and find that the splitting fields of $\psi_1(-X^2)$ and $\psi_3(-X^2)$ are same. Similarly, the splitting fields of $\psi_2(-X^2)$ and $\psi_4(-X^2)$ are same. Moreover, we compute that the degree of the extensions $\mathbb{Q}(E_i[3])$ over $\mathbb{Q}$ is 12 for $i = 1, \cdots, 4$.

Using MAGMA, we solve the division polynomial of each of the above four curves and in each case we find a rational root. These are the respective x-coordinates for the 3-torsion points which are found to be 2940, -8820, 2940, and -8820. The corresponding y-coordinates are the square roots of 14002632000, -518616000, 1143072000, and -661500000000. We can factorize them to get

$$2^6 3^6 5^3 7^4, -2^6 3^3 5^3 7^4, 2^8 3^6 5^3 7^2, -2^8 3^3 5^9 7^2.$$

Thus, we get a 3-torsion point P_i on the curve E_i for each $i = 1, \cdots, 4$. These points are

$$\begin{aligned} P_1 &= (2940, 2^3 3^3 7^2 5\sqrt{5}), \\ P_2 &= (-8820, 2^3 3.5.7^2\sqrt{15}i), \\ P_3 &= (2940, 2^4 3^3.5.7\sqrt{5}), \\ P_4 &= (-8820, 2^4.3.5^4.7\sqrt{15}i). \end{aligned}$$

Therefore both E_1 and E_3 have a 3-torsion point over $L = \mathbb{Q}(\sqrt{5})$. Also, both E_2 and E_4 have a 3-torsion point over $K = \mathbb{Q}(\sqrt{15}i)$. □

Our next goal is to show that $E_1[9] \cong E_3[9]$, $E_2[3] \cong E_4[3]$, and $E_2[9] \ncong E_4[9]$ as $G_{\mathbb{Q}}$-modules. Using SAGE, William Stein has checked that $E_1[9]$ and $E_3[9]$ are the same as subvarieties of $J_0(4900)$. Not only $E_1[9]$ and $E_3[9]$ are isomorphic as $G_{\mathbb{Q}}$-modules, but they are "equal" if we view E_1 and E_3 as subvarieties of the abelian variety $J_0(4900)$. However, the same technique can not be applied for the curves E_2 and E_4 as $E_2[9]$ and $E_4[9]$ are not subvarieties of $J_0(4900)$. We first prove that $E_2[3] \cong E_4[3]$ as $G_{\mathbb{Q}}$-modules. We point out that the same proof also works to give a proof of $G_{\mathbb{Q}}$-module isomorphism $E_1[3] \cong E_3[3]$.

Theorem 2.4.1. *As $G_{\mathbb{Q}}$-modules, $E_1[3] \cong E_3[3]$ and $E_2[3] \cong E_4[3]$.*

Proof. Recall the Weierstrass equations of E_1, E_2, E_3, and E_4 above. Let $L = \mathbb{Q}(\sqrt{5})$ and $K = \mathbb{Q}(i\sqrt{15})$. We denote the absolute Galois groups of L and K by G_L and G_K respectively. Let ρ_i denote the $G_{\mathbb{Q}}$-representation associated to $E_i[3]$, where $i = 1, \cdots, 4$. Then

$$\rho_2|_{G_K} \sim \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix},$$

where $\chi = \chi_3 \pmod 3$ is the mod 3 cyclotomic character. Similarly,

$$\rho_4|_{G_K} \sim \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}.$$

Moreover, as $G_{\mathbb{Q}}$-representations, we know that each ρ_i is reducible, since each of these curves admit a 3-isogeny. Suppose that

$$\rho_2(g) \sim \begin{pmatrix} \epsilon(g) & b(g) \\ 0 & \eta(g) \end{pmatrix} \quad \text{and} \quad \rho_4(g) \sim \begin{pmatrix} \epsilon'(g) & b'(g) \\ 0 & \eta'(g) \end{pmatrix} \quad \forall g \in G_{\mathbb{Q}},$$

where $\epsilon, \epsilon', \eta, \eta'$ are all characters of $G_{\mathbb{Q}}$. Note that the values of ϵ, η lie in $\{1, -1\}$. More precisely, if $\Delta := G_{\mathbb{Q}}/G_K =< \tau >$, then $\epsilon(\tau) = -1$ as there is no non-trivial rational 3-torsion. Therefore, $\eta(\tau) = -\chi(\tau)$.

Comparing the traces of $\rho_2(g)\mid_{G_K}$ we get $\epsilon(g)+\eta(g)=1+\chi(g)$, for $g\in G_{\mathbb{Q}}$. Therefore by Artin's theorem on linear independence of characters, either $\epsilon(g)=\chi(g)$ or 1 for $g\in G_K$. Suppose that $\epsilon(g)=\chi(g)$. Then $\rho_2\mid_{G_K}(g)\sim\begin{pmatrix}\chi(g) & b(g)\\ 0 & \eta(g)\end{pmatrix}$, which means that there is a point in $E_2[3]$, say P' such that $gP'=\chi(g)P'$. There is also a point P_2 in $E_2[3]$ such that $gP_2=P_2$. It is easy to see that P_2 is not in the span of P'. Hence with respect to these points as basis, we have $\rho_2\mid_{G_K}(g)\sim\begin{pmatrix}\chi(g) & 0\\ 0 & \eta(g)\end{pmatrix}$. Therefore the kernel of $\rho_2\mid_{G_K}$ cuts out a field whose extension degree over K is 2 or 4. This is not possible as the extension degree over K is computed to be 6 in the previous lemma. Hence, $\epsilon(g)=1$ and $\eta(g)=\chi(g)$ for $g\in G_K$.

Similarly, for the $G_{\mathbb{Q}}$-representation ρ_4, we can show that $\epsilon'(\tau)=-1$ and $\eta'(\tau)=-\chi(\tau)$. As above, $\epsilon'\mid_{G_K}(g)=1$ and $\eta'\mid_{G_K}(g)=\chi(g)$. Now, for any $\gamma=h\tau\in G_{\mathbb{Q}}$ with $h\in G_K$, we have

$$\epsilon'(h\tau)=-1=\epsilon(h\tau)\text{ and }\eta'(h\tau)=\chi(h\tau)=\eta(h\tau).$$

This implies that as $G_{\mathbb{Q}}$ representations, we have

$$\rho_2\sim\begin{pmatrix}\epsilon & b\\ 0 & \eta\end{pmatrix}\quad\text{and}\quad\rho_4\sim\begin{pmatrix}\epsilon & b'\\ 0 & \eta\end{pmatrix}.$$

Now for $g\in G_{\mathbb{Q}}$,

$$\begin{aligned}\rho_2(g)&\sim\begin{pmatrix}1 & 0\\ 0 & \eta(g)\end{pmatrix}\begin{pmatrix}\epsilon(g) & b(g)\\ 0 & \eta(g)\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & \eta^{-1}(g)\end{pmatrix}\\ &=\begin{pmatrix}\epsilon(g) & \eta^{-1}(g)b(g)\\ 0 & \eta(g)\end{pmatrix}.\end{aligned}$$

Let $\mathbf{F}=\mathbb{Z}/3\mathbb{Z}$ as a vector space over itself. Let $u=\eta^{-1}b$. For $g,h\in G_{\mathbb{Q}}$, we have $\rho_2(gh)=\rho_2(g)\rho_2(h)$. From this it can be easily seen that u is a 1-cocycle in $Z^1(G_{\mathbb{Q}},\mathbf{F}(\epsilon\eta^{-1}))$. Similarly, $v=\eta^{-1}b'$ is a 1-cocycle in $Z^1(G_{\mathbb{Q}},\mathbf{F}(\epsilon\eta^{-1}))$.

Suppose that u, v differ by a 1-coboundary d in $B^1(G_{\mathbb{Q}}, \mathbf{F}(\epsilon\eta^{-1}))$, say $d(g) = \epsilon(g)\eta^{-1}(g)t - t$ for some $t \in \mathbf{F}$. Then

$$\begin{pmatrix} 1 & \eta^{-1}(g)t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \epsilon(g) & u(g) \\ 0 & \eta(g) \end{pmatrix} \begin{pmatrix} 1 & -\eta^{-1}(g)t \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \epsilon(g) & u(g) - \{\epsilon(g)\eta^{-1}(g)t - t\} \\ 0 & \eta(g) \end{pmatrix}$$

$$= \begin{pmatrix} \epsilon(g) & u(g) - d(g) \\ 0 & \eta(g) \end{pmatrix}$$

$$= \begin{pmatrix} \epsilon(g) & v(g) \\ 0 & \eta(g) \end{pmatrix}$$

This proves that

$$\begin{pmatrix} \epsilon(g) & u(g) \\ 0 & \eta(g) \end{pmatrix} \sim \begin{pmatrix} \epsilon(g) & v(g) \\ 0 & \eta(g) \end{pmatrix}.$$

Therefore, to show that $E_2[3] \cong E_4[3]$ it is enough to show that $[b] = [b'] \in H^1(G_{\mathbb{Q}}, \mathbf{F}(\epsilon\eta^{-1}))$. To do this, we use the inflation-restriction sequence with respect to $G_K \subset G_{\mathbb{Q}}$. Recall that $\Delta = G_{\mathbb{Q}}/G_K =< \tau >$, then

$$0 \longrightarrow H^1(\Delta, \mathbf{F}(\epsilon\eta^{-1})^{G_K}) \longrightarrow H^1(G_{\mathbb{Q}}, \mathbf{F}(\epsilon\eta^{-1}))$$
$$\longrightarrow H^1(G_K, \mathbf{F}(\epsilon\eta^{-1}))^{\Delta} \longrightarrow H^2(\Delta, \mathbf{F}(\epsilon\eta^{-1})^{G_K}).$$

Since Δ acts non-trivially on the one dimensional space $\mathbf{F}(\epsilon\eta^{-1})$ and Δ is cyclic, therefore the first term of this sequence vanishes. Hence we have an inclusion

$$H^1(G_{\mathbb{Q}}, \mathbf{F}(\epsilon\eta^{-1})) \hookrightarrow H^1(G_K, \mathbf{F}(\epsilon\eta^{-1}))^{\Delta} \hookrightarrow H^1(G_K, \mathbf{F}(\epsilon\eta^{-1}))$$

where the first injection is a restriction map. But, we have seen earlier that $\epsilon \mid_{G_K} = 1$ so that $\eta \mid_{G_K} = \chi$. Using this, the previous inclusions can be written

as

$$H^1(G_{\mathbb{Q}}, \mathbf{F}(\epsilon\eta^{-1})) \hookrightarrow H^1(G_K, \mathbf{F}(\chi^{-1}))^{\Delta} \hookrightarrow H^1(G_K, \mathbf{F}(\chi^{-1})). \tag{2.16}$$

Let M be the extension over K cut out by χ, $H = G_M$ and $D = G(M/K)$. Then $M = K(\mu_3)$ so that D has order 2.

Using the inflation restriction sequence again, but with respect to $H \subset G_K$, we get

$$0 \to H^1(D, \mathbf{F}(\chi^{-1})^H) \to H^1(G_K, \mathbf{F}(\chi^{-1})) \to H^1(H, \mathbf{F}(\chi^{-1}))^D \to H^2(D, \mathbf{F}(\chi^{-1})^H).$$

As D is cyclic and H acts trivially on $\mathbf{F}$, we get the first term in the exact sequence to be

$$H^1(D, \mathbf{F}(\chi^{-1})) = \mathbf{F}(\chi^{-1})_D = \mathbf{F}(\chi^{-1})/\langle (1 - \chi^{-1}(g))\mathbf{F} | g \in D \rangle$$

Since χ^{-1} is not trivial on D, therefore $\langle (1 - \chi^{-1}(g))\mathbf{F} | g \in D \rangle = \mathbf{F}$ and hence the quotient is trivial. Therefore we get the following injection

$$H^1(G_K, \mathbf{F}(\chi^{-1})) \hookrightarrow H^1(H, \mathbf{F}(\chi^{-1}))^D$$

where the injection is given by the restriction map.

Combining this injection with the injection in (2.16), we get

$$H^1(G_{\mathbb{Q}}, \mathbf{F}(\epsilon\eta^{-1})) \hookrightarrow H^1(G_K, \mathbf{F}(\chi^{-1})) \hookrightarrow H^1(H, \mathbf{F}(\chi^{-1}))^D.$$

Let $b \mid_{G_K} = a, b' \mid_{G_K} = a'$. By the first injectivity, to show that b and b' are co-homologous it is enough to show that a and a' differ by a co-boundary. We give a proof of this below.

Since H acts trivially on $\mathbf{F}(\chi^{-1})$ therefore the third term in the above sequence is nothing but $\mathrm{Hom}(H, \mathbf{F})^D$. Hence the image of a, which is $a|_H$, is a homomorphism from $H \longrightarrow \mathbf{F}$. We now use the fact that the field extensions of

the 3-torsion points are the same as computed by Magma. Therefore the field cut out by $a|_H$ and $a'|_H$ are the same. In other words, the kernel of $a|_H$ and $a'|_H$ are the same. Since both $a|_H$ and $a'|_H$ are non-trivial it is also easy to see that they are surjective and hence if J denotes the kernel then both $a|_H$ and $a'|_H$ are isomorphisms from H/J onto $\mathbf{F}$. Since $|H/J| = |\mathbf{F}| = 3$, therefore $|\mathrm{Isom}(H/J, \mathbf{F})| = 2$ and hence either $a|_H = a'|_H$ or $a|_H = -a'|_H$.

If $a|_H = a'|_H$, then by injectivity of the above exact sequence it follows that $[a] = [a']$ and we are done.

Let $a|_H = -a'|_H = 2a'|_H$, then $[a] = [2a']$. Therefore $[b] = [2b']$. Note that $[2b'] = 2[b']$, so that we have the following equivalence

$$\begin{pmatrix} \epsilon & b \\ 0 & \eta \end{pmatrix} \sim \begin{pmatrix} \epsilon & 2b' \\ 0 & \eta \end{pmatrix}.$$

Now, since we are computing mod 3, we have the following

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} \epsilon & b' \\ 0 & \eta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} \epsilon & 2b' \\ 0 & \eta \end{pmatrix}.$$

Therefore

$$\begin{pmatrix} \epsilon & 2b' \\ 0 & \eta \end{pmatrix} \sim \begin{pmatrix} \epsilon & b' \\ 0 & \eta \end{pmatrix}.$$

This implies that

$$\begin{pmatrix} \epsilon & b \\ 0 & \eta \end{pmatrix} \sim \begin{pmatrix} \epsilon & b' \\ 0 & \eta \end{pmatrix}$$

Therefore, $\rho_2 \sim \rho_4$. In other words, the mod 3 representations are isomorphic. This proves that $E_2[3]$ and $E_4[3]$ are isomorphic as $G_{\mathbb{Q}}$-modules.

In a similar manner, since the elliptic curves E_1 and E_3 have a 3-torsion point over $L = \mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(E_1[3]) = \mathbb{Q}(E_3[3])$, along with the fact that $\mathbb{Q}(E_1[3])$ has degree 12 over $\mathbb{Q}$, we see that $\rho_1 \sim \rho_3$, thereby completing the proof. □

Theorem 2.4.2. *As $G_{\mathbb{Q}}$-modules, $E_1[9] \cong E_3[9]$ and $E_2[9] \ncong E_4[9]$.*

Proof. Using Sage, William Stein has checked that $E_1[9]$ and $E_3[9]$ are isomorphic as Galois modules, in fact "equal", as subvarieties of $J_0(4900)$. The 9-division polynomials of E_2 and E_4 have factors of degree 1+3+9+27. Using Sage it can be checked that the two degree 27 polynomials (the largest factors of the two 9-division polynomials) do not define isomorphic fields. Let $f : E_2[9] \longrightarrow E_4[9]$ be an isomorphism of Galois modules. Then for each $P \in E_2[9]$ its field of definition $\mathbb{Q}(P)$ is equal to $\mathbb{Q}(f(P))$. Clearly subgroup of $G_{\mathbb{Q}}$ fixing $\{P, -P\}$ is the same subgroup for P as for $f(P)$. The fixed field of this subgroup is $\mathbb{Q}(x(P))$, hence $\mathbb{Q}(x(P)) = \mathbb{Q}(x(f(P))$. Since the last fact holds for every (nonzero) $P \in E_2[9]$, it follows that the two 9-division polynomials (whose roots are all the $x(P)$ for nonzero P) match up, in the sense that there is a bijection from the irreducible factors of the first to those of the second such that for each irreducible factor h_2 of the first which matches the factor h_4 of the second, the fields $\mathbb{Q}[x]/(h_2)$ and $\mathbb{Q}[x]/(h_4)$ are isomorphic. But $E_2[9]$ and $E_4[9]$ have a single irreducible factor of degree 27 in its 9-division polynomial, but these do not define isomorphic number fields. This proves that $E_2[9] \ncong E_4[9]$ as Galois modules. □

Using MAGMA, we compute the first coefficients of the p-adic L-functions of E_1 and E_3, and they are not divisible by 3. Therefore, assuming the *main conjecture*, the μ-invariant of E_1 and E_3 are 0. Moreover, since the ratio of the periods is 3 in each isogeny class, so the μ-invariant of E_2 and E_4 are 1. This numerically verifies our Main theorem.

Chapter 3

p-Adic Properties of Mahler Coefficients

In this chapter, we derive p-adic properties of certain Mahler coefficients exploiting some combinatorial identities. These p-adic properties of the Mahler coefficients are used to determine a relation between the λ-invariants of a p-adic measure on $\mathbb{Z}_p^n$ and its Γ-transform in the next chapter.

3.1 Introduction

A classical theorem of Mahler (see [22, p.p. 99, Theorem 1.3]) states that any continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ may be written uniquely in the form

$$f(x) = \sum_{n=0}^{\infty} a_n(f) \binom{x}{n},$$

where $a_n(f) \in \mathbb{Q}_p, a_n(f) \mapsto 0$ as $n \mapsto \infty$. In fact

$$a_n(f) = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} f(j). \tag{3.1}$$

This theorem may be generalized to continuous functions $f : \mathbb{Z}_p \to K$, where

K is any finite extension of $\mathbb{Q}_p$. Note that if $\mathcal{O}$ is the ring of integers of K and $f : \mathbb{Z}_p \to \mathcal{O}$, then $a_n(f) \in \mathcal{O}$.

Furthermore, if $f : \mathbb{Z}_p^n \to \mathcal{O}$ is continuous, we may write (by repeated application of the generalization of Mahler theorem)

$$f(x_1, \cdots, x_n) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} a_{m_1,\cdots,m_n}(f) \binom{x_1}{m_1} \cdots \binom{x_n}{m_n},$$

where

$$a_{m_1,\cdots,m_n}(f) = \sum_{j_1=0}^{m_1} \cdots \sum_{j_n=0}^{m_n} (-1)^{m_1-j_1} \cdots (-1)^{m_n-j_n} \binom{m_1}{j_1} \cdots \binom{m_n}{j_n} f(j_1, \cdots, j_n)$$
$$\to 0 \quad \text{in} \quad \mathcal{O}.$$

The constants $a_{m_1,\cdots,m_n}(f)$ are called the *Mahler coefficients* of the function f.

Let u be a topological generator of $1 + p\mathbb{Z}_p$. Let us consider the continuous functions $f_m : \mathbb{Z}_p \to \mathbb{Z}_p$ and $f_{m_1,\cdots,m_n} : \mathbb{Z}_p^n \to \mathbb{Z}_p$ defined by $f_m(x) = \binom{u^x}{m}$ and $f_{m_1,\cdots,m_n}(x_1, \cdots, x_n) = f_{m_1}(x_1) \cdots f_{m_n}(x_n)$, respectively.

Using the classical theorem of Mahler, we find the following:

$$f_m(x) = \binom{u^x}{m} = \sum_{j=0}^{\infty} a_j(f_m) \binom{x}{j} \tag{3.2}$$

$$f_{m_1,\cdots,m_n}(x_1, \cdots, x_n) = \sum_{j_1=0}^{\infty} \cdots \sum_{j_n=0}^{\infty} a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n}) \binom{x_1}{m_1} \cdots \binom{x_n}{m_n}. \tag{3.3}$$

Now, we have the following nice relation

$$\begin{aligned}
&a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n}) \\
&= \sum_{i_1=0}^{j_1} \cdots \sum_{i_n=0}^{j_n} (-1)^{j_1-i_1} \cdots (-1)^{j_n-i_n} \binom{j_1}{i_1} \cdots \binom{j_n}{i_n} f_{m_1,\cdots,m_n}(i_1, \cdots, i_n) \\
&= \sum_{i_1=0}^{j_1} \cdots \sum_{i_n=0}^{j_n} (-1)^{j_1-i_1} \cdots (-1)^{j_n-i_n} \binom{j_1}{i_1} \cdots \binom{j_n}{i_n} f_{m_1}(i_1) \cdots f_{m_n}(i_n) \\
&= a_{j_1}(f_{m_1}) \cdots a_{j_n}(f_{m_n})
\end{aligned} \tag{3.4}$$

The primary goal of this chapter is to study certain p-adic properties of the Mahler coefficients $a_j(f_m)$ and $a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n})$. To achieve this goal, we need certain combinatorial identities which are derived in the next section.

3.2 Certain Combinatorial Identities

The following result was a crucial ingredient in the work of Childress [14, p.p. 369, Lemma 4].

Result 3.2.1. *For $n \geq 1$, we have*

$$\sum_{i=1}^{n}(-1)^{n-i}\binom{n}{i}\binom{ti}{n} = t^n.$$

Here we prove a more general result.

Lemma 3.2.1. *For non-negative integers n, t, k, we have*

$$\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}\binom{t(i+k)}{n} = t^n. \tag{3.5}$$

Proof. The result is obvious for $t = 0$ or $n = 0$. So we assume $n, t \geq 1$ and $k \geq 0$. Let N, N', T be sets such that $N \subseteq N', |N| = n, |N'| = n + k$, and $|T| = t$. Let R be the set of all n-subsets of $N' \times T$. Clearly $|R| = \binom{t(n+k)}{n}$. Also, for $a \in N$, let R_a be the set of all n-subsets A of $N' \times T$ such that $(a, b) \notin A$ for any $b \in T$. Obviously R_a is the set of all n-subsets of $(N' - \{a\}) \times T$ and hence $|R_a| = \binom{t(n+k-1)}{n}$.

For $I \subseteq N$, let R_I be the set of all n-subsets A of $N' \times T$ such that $(a, b) \notin A$ for any $a \in I$ and for any $b \in T$. Clearly R_I is the set of all n-subsets of $(N' - I) \times T$ and hence

$$|R_I| = \binom{t(n+k-i)}{n}, \text{ where } |I| = i. \tag{3.6}$$

If $I = \{a_1, \cdots, a_i\}$, then clearly $R_I = R_{a_1} \cap \cdots \cap R_{a_i}$. Thus

$$|R_{a_1} \cap \cdots \cap R_{a_i}| = \binom{t(n+k-i)}{n}.$$

By inclusion-exclusion principle, we get

$$\begin{aligned}
&|\bigcup_{a\in N} R_a| \\
&= \sum_{a\in N} |R_a| - \sum_{\{a_1,a_2\}\subseteq N} |R_{a_1} \cap R_{a_2}| + \cdots + (-1)^{i+1} \sum_{\{a_1,\cdots,a_i\}\subseteq N} |R_{a_1} \cap \cdots \cap R_{a_i}| \\
&\qquad + \cdots + (-1)^{n+1} |\bigcap_{a\in N} R_a| \\
&= \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} \binom{(n+k-i)t}{n}. \qquad (3.7)
\end{aligned}$$

Therefore,

$$\begin{aligned}
&|R - \bigcup_{a\in N} R_a| \\
&= |R| - |\bigcup_{a\in N} R_a| \\
&= \binom{t(n+k)}{n} - \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} \binom{(n+k-i)t}{n} \\
&= \sum_{i=0}^{n} (-1)^{i} \binom{n}{i} \binom{t(n+k-i)}{n} \\
&= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \binom{t(i+k)}{n}. \qquad (3.8)
\end{aligned}$$

A function $f : N \to T$ may be viewed as an n-subset of $N \times T$. Conversely, an n-subset $A \subseteq N \times T$ defines a function $f : N \to T$ if and only if the cardinality of the set $\{a \in N : (a, b) \in A \text{ for some } b \in T\}$ is equal to n. Therefore, it is not difficult to see that there is a one-to-one correspondence between $R - \bigcup_{a\in N} R_a$ and the set of all functions from N to T. Thus $|R - \bigcup_{a\in N} R_a| = t^n$, which proves the result because of (3.8). □

Remark 3.2.1. *The result 3.2.1 of Childress is nothing but lemma 3.2.1 with* $k = 0$.

Lemma 3.2.2. *For non-negative integers* n, t *with* $n > 1$, *we have*

$$\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}\binom{ti}{n-1} = 0.$$

Proof. Since $n > 1$, we have $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$. Using this and Lemma 3.2.1 for $k = 1$, we get

$$\begin{aligned}
&\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}\binom{ti}{n-1} \\
&= \left\{\sum_{i=0}^{n}(-1)^{n-i}\binom{n-1}{i}\binom{ti}{n-1}\right\} + \left\{\sum_{i=0}^{n}(-1)^{n-i}\binom{n-1}{i-1}\binom{ti}{n-1}\right\} \\
&= -\left\{\sum_{i=0}^{n-1}(-1)^{n-1-i}\binom{n-1}{i}\binom{ti}{n-1}\right\} + \left\{\sum_{i=0}^{n-1}(-1)^{n-1-i}\binom{n-1}{i}\binom{t(i+1)}{n-1}\right\} \\
&= -t^{n-1} + t^{n-1} = 0.
\end{aligned}$$

This completes the proof of the lemma. □

3.3 p-adic properties of Mahler coefficients

Let us fix a topological generator $u = 1 + t_1 p + t_2 p^2 + \cdots$ of $1 + p\mathbb{Z}_p$. Hence t_1 is a unit. We now prove two important binomial expansions in the following lemma.

Lemma 3.3.1. *For* $n \geq 1$, *we have*

$$(1+T)^{u^n} \equiv (1+T)(1+T^p)^{nt_1}(1+T^{p^2})^{\frac{n(n-1)}{2}t_1^2+nt_2} + \textit{higher order terms} \pmod p, \tag{3.9}$$

$$(1+T)^{u^{p+n}} \equiv (1+T)(1+T^p)^{nt_1}(1+T^{p^2})^{t_1+\frac{n(n-1)}{2}t_1^2+nt_2} + \textit{higher order terms} \pmod p. \tag{3.10}$$

Proof. For any $k \geq 1$, we have

$$(1+T)^{p^k} \equiv (1+T^{p^k}) \pmod{p}.$$

This implies that

$$\begin{aligned}(1+T)^u &= (1+T)^{1+t_1p+t_2p^2+\cdots} \\ &\equiv (1+T)(1+T^p)^{t_1}(1+T^{p^2})^{t_2} + \text{ higher order terms } (\text{mod } p).\end{aligned}$$

Hence the statement (3.9) is true for $n = 1$. Suppose that it is true for a given n. Then

$$\begin{aligned}&(1+T)^{u^{n+1}} \\ &= (1+T)^{u^n(1+t_1p+t_2p^2+\cdots)} \\ &\equiv (1+T)^{u^n}(1+T^p)^{t_1u^n}(1+T^{p^2})^{t_2u^n} + \text{ higher order terms } (\text{mod } p) \\ &\equiv (1+T)(1+T^p)^{nt_1}(1+T^{p^2})^{\frac{n(n-1)}{2}t_1^2+nt_2}(1+T^p)^{t_1}(1+T^{p^2})^{nt_1{}^2}(1+T^{p^2})^{t_2} \\ &\quad + \text{higher order terms } (\text{mod } p) \\ &\equiv (1+T)(1+T^p)^{(n+1)t_1}(1+T^{p^2})^{\frac{(n+1)n}{2}t_1^2+(n+1)t_2} \\ &\quad + \text{ higher order terms } (\text{mod } p). \qquad (3.11)\end{aligned}$$

Hence the result is true for $n+1$. Using the principle of mathematical induction, the statement (3.9) is true for any $n \geq 1$. Again,

$$u^p = 1 + t_1p^2 + \text{ higher order terms.} \qquad (3.12)$$

Using (3.9) and (3.12), we find that

$$\begin{aligned}(1+T)^{u^{p+n}} &= (1+T)^{u^n(1+t_1p^2+\cdots)} \\ &\equiv (1+T)^{u^n}(1+T^{p^2})^{t_1u^n} + \text{ higher order terms } (\text{mod } p).\end{aligned}$$

$$\equiv (1+T)(1+T^p)^{nt_1}(1+T^{p^2})^{\frac{n(n-1)}{2}t_1^2+nt_2}(1+T^{p^2})^{t_1}$$
$$+ \text{ higher order terms } (\text{mod } p).$$
$$\equiv (1+T)(1+T^p)^{nt_1}(1+T^{p^2})^{t_1+\frac{n(n-1)}{2}t_1^2+nt_2}$$
$$+ \text{ higher order terms } (\text{mod } p). \tag{3.13}$$

This completes the proof of the lemma. □

3.3.1 Mahler Coefficients $a_j(f_m)$

Using the binomial expansions (3.9) and (3.10), we prove the following lemmas about the Mahler coefficients $a_j(f_m)$ for different j and m. Recall that

$$f_m(x) = \binom{u^x}{m} \quad \text{and} \quad a_j(f_m) = \sum_{i=0}^{j}(-1)^{j-i}\binom{j}{i}f_m(i).$$

Lemma 3.3.2. *Suppose that $1 \le k < p$, then $a_k(f_{pk}) \equiv {t_1}^k \pmod p$. Also,*

$$a_p(f_{p^2}) \equiv t_1 \pmod p \quad \textit{and} \quad a_{p+1}(f_{p^2}) \equiv 0 \pmod p.$$

Proof. From (3.1), we have

$$a_k(f_{pk}) = \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}\binom{u^j}{pk}. \tag{3.14}$$

But, $\binom{u^j}{pk}$ is the co-efficient of T^{pk} in the expansion of $(1+T)^{u^j}$. Here $j \le k < p$ and using (3.9), we find that

$$\binom{u^j}{pk} \equiv \binom{jt_1}{k} \pmod p. \tag{3.15}$$

From (3.14), (3.15) and Result 3.2.1, we find that

$$a_k(f_{pk}) \equiv \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}\binom{jt_1}{k}$$
$$\equiv t_1^k \pmod p. \tag{3.16}$$

Again,

$$a_p(f_{p^2}) = \sum_{j=0}^{p}(-1)^{p-j}\binom{p}{j}\binom{u^j}{p^2}$$
$$\equiv \binom{u^p}{p^2} \pmod p \tag{3.17}$$

and

$$a_{p+1}(f_{p^2}) = \sum_{j=0}^{p+1}(-1)^{p+1-j}\binom{p+1}{j}\binom{u^j}{p^2}$$
$$\equiv \binom{u^{p+1}}{p^2} - \binom{u^p}{p^2} - \binom{u}{p^2} \pmod p. \tag{3.18}$$

From (3.10) and (3.9), we find that

$$\binom{u}{p^2} \equiv t_2 \pmod p \tag{3.19}$$
$$\binom{u^p}{p^2} \equiv t_1 \pmod p \tag{3.20}$$
$$\binom{u^{p+1}}{p^2} \equiv t_1 + t_2 \pmod p \tag{3.21}$$

Using (3.17) - (3.21), we complete the proof of the lemma. □

Lemma 3.3.3. *Suppose that* $1 \le k < p$ *and* $p^2 + (k-1)p \le m < p^2 + kp$. *Then*

$$a_{p+k}(f_m) \equiv 0 \pmod p.$$

Proof. From (3.1), we have

$$a_{p+k}(f_m) = \sum_{j=0}^{p+k}(-1)^{p+k-j}\binom{p+k}{j}\binom{u^j}{m}. \tag{3.22}$$

But, $\binom{u^j}{m}$ is the co-efficient of T^m in the expansion of $(1+T)^{u^j}$. Clearly, if $p^2 + (k-1)p \le m < p^2 + kp$ and $m \ne p^2 + (k-1)p, p^2 + (k-1)p + 1$, then from (3.10) and (3.9) we find that the co-efficient of T^m in $(1+T)^{u^j}$ is

zero modulo p. Also, co-efficients of T^m modulo p in $(1+T)^{u^j}$ are equal for $m = p^2+(k-1)p, p^2+(k-1)p+1$. Thus, to prove that $a_{p+k}(f_m)$ is zero modulo p when $m = p^2+(k-1)p, p^2+(k-1)p+1$, we need to prove for $m = p^2+(k-1)p$ only. If $k = 1$, then

$$\begin{aligned} a_{p+1}(f_{p^2}) &\equiv -\binom{u}{p^2} - \binom{u^p}{p^2} + \binom{u^{p+1}}{p^2} \\ &\equiv -t_2 - t_1 + (t_1 + t_2) \equiv 0 \pmod{p}. \end{aligned} \tag{3.23}$$

Therefore, we assume that $k > 1$. From (3.10) and (3.9), we have

$$\begin{aligned} \binom{u^j}{m} &= \text{co-efficient of } T^m \text{ in the expansion of } (1+T)^{u^j} \\ &\equiv \binom{jt_1}{k-1} \left\{ \frac{j(j-1)}{2} t_1^2 + jt_2 \right\} \pmod{p} \ if \ j < p \end{aligned} \tag{3.24}$$

and

$$\binom{u^j}{m} \equiv \binom{it_1}{k-1} \left\{ t_1 + \frac{i(i-1)}{2} t_1^2 + it_2 \right\} \pmod{p} \ if \ j = p+i, 0 \le i < p. \tag{3.25}$$

Now,

$$a_{p+k}(f_m) = \sum_{j=0}^{p+k} (-1)^{p+k-j} \binom{p+k}{j} \binom{u^j}{m}$$

$$\begin{aligned} &\equiv \sum_{j=0}^{k} (-1)^{p+k-j} \binom{p+k}{j} \binom{jt_1}{k-1} \left\{ \frac{j(j-1)}{2} t_1^2 + jt_2 \right\} \\ &+ \sum_{j=p}^{p+k} (-1)^{p+k-j} \binom{p+k}{j} \binom{u^j}{m} \\ &\equiv -\sum_{j=0}^{k} (-1)^{k-j} \binom{p+k}{j} \binom{jt_1}{k-1} \left\{ \frac{j(j-1)}{2} t_1^2 + jt_2 \right\} \\ &+ \sum_{j=0}^{k} (-1)^{k-j} \binom{p+k}{k-j} \binom{jt_1}{k-1} \left\{ t_1 + \frac{j(j-1)}{2} t_1^2 + jt_2 \right\} \pmod{p}. \end{aligned} \tag{3.26}$$

Again, $\binom{p+k}{j} \equiv \binom{k}{j} \pmod{p}$ and hence (3.26) implies that

$$a_{p+k}(f_m) \equiv \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} \binom{jt_1}{k-1} t_1 \pmod{p}. \tag{3.27}$$

Using Lemma 3.2.2, we complete the proof of $a_{p+k}(f_m) \equiv 0 \pmod{p}$ when $m = p^2 + (k-1)p$ and this completes the proof of the lemma. □

Lemma 3.3.4. *Suppose that* $1 \leq k < p$. *Then*

$$a_{p+k}(f_{p^2+kp}) \equiv t_1^{k+1} \pmod{p} \text{ and } a_{p+k+1}(f_{p^2+kp}) \equiv 0 \pmod{p}.$$

Proof. Proceeding as Lemma 3.3.3, we find that

$$a_{p+k}(f_{p^2+kp}) \equiv t_1 \times \left\{ \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} \binom{jt_1}{k} \right\} \pmod{p}$$

$$\text{and} \quad a_{p+k+1}(f_{p^2+kp}) \equiv t_1 \times \left\{ \sum_{j=0}^{k+1} (-1)^{k+1-j} \binom{k+1}{j} \binom{jt_1}{k} \right\} \pmod{p}.$$

Using Result 3.2.1 and Lemma 3.2.2, we complete the proof of the lemma. □

Lemma 3.3.5. *Suppose that* $2p^2 - p \leq m < 2p^2$. *Then* $a_{2p}(f_m) \equiv 0 \pmod{p}$. *Also,*

$$a_{2p}(f_{2p^2}) \equiv t_1^2 \pmod{p}, \quad a_{2p+1}(f_{2p^2}) \equiv 0 \pmod{p}, \quad \text{and } a_{2p+2}(f_{2p^2}) \equiv 0 \pmod{p}.$$

Proof. Suppose that $2p^2 - p \leq m < 2p^2$. From (3.1), we have

$$\begin{aligned} a_{2p}(f_m) &= \sum_{j=0}^{2p} (-1)^{2p-j} \binom{2p}{j} \binom{u^j}{m} \\ &\equiv -\binom{2p}{p} \binom{u^p}{m} + \binom{u^{2p}}{m} \\ &\equiv \text{co-efficient of } T^m \text{ in } \left\{ -\binom{2p}{p} \times (1+T)^{u^p} + (1+T)^{u^{2p}} \right\} \\ &\equiv 0 \pmod{p}. \end{aligned} \tag{3.28}$$

We obtain (3.28) using the binomial expansion (3.10).

Again,

$$\begin{aligned} a_{2p}(f_{2p^2}) &\equiv -\binom{2p}{p}\binom{u^p}{2p^2} + \binom{u^{2p}}{2p^2} \\ &\equiv \text{co-efficient of } T^{2p^2} \text{ in } \left\{ -\binom{2p}{p} \times (1+T)^{u^p} + (1+T)^{u^{2p}} \right\} \\ &\equiv -2\binom{t_1}{2} + \binom{2t_1}{2} \\ &\equiv t_1^2 \pmod{p}. \end{aligned} \tag{3.29}$$

Also, modulo p

$$\begin{aligned} & a_{2p+1}(f_{2p^2}) \\ &\equiv \binom{u}{2p^2} + \binom{2p+1}{p}\left\{\binom{u^p}{2p^2} - \binom{u^{p+1}}{2p^2}\right\} - \binom{u^{2p}}{2p^2} + \binom{u^{2p+1}}{2p^2} \\ &\equiv \text{co-efficient of } T^{2p^2} \text{ in } (1+T)^u + \binom{2p+1}{p}\left\{(1+T)^{u^p} - (1+T)^{u^{p+1}}\right\} \\ &\qquad\qquad - (1+T)^{u^{2p}} + (1+T)^{u^{2p+1}} \\ &\equiv \binom{t_2}{2} + \binom{2p+1}{p}\left\{\binom{t_1}{2} - \binom{t_1+t_2}{2}\right\} - \binom{2t_1}{2} + \binom{2t_1+t_2}{2}. \end{aligned} \tag{3.30}$$

But, $\binom{2p+1}{p} \equiv 2 \pmod{p}$. Using this in (3.30), we find that

$$a_{2p+1}(f_{2p^2}) \equiv 0 (\text{mod } p). \tag{3.31}$$

Finally, we prove that $a_{2p+2}(f_{2p^2}) \equiv 0 \pmod{p}$.

Using $\binom{2p+2}{p} \equiv 2 \pmod{p}$ and $\binom{2p+2}{p+1} \equiv 4 \pmod{p}$, we find that

$$\begin{aligned} & a_{2p+2}(f_{2p^2}) \\ &\equiv -2\binom{u}{2p^2} + \binom{u^2}{2p^2} - 2\binom{u^p}{2p^2} + 4\binom{u^{p+1}}{2p^2} \\ &\qquad - 2\binom{u^{p+2}}{2p^2} + \binom{u^{2p}}{2p^2} - 2\binom{u^{2p+1}}{2p^2} + \binom{u^{2p+2}}{2p^2} \end{aligned}$$

$$\begin{aligned}
&\equiv \text{co-efficient of } T^{2p^2} \text{ in } -2(1+T)^u + (1+T)^{u^2} - 2(1+T)^{u^p} + 4(1+T)^{u^{p+1}} \\
&\quad - 2(1+T)^{u^{p+2}} + (1+T)^{u^{2p}} - 2(1+T)^{u^{2p+1}} + (1+T)^{u^{2p+2}} \\
&\equiv -2\binom{t_2}{2} + \binom{t_1^2+2t_2}{2} - 2\binom{t_1}{2} + 4\binom{t_1+t_2}{2} - 2\binom{t_1^2+t_1+2t_2}{2} \\
&\qquad + \binom{2t_1}{2} - 2\binom{2t_1+t_2}{2} + \binom{t_1^2+2t_1+2t_2}{2} \\
&\equiv 0 (\text{mod } p). \qquad (3.32)
\end{aligned}$$

This completes the proof of the lemma. □

3.3.2 Mahler coefficients $a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n})$

Using the p-adic properties of the Mahler coefficients $a_j(f_m)$ and (3.4), one can derive p-adic properties of the Mahler coefficients $a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n})$. We now prove certain p-adic properties of these Mahler coefficients in the following lemmas.

Lemma 3.3.6. *Suppose that $1 \leq k < p$ and $p^2 + (k-1)p \leq m < p^2 + kp$. Let $m_1 + \cdots + m_n$ be a partition of m such that $k_1 + \cdots + k_n = p + k$, where $k_i = \text{ord}_p(m_i!), i = 1, \cdots, n$. Then we have*

$$a_{k_1,\cdots,k_n}(f_{m_1,\cdots,m_n}) \equiv 0 \ (\text{mod } p).$$

Proof. Clearly, $k_i = \text{ord}_p(m_i!) \neq p$ for all i, because $\text{ord}_p((p^2-p)!) = p-1$ and $\text{ord}_p(p^2!) = p+1$. Hence we have the following two cases only.

Case 1: Suppose that $k_i > p$ for some i. Then $k_i = p + l_i, 0 < l_i \leq k$ and hence $p^2 + (l_i - 1)p \leq m_i < p^2 + l_i p$. By Lemma 3.3.3, we get

$$a_{k_i}(f_{m_i}) \equiv 0 \ (\text{mod } p). \qquad (3.33)$$

Case 2: Suppose that $k_i < p$ for some i. Then $pk_i \leq m_i < p(k_i+1)$. We know that

$$a_{k_i}(f_{m_i}) = \sum_{j=0}^{k_i} (-1)^{k_i-j} \binom{k_i}{j} \binom{u^j}{m_i}. \tag{3.34}$$

But, $\binom{u^j}{m_i}$ is the coefficient of T^{m_i} in the expansion of $(1+T)^{u^j}$. From (3.9), we find that $\binom{u^j}{m_i}$ is congruent to zero modulo p if $m_i \neq pk_i, pk_i+1$. This implies that

$$a_{k_i}(f_{m_i}) \equiv 0 \pmod{p} \text{ if } m_i \neq pk_i, pk_i+1. \tag{3.35}$$

Thus, for any partition $m_1+\cdots+m_n$ of m, where $k_i = ord_p(m_i!)$ are as given in the lemma, (3.33) and (3.35) imply that $a_{k_1,\cdots,k_n}(f_{m_1,\cdots,m_n}) \equiv 0 \pmod{p}$ unless $m_i = pk_i$ or $m_i = pk_i+1$. With out loss of generality, suppose that $m_i = pk_i$ for $i = 1,\cdots,l$ and $m_i = pk_i+1$ for $i = l+1,\cdots,n$. Then $m = m_1+\cdots+m_n = p(p+k)+(n-l)$, which is a contradiction to the fact that $m < p^2+kp$. This completes the proof of the lemma. □

Lemma 3.3.7. *Suppose that* $2p^2 - p \leq m < 2p^2$. *Let* $m_1+\cdots+m_n$ *be a partition of* m *such that* $k_1+\cdots+k_n = 2p$, *where* $k_i = \mathrm{ord}_p(m_i!), i = 1,\cdots,n$. *Then we have*

$$a_{k_1,\cdots,k_n}(f_{m_1,\cdots,m_n}) \equiv 0 \pmod{p}.$$

Proof. Suppose that $k_i = 2p$ for some i. Then $2p^2 - p \leq m_i < 2p^2$ and hence from the Lemma 3.3.5, we get

$$a_{k_i}(f_{m_i}) \equiv 0 \pmod{p} \tag{3.36}$$

This implies that $a_{k_1,\cdots,k_n}(f_{m_1,\cdots,m_n}) \equiv 0 \pmod{p}$. The other two cases are $p < k_i < 2p$ and $k_i < p$ as $k_i \neq p$. As shown in the proof of the Lemma 3.3.6,

$$a_{k_1,\cdots,k_n}(f_{m_1,\cdots,m_n}) \equiv 0 \pmod{p} \text{ unless } m_i = pk_i \text{ or } m_i = pk_i+1. \tag{3.37}$$

With out loss of generality, suppose that $m_i = pk_i$ for $i = 1, \cdots, l$ and $m_i = pk_i + 1$ for $i = l+1, \cdots, n$. Then $m = m_1 + \cdots + m_n = 2p^2 + (n-l)$, which is a contradiction to the fact that $m < 2p^2$. This completes the proof of the lemma. □

Chapter 4

Iwasawa Invariants of p-Adic Measures and Γ-Transforms

In this chapter we give a generalization of an existing result of Satoh, Kida and Childress which deals with p-adic measures on $\mathbb{Z}_p$ to p-adic measures on $\mathbb{Z}_p^n$ for any n. We determine a relation between the λ-invariants of a p-adic measure on $\mathbb{Z}_p^n$ and its Γ-transform. We prove this result using the p-adic properties of Mahler coefficients discussed in Chapter 3.

4.1 Introduction

Fix an odd prime p. Let $\mathcal{O}$ be the ring of integers in a finite extension of $\mathbb{Q}_p$ with a local parameter π. We write $\mathbb{Z}_p^\times = V \times U$ where V is the group of $(p-1)$st roots of unity in $\mathbb{Z}_p$ and $U = 1 + p\mathbb{Z}_p$. Let u be a topological generator of U. The projections from $\mathbb{Z}_p^\times$ onto V and U are denoted by ω and $<>$ respectively. We have an isomorphism $\phi : \mathbb{Z}_p \to U$ given by $\phi(y) = u^y$.

In chapter 1, we defined p-adic measures on $\mathbb{Z}_p$ and convolution of two such measures. One can easily extend those definitions to define p-adic measures on

$\mathbb{Z}_p^n$ and their convolution for any $n \geq 1$. Let $\Lambda_{(n)}$ denote the $\mathcal{O}$-valued measures on $\mathbb{Z}_p^n$. It is well-known, (see e.g. [14]), that $\Lambda_{(1)}$ is a ring under convolution, and is isomorphic to the formal power series ring $\mathcal{O}[[T-1]]$. Explicitly, for $x \in \mathbb{Z}_p$, let

$$T^x = \sum_{n=0}^{\infty} \binom{x}{n} (T-1)^n \in \mathcal{O}[[T-1]].$$

The power series associated to a measure $\alpha \in \Lambda_{(1)}$ is then defined by

$$\widehat{\alpha}(T) = \int_{\mathbb{Z}_p} T^x d\alpha(x) = \sum_{n=0}^{\infty} b_n(\alpha)(T-1)^n$$

where

$$b_n(\alpha) = \int_{\mathbb{Z}_p} \binom{x}{n} d\alpha(x).$$

The natural generalizations of the above results to larger values of n are true. $\mathcal{O}$-valued measures on $\mathbb{Z}_p^n$ correspond to power series in $\mathcal{O}[[T_1-1, \cdots, T_n-1]]$. This correspondence is given by

$$\begin{aligned}\widehat{\alpha}(T_1, \cdots, T_n) &= \int_{\mathbb{Z}_p^n} T_1^{x_1} \cdots T_n^{x_n} d\alpha(x_1, \cdots, x_n) \\ &= \sum_{m_1=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} \left(\int_{\mathbb{Z}_p^n} \binom{x_1}{m_1} \cdots \binom{x_n}{m_n} d\alpha(x_1, \cdots, x_n) \right) \\ &\qquad \times (T_1-1)^{m_1} \cdots (T_n-1)^{m_n}. \end{aligned} \tag{4.1}$$

Similar to the case $n=1$, we have the following integration formulas:

$$\begin{aligned}&\int_{\mathbb{Z}_p^n} x_1^{m_1} \cdots x_n^{m_n} d\alpha(x_1, \cdots, x_n) \\ &= \left(T_1 \frac{d}{dT_1}\right)^{m_1} \cdots \left(T_n \frac{d}{dT_n}\right)^{m_n} \widehat{\alpha}(T_1, \cdots, T_n)|_{T_1=\cdots=T_n=1} \end{aligned} \tag{4.2}$$

Let α be a $\mathcal{O}$-valued measure on $\mathbb{Z}_p^n$. For $(a_1, \cdots, a_n) \in (\mathbb{Z}_p^\times)^n$, denote by $\alpha \circ (a_1, \cdots, a_n)$ the measure on $\mathbb{Z}_p^n$ given by

$$\alpha \circ (a_1, \cdots, a_n)(A_1 \times \cdots \times A_n) = \alpha(a_1 A_1, \cdots, a_n A_n),$$

where A_i are compact open subsets of $\mathbb{Z}_p$. Also, if $A = (A_1, \cdots, A_n) \subseteq \mathbb{Z}_p^n$, where all A_i are compact open subsets of $\mathbb{Z}_p$, $\alpha|_A$ denotes the measure obtained by restricting α to A and extending by 0.

The Γ-transform of a measure $\alpha \in \Lambda_{(n)}$ is defined as a function of the p-adic variables $s_1, \cdots, s_n$ given by

$$\Gamma_\alpha(s_1, \cdots, s_n) = \int_{(\mathbb{Z}_p^\times)^n} < x_1 >^{s_1} \cdots < x_n >^{s_n} d\alpha(x_1, \cdots, x_n).$$

If we put $d\alpha(a_1x_1, \cdots, a_nx_n)$ for $d(\alpha \circ (a_1, \cdots, a_n))(x_1, \cdots, x_n)$, splitting up the integral, we can also write

$$\begin{aligned}
&\Gamma_\alpha(s_1, \cdots, s_n) \\
&= \sum_{\eta_1 \in V} \cdots \sum_{\eta_n \in V} \int_{U^n} < \eta_1 x_1 >^{s_1} \cdots < \eta_n x_n >^{s_n} d\alpha(\eta_1 x_1, \cdots, \eta_n x_n) \\
&= \int_{U^n} x_1^{s_1} \cdots x_n^{s_n} d\beta(x_1, \cdots, x_n),
\end{aligned}$$

where

$$\beta = \sum_{\eta_1 \in V} \cdots \sum_{\eta_n \in V} (\alpha \circ (\eta_1, \cdots, \eta_n))|_{U^n},$$

a measure on U^n.

Now the measure β may be viewed as a measure on $\mathbb{Z}_p^n$ via the isomorphism ϕ:

$$\tilde{\beta}(A_1, \cdots, A_n) = \beta(\phi(A_1), \cdots, \phi(A_n)).$$

Let us write $d\beta(u^{y_1}, \cdots, u^{y_n})$ for $d\tilde{\beta}(y_1, \cdots, y_n)$. Let $G(T_1, \cdots, T_n)$ be the power series associated to $\tilde{\beta}$, that is,

$$G(T_1, \cdots, T_n) = \int_{\mathbb{Z}_p^n} T_1^{y_1} \cdots T_n^{y_n} d\beta(u^{y_1}, \cdots, u^{y_n}).$$

Then $\Gamma_\alpha(s_1, \cdots, s_n) = G(u^{s_1}, \cdots, u^{s_n})$.

For a more thorough treatment of p-adic measure theory, see [12, 22].

4.2 Iwasawa λ-invariants and Γ-transforms

The Iwasawa μ- and λ- invariants of a power series

$$F(T) = \sum_{n=0}^{\infty} a_n (T-1)^n \in \mathcal{O}[[T-1]]$$

are defined by

$$\mu(F(T)) = \min\{ord(a_n) : n \geq 0\}$$
$$\lambda(F(T)) = \min\{n : ord(a_n) = \mu(F(T))\}.$$

Analogously, we define the Iwasawa μ- and λ- invariants of a power series

$$F(T_1, \cdots, T_n) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} a_{m_1,\cdots,m_n} (T_1-1)^{m_1} \cdots (T_n-1)^{m_n}$$
$$\in \mathcal{O}[[T_1-1, \cdots, T_n-1]]$$

as follows:

$$\mu(F(T_1, \cdots, T_n)) = \min\{ord(a_{m_1,\cdots,m_n}) : m_i \geq 0 \quad \forall i\}$$
$$\lambda(F(T_1, \cdots, T_n)) = \min\{m_1 + \cdots + m_n : ord(a_{m_1,\cdots,m_n}) = \mu(F(T_1, \cdots, T_n))\}.$$

For a measure $\alpha \in \Lambda_{(n)}$, we understand $\mu(\alpha)$ and $\lambda(\alpha)$ to mean $\mu(\widehat{\alpha}(T_1, \cdots, T_n))$ and $\lambda(\widehat{\alpha}(T_1, \cdots, T_n))$.

Let $\alpha \in \Lambda_{(n)}$. That is, α is a $\mathcal{O}$-valued measure on $\mathbb{Z}_p^n$. Let u be a fixed topological generator of $U = 1 + p\mathbb{Z}_p$, and let $G(T_1, \cdots, T_n)$ satisfy $G(u^{s_1}, \cdots, u^{s_n}) = \Gamma_\alpha(s_1, \cdots, s_n)$, so that

$$G(T_1, \cdots, T_n) = \int_{\mathbb{Z}_p} T_1^{y_1} \cdots T_n^{y_n} d\beta(u^{y_1}, \cdots, u^{y_n}),$$
$$\text{where } \beta = \sum_{\eta_1 \in V} \cdots \sum_{\eta_n \in V} (\alpha \circ (\eta_1, \cdots, \eta_n))|_{U^n}. \tag{4.3}$$

Note that β is a measure on U^n. We extend β to $\mathbb{Z}_p^n$ by 0 and then we get a power series

$$\widehat{\beta}(T_1, \cdots, T_n) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} b_{m_1,\cdots,m_n}(T_1-1)^{m_1} \cdots (T_n-1)^{m_n}. \tag{4.4}$$

Suppose that

$$G(T_1, \cdots, T_n) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} g_{m_1,\cdots,m_n}(T_1-1)^{m_1} \cdots (T_n-1)^{m_n}. \tag{4.5}$$

In case of $n = 1$, Sinnott proved that $\mu(G(T)) = \mu(\alpha^* + \alpha^* \circ (-1))$, if $\widehat{\alpha}(T)$ is a rational function of T (see [24, p.p. 276, Theorem 1]). Here $\alpha^* = \alpha|_{\mathbb{Z}_p^\times}$. It was Kida who first obtained a relation between the λ-invariant of a measure on $\mathbb{Z}_p$ and its Γ-transform with a fixed topological generator [25]. Later, in case of $n = 1$, Childress proved that $\mu(G(T)) = \mu(\beta)$ and $\lambda(\beta) = p\lambda(G(T))$ if $\lambda(G(T)) \leq p$ (see [14, Lemma 1 & Theorem 1]). Satoh obtained the same result without any condition on $\lambda(G(T))$, but his approach was based on certain properties of Stirling numbers [10]. In this chapter, we prove the following main result which gives a relation between $\lambda(G(T_1, \cdots, T_n))$ and $\lambda(\beta)$ for any n.

Theorem 4.2.1. *If* $\lambda(G(T_1, \cdots, T_n)) \leq 2p$, *then* $\lambda(\beta) = p\lambda(G(T_1, \cdots, T_n))$.

We prove this theorem following the approach discussed in Chapter 3 and Childress [14]. We really do not know whether the method of Satoh based on certain properties of Stirling numbers can be generalized to prove Theorem 4.2.1. We now prove a lemma which is a generalization of Lemma 1 proved by Childress in [14]. As before, suppose

$$\widehat{\beta}(T_1, \cdots, T_n) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} b_{m_1,\cdots,m_n}(T_1-1)^{m_1} \cdots (T_n-1)^{m_n}$$

and

$$G(T_1, \cdots, T_n) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} g_{m_1,\cdots,m_n}(T_1-1)^{m_1} \cdots (T_n-1)^{m_n}.$$

Recall that the functions $f_m : \mathbb{Z}_p \to \mathbb{Z}_p$ and $f_{m_1,\cdots,m_n} : \mathbb{Z}_p^n \to \mathbb{Z}_p$ are defined by

$$f_m(x) = \binom{u^x}{m} \quad \text{and} \quad f_{m_1,\cdots,m_n}(x_1,\cdots,x_n) = f_{m_1}(x_1)\cdots f_{m_n}(x_n), \quad \text{respectively.}$$

Also, if $a_j(f_m)$ and $a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n})$ are the Mahler coefficients of f_m and $f_{m_1,\cdots,m_n}$ respectively, then (3.4) implies that

$$a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n}) = a_{j_1}(f_{m_1})\cdots a_{j_n}(f_{m_n}). \tag{4.6}$$

Lemma 4.2.1. *Let α be a measure on $\mathbb{Z}_p^n$. Then $\mu(G(T_1,\cdots,T_n)) = \mu(\beta)$.*

Proof. Let $\mu(G(T_1,\cdots,T_n)) = \nu$. Then

$$g_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi^\nu} \quad \text{for every} \quad m_i \geq 0, i = 1,\cdots,n. \tag{4.7}$$

Now,

$$\begin{aligned} b_{m_1,\cdots,m_n} &= \int_{U^n} \binom{x_1}{m_1}\cdots\binom{x_n}{m_n} d\beta(x_1,\cdots,x_n) \\ &= \int_{\mathbb{Z}_p^n} \binom{u^{x_1}}{m_1}\cdots\binom{u^{x_n}}{m_n} d\beta(u^{x_1},\cdots,u^{x_n}). \end{aligned} \tag{4.8}$$

If $a_j(f_m)$ and $a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n})$ denote the Mahler coefficients of f_m and $f_{m_1,\cdots,m_n}$, then $a_j(f_m)$, $a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n}) \in \mathbb{Z}_p$. From (4.6), we have

$$a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n}) = a_{j_1}(f_{m_1})\cdots a_{j_n}(f_{m_n}). \tag{4.9}$$

Using (4.8) and (4.9), we find that

$$\begin{aligned} b_{m_1,\cdots,m_n} &= \int_{\mathbb{Z}_p^n} \binom{u^{x_1}}{m_1}\cdots\binom{u^{x_n}}{m_n} d\beta(u^{x_1},\cdots,u^{x_n}) \\ &= \sum_{j_1=0}^{\infty}\cdots\sum_{j_n=0}^{\infty} a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n}) \int_{\mathbb{Z}_p^n} \binom{x_1}{j_1}\cdots\binom{x_n}{j_n} d\beta(u^{x_1},\cdots,u^{x_n}) \\ &= \sum_{j_1=0}^{\infty}\cdots\sum_{j_n=0}^{\infty} a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n}) g_{j_1,\cdots,j_n} \end{aligned} \tag{4.10}$$

From (4.7) and (4.10), we get $b_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi^\nu}$ for every $m_i \geq 0$. This implies that $\mu(\beta) \geq \nu$.

Similarly, let $\mu(\beta) = \tau$. Then

$$b_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi^\tau} \text{ for every } m_i \geq 0, i = 1, \cdots, n. \tag{4.11}$$

Now,

$$\begin{aligned} g_{m_1,\cdots,m_n} &= \int_{\mathbb{Z}_p^n} \binom{x_1}{m_1} \cdots \binom{x_n}{m_n} d\beta(u^{x_1}, \cdots, u^{x_n}) \\ &= \int_{U^n} \binom{\log_u^{y_1}}{m_1} \cdots \binom{\log_u^{y_n}}{m_n} d\beta(y_1, \cdots, y_n), \end{aligned} \tag{4.12}$$

where

$$\log_u^{y_i} = \frac{\log y_i}{\log u}.$$

Let

$$h_{m_1,\cdots,m_n}(y_1, \cdots, y_n) = \binom{\log_u^{y_1}}{m_1} \cdots \binom{\log_u^{y_n}}{m_n}.$$

Then (4.11) and (4.12) imply that

$$\begin{aligned} g_{m_1,\cdots,m_n} &= \int_{U^n} \binom{\log_u^{y_1}}{m_1} \cdots \binom{\log_u^{y_n}}{m_n} d\beta(y_1, \cdots, y_n) \\ &= \int_{U^n} h_{m_1,\cdots,m_n}(y_1, \cdots, y_n) d\beta(y_1, \cdots, y_n) \\ &= \sum_{j_1=0}^{\infty} \cdots \sum_{j_n=0}^{\infty} a_{j_1,\cdots,j_n}(h_{m_1,\cdots,m_n}) b_{j_1,\cdots,j_n} \\ &\equiv 0 \pmod{\pi^\tau} \text{ for every } m_i \geq 0. \end{aligned}$$

Hence, $\mu(G(T_1, \cdots, T_n)) \geq \tau$. This completes the proof of the lemma. □

Let α be a $\mathcal{O}$ valued measure on $\mathbb{Z}_p$. Say $\widehat{\beta} = \sum_{n=0}^{\infty} b_n (T-1)^n$ and $G(T) = \sum_{n=0}^{\infty} g_n (T-1)^n$. The following result is due to Childress.

Result 4.2.1. *([14, p.p. 364, Lemma 2]) Let n be a positive integer. We have*

$$m!b_m \equiv m! \sum_{r=0}^{n} g_r a_r(f_m) \pmod{p^{n+1}\mathcal{O}}.$$

The following lemma is an easy generalization of the above result. Let $\alpha \in \Lambda_{(n)}$. That is, α is a $\mathcal{O}$-valued measure on $\mathbb{Z}_p^n$. Let u be a fixed topological generator of $U = 1 + p\mathbb{Z}_p$, and let $G(T_1, \cdots, T_n)$ satisfy $G(u^{s_1}, \cdots, u^{s_n}) = \Gamma_\alpha(s_1, \cdots, s_n)$, so that

$$G(T_1, \cdots, T_n) = \int_{\mathbb{Z}_p} T_1^{y_1} \cdots T_n^{y_n} d\beta(u^{y_1}, \cdots, u^{y_n}),$$
$$\text{where } \beta = \sum_{\eta_1 \in V} \cdots \sum_{\eta_n \in V} (\alpha \circ (\eta_1, \cdots, \eta_n))|_{U^n}. \tag{4.13}$$

Note that β is a measure on U^n. We extend β to $\mathbb{Z}_p^n$ by 0 and then we get a power series

$$\widehat{\beta}(T_1, \cdots, T_n) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} b_{m_1,\cdots,m_n} (T_1 - 1)^{m_1} \cdots (T_n - 1)^{m_n}. \tag{4.14}$$

Also, the Γ-transform of a measure $\alpha \in \Lambda_{(n)}$ is defined as a function of the p-adic variables $s_1, \cdots, s_n$ given by

$$\Gamma_\alpha(s_1, \cdots, s_n) = \int_{(\mathbb{Z}_p^\times)^n} < x_1 >^{s_1} \cdots < x_n >^{s_n} d\alpha(x_1, \cdots, x_n).$$

If we put $d\alpha(a_1 x_1, \cdots, a_n x_n)$ for $d(\alpha \circ (a_1, \cdots, a_n))(x_1, \cdots, x_n)$, splitting up the integral, we can also write

$$\begin{aligned}
&\Gamma_\alpha(s_1, \cdots, s_n) \\
&= \sum_{\eta_1 \in V} \cdots \sum_{\eta_n \in V} \int_{U^n} < \eta_1 x_1 >^{s_1} \cdots < \eta_n x_n >^{s_n} d\alpha(\eta_1 x_1, \cdots, \eta_n x_n) \\
&= \int_{U^n} x_1^{s_1} \cdots x_n^{s_n} d\beta(x_1, \cdots, x_n),
\end{aligned} \tag{4.15}$$

where

$$\beta = \sum_{\eta_1 \in V} \cdots \sum_{\eta_n \in V} (\alpha \circ (\eta_1, \cdots, \eta_n))|_{U^n},$$

a measure on U^n.

Now the measure β may be viewed as a measure on $\mathbb{Z}_p^n$ via the isomorphism ϕ:

$$\tilde{\beta}(A_1, \cdots, A_n) = \beta(\phi(A_1), \cdots, \phi(A_n)).$$

If $G(T_1, \cdots, T_n)$ is the power series associated with the measure $\tilde{\beta}$, then

$$\Gamma_\alpha(s_1, \cdots, s_n) = G(u^{s_1}, \cdots, u^{s_n}).$$

Suppose that

$$G(T_1, \cdots, T_n) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} g_{m_1,\cdots,m_n} (T_1 - 1)^{m_1} \cdots (T_n - 1)^{m_n}. \tag{4.16}$$

Let

$$\begin{aligned} S_{m_1,\cdots,m_n}(x_1, \cdots, x_n) &= m_1! \cdots m_n! \binom{x_1}{m_1} \cdots \binom{x_n}{m_n} \\ &= \sum_{i_1=1}^{m_1} \cdots \sum_{i_n=1}^{m_n} c_{i_1,\cdots,i_n} x_1^{i_1} \cdots x_n^{i_n}. \end{aligned} \tag{4.17}$$

Note that $c_{i_1,\cdots,i_n} \in \mathbb{Z}$.

Lemma 4.2.2. *Modulo $p^{n+k_1+\cdots+k_n}\mathcal{O}$, we have*

$$m_1! \cdots m_n! b_{m_1,\cdots,m_n} \equiv m_1! \cdots m_n! \sum_{j_1=0}^{k_1} \cdots \sum_{j_n=0}^{k_n} g_{j_1,\cdots,j_n} a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n}), \tag{4.18}$$

where $a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n})$ are the Mahler coefficients of $f_{m_1,\cdots,m_n}(x_1, \cdots, x_n)$.

Proof. By (4.1), we have

$$\begin{aligned} m_1! \cdots m_n! b_{m_1,\cdots,m_n} &= \int_{U^n} S_{m_1,\cdots,m_n}(x_1, \cdots, x_m) d\beta(x_1, \cdots, x_n) \\ &= \sum_{i_1=1}^{m_1} \cdots \sum_{i_n=1}^{m_n} c_{i_1,\cdots,i_n} \int_{U^n} x_1^{i_1} \cdots x_n^{i_n} d\beta(x_1, \cdots, x_n), \end{aligned}$$

which, by (4.13) and (4.15), is equal to

$$\begin{aligned}
&\sum_{i_1}^{m_1}\cdots\sum_{i_n}^{m_n} c_{i_1,\cdots,i_n}\Gamma_\alpha(i_1,\cdots,i_n)\\
&=\sum_{i_1}^{m_1}\cdots\sum_{i_n}^{m_n} c_{i_1,\cdots,i_n}G(u^{i_1},\cdots,u^{i_n})\\
&=\sum_{i_1}^{m_1}\cdots\sum_{i_n}^{m_n} c_{i_1,\cdots,i_n}\sum_{r_1=0}^{\infty}\cdots\sum_{r_n=0}^{\infty} g_{r_1,\cdots,r_n}(u^{i_1}-1)^{r_1}\cdots(u^{i_n}-1)^{r_n}. \qquad (4.19)
\end{aligned}$$

But, $p^{k+1}|(u^i-1)^r$ for $r>k$ and $i\geq 1$.

Therefore, modulo $p^{n+k_1+\cdots+k_n}\mathcal{O}$, we have

$$\begin{aligned}
&m_1!\cdots m_n!b_{m_1,\cdots,m_n}\\
&\equiv\sum_{i_1}^{m_1}\cdots\sum_{i_n}^{m_n} c_{i_1,\cdots,i_n}\sum_{r_1=0}^{k_1}\cdots\sum_{r_n=0}^{k_n} g_{r_1,\cdots,r_n}(u^{i_1}-1)^{r_1}\cdots(u^{i_n}-1)^{r_n}. \qquad (4.20)
\end{aligned}$$

Expanding the terms $(u^{i_j}-1)^{r_j}, j=1,\cdots,n$, we find that modulo $p^{n+k_1+\cdots+k_n}\mathcal{O}$,

$$\begin{aligned}
&m_1!\cdots m_n!b_{m_1,\cdots,m_n}\\
&\equiv\sum_{r_1=0}^{k_1}\cdots\sum_{r_n=0}^{k_n} g_{r_1,\cdots,r_n}\sum_{j_1=0}^{r_1}\cdots\sum_{j_n}^{r_n}(-1)^{r_1+\cdots+r_n-j_1-\cdots-j_n}\binom{r_1}{j_1}\binom{u^{j_1}}{m_1}\cdots\binom{r_n}{j_n}\binom{u^{j_n}}{m_n}\\
&\equiv m_1!\cdots m_n!\sum_{r_1=0}^{k_1}\cdots\sum_{r_n=0}^{k_n} g_{r_1,\cdots,r_n}a_{r_1,\cdots,r_n}(f_{m_1,\cdots,m_n}). \qquad (4.21)
\end{aligned}$$

This completes the proof of the lemma. □

From the above lemma, we have the following result.

Corollary 4.2.1. *If* $ord_p(m_1!\cdots m_n!)\leq k_1+\cdots+k_n$, *then*

$$b_{m_1,\cdots,m_n}\equiv\sum_{j_1=0}^{k_1}\cdots\sum_{j_n=0}^{k_n} g_{j_1,\cdots,j_n}a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n})\pmod{p^n\mathcal{O}}. \qquad (4.22)$$

4.3 Proof of the main result

We now give a prove of the Theorem 4.2.1. In the proof, we use certain p-adic properties of the Mahler coefficients $a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n})$ discussed in Chapter 3.

We may assume that $\mu(G(T_1,\cdots,T_n)) = 0$, because $\mu(G(T_1,\cdots,T_n)) = \mu(\beta)$ by Lemma 4.2.1, and for any power series $F(T_1,\cdots,T_n) \in \mathcal{O}[[T_1-1,\cdots,T_n-1]]$, if $\pi|F(T_1,\cdots,T_n)$ then $\lambda(\pi^{-1}F(T_1,\cdots,T_n)) = \lambda(F(T_1,\cdots,T_n))$.

Case 1: Suppose that $\lambda(G(T_1,\cdots,T_n)) = k < p$. Then there exists a partition $k_1+\cdots+k_n$ of k such that $g_{k_1,\cdots,k_n}$ is a unit in $\mathcal{O}$ and for every $m_i \geq 0$ satisfying $m_1+\cdots+m_n < k$, $g_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi}$. If $r < pk$, then for any partition $r_1+\cdots+r_n$ of r, we find that $\mathrm{ord}_p(r_1!\cdots r_n!) = \mathrm{ord}_p(r_1!)+\cdots+\mathrm{ord}_p(r_n!) \leq k-1$. If $l_i = \mathrm{ord}_p(r_i!)$, then from (4.22) we get

$$b_{r_1,\cdots,r_n} \equiv \sum_{j_1=0}^{l_1}\cdots\sum_{j_n=0}^{l_n} g_{j_1,\cdots,j_n}a_{j_1,\cdots,j_n}(f_{r_1,\cdots,r_n}) \equiv 0 \pmod{\pi}. \tag{4.23}$$

Now consider the partition $k_1+\cdots+k_n$ of k. Then $pk_1+\cdots+pk_n$ is a partition of pk such that $\mathrm{ord}_p(pk_i) = k_i$. From (4.22), (4.6) and Lemma 3.3.2, we get

$$\begin{aligned} b_{pk_1,\cdots,pk_n} &\equiv \sum_{j_1=0}^{k_1}\cdots\sum_{j_n=0}^{k_n} g_{j_1,\cdots,j_n}a_{j_1,\cdots,j_n}(f_{pk_1,\cdots,pk_n}) \\ &\equiv g_{k_1,\cdots,k_n}a_{k_1,\cdots,k_n}(f_{pk_1,\cdots,pk_n}) \equiv g_{k_1,\cdots,k_n}t_1^k \pmod{\pi}, \end{aligned} \tag{4.24}$$

which is a unit in $\mathcal{O}$. This proves that

$$\lambda(\beta) = pk_1+\cdots+pk_n = pk = p\lambda(G(T_1,\cdots,T_n)).$$

Case 2: Suppose that $\lambda(G(T_1,\cdots,T_n)) = p$. Then there exists a partition $k_1+\cdots+k_n$ of p such that $g_{k_1,\cdots,k_n}$ is a unit in $\mathcal{O}$ and for every $m_i \geq 0$ satisfying $m_1+\cdots+m_n < p$, $g_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi}$. Let $m < p^2$. Then for every partition $m_1+\cdots+m_n$ of m, we get $l_1+\cdots+l_n \leq p-1$, where $l_i = \mathrm{ord}_p(m_i!)$. As

shown in the previous case, this implies that $b_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi}$. Let us now consider the partition $pk_1 + \cdots + pk_n$ of p^2. If $k_i = p$ for some i, then $k_j = 0$ for all $j \neq i$. Hence, from (4.22) and Lemma 3.3.2, we get

$$\begin{aligned} b_{0,\cdots,0,p^2,0,\cdots,0} &\equiv g_{0,\cdots,0,p,0,\cdots,0} a_p(f_{p^2}) + g_{0,\cdots,0,p+1,0,\cdots,0} a_{p+1}(f_{p^2}) \\ &\equiv g_{0,\cdots,0,p,0,\cdots,0} t_1 \pmod{\pi}, \end{aligned} \tag{4.25}$$

which is a unit in $\mathcal{O}$. If all $k_i < p$, then using (4.24), we obtain

$$b_{pk_1,\cdots,pk_n} \equiv g_{k_1,\cdots,k_n} t_1^p \pmod{\pi}, \tag{4.26}$$

which is a unit in $\mathcal{O}$. This proves that

$$\lambda(\beta) = pk_1 + \cdots + pk_n = p^2 = p\lambda(G(T_1, \cdots, T_n)).$$

Case 3: Suppose that $p < \lambda(G(T_1, \cdots, T_n)) < 2p$. Let $\lambda(G(T_1, \cdots, T_n)) = p + k$, where $1 \leq k < p$. Then there exists a partition $k_1 + \cdots + k_n$ of $p + k$ such that $g_{k_1,\cdots,k_n}$ is a unit in $\mathcal{O}$ and for every $m_i \geq 0$ satisfying $m_1 + \cdots + m_n < p + k$, $g_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi}$. Let $m < p^2 + (k-1)p$. Then $\mathrm{ord}_p(m!) < p + k$ and hence for any partition $m_1 + \cdots + m_n$ of m, we have $l_1 + \cdots + l_n < p + k$, where $l_i = \mathrm{ord}_p(m_i!)$. As shown in the case 1, this implies that $b_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi}$. If $p^2 + (k-1)p \leq m < p^2 + kp$, then $\mathrm{ord}_p(m!) = p + k$. Therefore, for every partition $m_1 + \cdots + m_n$ of m, we get $l_1 + \cdots + l_n \leq p + k$, where $l_i = \mathrm{ord}_p(m_i!)$. If $l_1 + \cdots + l_n < p + k$, then we have already proved that $b_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi}$. Again if $l_1 + \cdots + l_n = p + k$, then

$$b_{m_1,\cdots,m_n} \equiv g_{l_1,\cdots,l_n} a_{l_1,\cdots,l_n}(f_{m_1,\cdots,m_n}) \pmod{\pi}. \tag{4.27}$$

Using Lemma 3.3.6, we find that $b_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi}$. Let us now consider the partition $k_1 + \cdots + k_n$ of $p + k$. Then $pk_1 + \cdots + pk_n$ is a partition of

$p^2 + pk$. If $k_i < p$, then $\mathrm{ord}_p(pk_i!) = k_i$. Also, $k_i = p$ implies $\mathrm{ord}_p((pk_i)!) = p + 1 = k_i + 1$. If $k_i > p$, then $k_i = p + l_i$, where $1 \leq l_i \leq k$ and hence $\mathrm{ord}_p(pk_i) = \mathrm{ord}_p((p^2 + pl_i)!) = p + l_i + 1 = k_i + 1$. From Lemma 3.3.2 and Lemma 3.3.3, we have

$$a_{p+1}(f_{p^2}) \equiv 0 \pmod{p} \quad \text{and} \quad a_{p+l_i+1}(f_{p^2+l_ip}) \equiv 0 \pmod{p}.$$

Again, if $k_i < p$, then from Lemma 3.3.2, we get $a_{k_i}(f_{pk_i}) \equiv {t_1}^{k_i} \pmod{p}$. Also, $a_p(f_{p^2}) \equiv t_1 \pmod{p}$ and if $1 \leq l_i < p$, then $a_{p+l_i}(f_{p^2+l_ip}) \equiv t_1^{l_i+1} \pmod{p}$. This implies that, if $h_i = \mathrm{ord}_p(pk_i!)$ for $i = 1, \cdots, n$, then

$$\begin{aligned} b_{pk_1,\cdots,pk_n} &\equiv \sum_{j_1=0}^{h_1} \cdots \sum_{j_n=0}^{h_n} g_{j_1,\cdots,j_n} a_{j_1,\cdots,j_n}(f_{pk_1,\cdots,pk_n}) \\ &\equiv g_{k_1,\cdots,k_n} a_{k_1,\cdots,k_n}(f_{pk_1,\cdots,pk_n}) \pmod{\pi}, \end{aligned} \tag{4.28}$$

which is a unit in $\mathcal{O}$. This proves that

$$\lambda(\beta) = pk_1 + \cdots + pk_n = p^2 + pk = p\lambda(G(T_1, \cdots, T_n)).$$

Case 4: Suppose that $\lambda(G(T_1, \cdots, T_n)) = 2p$. Then there exists a partition $k_1 + \cdots + k_n$ of $2p$ such that $g_{k_1,\cdots,k_n}$ is a unit in $\mathcal{O}$ and for every $m_i \geq 0$ satisfying $m_1 + \cdots + m_n < 2p$, $g_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi}$. Let $m < 2p^2 - p$. Then for every partition $m_1 + \cdots + m_n$ of m we have $l_1 + \cdots + l_n < 2p$, where $l_i = \mathrm{ord}_p(m_i!)$. As shown in the case 1, this implies that $b_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi}$. If $2p^2 - p \leq m < 2p^2$, then for every partition $m_1 + \cdots + m_n$ of m we have $l_1 + \cdots + l_n \leq 2p$. If $l_1 + \cdots + l_n < 2p$, then we have already observed that $b_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi}$. Also, if $l_1 + \cdots + l_n = 2p$, then from Lemma 3.3.7 we get $b_{m_1,\cdots,m_n} \equiv 0 \pmod{\pi}$. Let us now consider the partition $k_1 + \cdots + k_n$ of $2p$. Then $pk_1 + \cdots + pk_n$ is a partition of $2p^2$. If $k_i = 2p$ for some i, then

$\text{ord}_p(pk_i) = 2p + 2$. But from Lemma 3.3.5, we get

$$a_{2p+1}(f_{2p^2}) \equiv 0 \pmod{p} \text{ and } a_{2p+2}(f_{2p^2}) \equiv 0 \pmod{p}.$$

Using this and considering the other possible values of k_i as shown in the previous case, we obtain

$$\begin{aligned} b_{pk_1,\cdots,pk_n} &\equiv \sum_{j_1=0}^{h_1} \cdots \sum_{j_n=0}^{h_n} g_{j_1,\cdots,j_n} a_{j_1,\cdots,j_n}(f_{pk_1,\cdots,pk_n}) \\ &\equiv g_{k_1,\cdots,k_n} a_{k_1,\cdots,k_n}(f_{pk_1,\cdots,pk_n}) \pmod{\pi}, \end{aligned} \tag{4.29}$$

where $h_i = \text{ord}_p(pk_i!)$. Again, from Lemma 3.3.5 we get

$$a_{2p}(f_{2p^2}) \equiv t_1^2 \pmod{p}.$$

Considering the other possibilities as shown in the previous case, (4.29) implies that $b_{pk_1,\cdots,pk_n}$ a unit in $\mathcal{O}$. This proves that

$$\lambda(\beta) = pk_1 + \cdots + pk_n = 2p^2 = p\lambda(G(T_1, \cdots, T_n)).$$

This completes the proof of the main theorem. □

Chapter 5

Coefficients of a p-Adic Measure and its Γ-Transform

In this chapter we discuss some consequences of the results of Chapter 4. We relate the coefficients of a p-adic measure α on $\mathbb{Z}_p^2$ to the λ-invariant of the Iwasawa series of the Γ-transform of α. One can produce similar results for any α defined on $\mathbb{Z}_p^n$, but the number of coefficients of $\widehat{\alpha}(T_1 - 1, \cdots, T_n - 1)$ which are involved increases with n.

5.1 Introduction

In case of $n = 1$, Childress in her paper [13] showed how the coefficients of the power series associated to a p-adic measure α on $\mathbb{Z}_p$ are related to the coefficients of the measure β. She proved congruences modulo p amongst these coefficients. Finally, using these congruences and the results of [14], [25] and [10], she related the coefficients of α to the λ-invariant of the Iwasawa series of the Γ-transform of α. Following her approach, one can generalize the congruences modulo p amongst the coefficients of a p-adic measure α on $\mathbb{Z}_p^n$ and the coefficients of the

associated measure β.

Recall that $\mathcal{O}$ denotes the ring of integers in a finite extension of $\mathbb{Q}_p$ with a local parameter π, where p is a fixed odd prime. We write $\mathbb{Z}_p^\times = V \times U$ where V is the group of $(p-1)$st roots of unity in $\mathbb{Z}_p$ and $U = 1 + p\mathbb{Z}_p$. Let u be a topological generator of U. The projections from $\mathbb{Z}_p^\times$ onto V and U are denoted by ω and $<>$ respectively. We have an isomorphism $\phi : \mathbb{Z}_p \to U$ given by $\phi(y) = u^y$.

Let $\Lambda_{(n)}$ denote the $\mathcal{O}$-valued measures on $\mathbb{Z}_p^n$. The Iwasawa power series associated with $\alpha \in \Lambda_{(n)}$ is given by

$$\begin{aligned}\widehat{\alpha}(T_1, \cdots, T_n) &= \int_{\mathbb{Z}_p^n} T_1^{x_1} \cdots T_n^{x_n} d\alpha(x_1, \cdots, x_n) \\ &= \sum_{m_1=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} \left(\int_{\mathbb{Z}_p^n} \binom{x_1}{m_1} \cdots \binom{x_n}{m_n} d\alpha(x_1, \cdots, x_n) \right) \\ &\qquad \times (T_1 - 1)^{m_1} \cdots (T_n - 1)^{m_n}. \end{aligned} \tag{5.1}$$

Similar to the case $n = 1$, we have the following integration formulas:

$$\begin{aligned}&\int_{\mathbb{Z}_p^n} x_1^{m_1} \cdots x_n^{m_n} d\alpha(x_1, \cdots, x_n) \\ &= \left(T_1 \frac{d}{dT_1} \right)^{m_1} \cdots \left(T_n \frac{d}{dT_n} \right)^{m_n} \widehat{\alpha}(T_1, \cdots, T_n)|_{T_1 = \cdots = T_n = 1} \end{aligned} \tag{5.2}$$

For $s_1, \cdots, s_n \in \mathbb{Z}_p$, let each of $k_1, \cdots, k_n$ vary through a sequence of positive integers satisfying $k_j \to s_j$ p-adically and $k_j \equiv 0 \pmod{p-1}$. Then the Γ-transform of a measure $\alpha \in \Lambda_{(n)}$ is defined as a function of the p-adic variables $s_1, \cdots, s_n$ given by

$$\begin{aligned}\Gamma_\alpha(s_1, \cdots, s_n) &= \lim_{k_1, \cdots, k_n} \int_{\mathbb{Z}_p^n} x_1^{k_1} \cdots x_n^{k_n} d\alpha(x_1, \cdots, x_n) \\ &= \int_{(\mathbb{Z}_p^\times)^n} < x_1 >^{s_1} \cdots < x_n >^{s_n} d\alpha(x_1, \cdots, x_n). \end{aligned} \tag{5.3}$$

If we put $d\alpha(a_1x_1, \cdots, a_nx_n)$ for $d(\alpha \circ (a_1, \cdots, a_n))(x_1, \cdots, x_n)$, splitting up the integral, we can also write

$$\begin{aligned}
&\Gamma_\alpha(s_1, \cdots, s_n) \\
&\quad = \sum_{\eta_1 \in V} \cdots \sum_{\eta_n \in V} \int_{U^n} < \eta_1 x_1 >^{s_1} \cdots < \eta_n x_n >^{s_n} d\alpha(\eta_1 x_1, \cdots, \eta_n x_n) \\
&\quad = \int_{U^n} x_1^{s_1} \cdots x_n^{s_n} d\beta(x_1, \cdots, x_n),
\end{aligned}$$

where

$$\beta = \sum_{\eta_1 \in V} \cdots \sum_{\eta_n \in V} (\alpha \circ (\eta_1, \cdots, \eta_n))|_{U^n},$$

a measure on U^n. We extend β to $\mathbb{Z}_p^n$ by 0 and then we get a power series

$$\widehat{\beta}(T_1, \cdots, T_n) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} b_{m_1, \cdots, m_n} (T_1 - 1)^{m_1} \cdots (T_n - 1)^{m_n}. \tag{5.4}$$

Again, the measure β may be viewed as a measure on $\mathbb{Z}_p^n$ via the isomorphism ϕ:

$$\tilde{\beta}(A_1, \cdots, A_n) = \beta(\phi(A_1), \cdots, \phi(A_n)).$$

Let us write $d\beta(u^{y_1}, \cdots, u^{y_n})$ for $d\tilde{\beta}(y_1, \cdots, y_n)$. Let $G(T_1, \cdots, T_n)$ be the power series associated to $\tilde{\beta}$, that is,

$$G(T_1, \cdots, T_n) = \int_{\mathbb{Z}_p^n} T_1^{y_1} \cdots T_n^{y_n} d\beta(u^{y_1}, \cdots, u^{y_n}).$$

Then $\Gamma_\alpha(s_1, \cdots, s_n) = G(u^{s_1}, \cdots, u^{s_n})$.

Thus, for a given $\mathcal{O}$-valued measure α on $\mathbb{Z}_p^n$, we can define the Γ-transform of α. Splitting up the integral of the Γ-transform, one obtains a new measure $\beta = \sum_{\eta_1 \in V} \cdots \sum_{\eta_n \in V} (\alpha \circ (\eta_1, \cdots, \eta_n))|_{U^n}$, which is a measure on U^n, where $U = 1 + p\mathbb{Z}_p$. Now there are two ways of getting a measure on $\mathbb{Z}_p^n$ from β. The first one is $\tilde{\beta}$ which is obtained through the isomorphism $\phi : \mathbb{Z}_p \to U$. If

the power series associated with $\tilde{\beta}$ is $G(T_1, \cdots, T_n)$, then it is related to the Γ-transform of α as follows:

$$\Gamma_\alpha(s_1, \cdots, s_n) = G(u^{s_1}, \cdots, u^{s_n}),$$

where u is a topological generator of U. The second one is obtained from β by extending 0 to $\mathbb{Z}_p^n$. We shall denote it again by β.

5.2 The series associated to β

Let α be a $\mathcal{O}$-valued measure on $\mathbb{Z}_p$. We know that $\mathbb{Z}_p^\times = V \times U$ where V is the group of $(p-1)$st roots of unity in $\mathbb{Z}_p$ and $U = 1 + p\mathbb{Z}_p$. For $\eta \in V$, we have

$$\begin{aligned} \widehat{\alpha \circ \eta}(T) &= \int_{\mathbb{Z}_p} T^x d(\alpha \circ \eta)(x) \\ &= \int_{\mathbb{Z}_p} T^{\eta^{-1}x} d\alpha(x) \\ &= \widehat{\alpha}(T^{\overline{\eta}}), \end{aligned} \tag{5.5}$$

where $\overline{\eta} = \eta^{-1}$.

Again, $(\alpha \circ \eta)|_U = (\alpha|_{\eta U}) \circ \eta$. Therefore, if $\beta = \sum_{\eta \in V} (\alpha \circ \eta)|_U$, we have

$$\widehat{\beta}(T) = \sum_{\eta \in V} \widehat{\alpha|_{\eta U}}(T^{\overline{\eta}}). \tag{5.6}$$

Let us fix a primitive pth root of unity ζ. The characteristic function of $\mathbb{Z}_p^\times$ is

$$1 - \frac{1}{p} \sum_{j=0}^{p-1} \zeta^{jx}.$$

Childress in her paper [13, Theorem 4, p.p. 251] gave some congruences between the coefficients of $\widehat{\alpha}(T)$ and $\widehat{\alpha|_{\eta U}}(T)$. We now state her result below.

Result 5.2.1. *Let α be a $\mathcal{O}$-valued measure on $\mathbb{Z}_p$ and let $\widehat{\alpha}(T) = \sum a_i(T-1)^i$ be the associated power series. Given a non-negative integer k, let n be the integer such that $np < k \leq (n+1)p$. Then the coefficients of $(T-1)^k$ in $\widehat{\alpha|_{\mathbb{Z}_p^\times}}(T)$ is c_k, where modulo $p\mathcal{O}$*

$$c_k \equiv \begin{cases} a_k, & \text{when } np < k < (n+1)p; \\ \sum_{i=(n+1)p+1}^{(n+2)p-1} (-1)^{i-n} a_i, & \text{when } k = (n+1)p. \end{cases}$$

The following result is due to Childress.

Result 5.2.2. *([13, p.p. 254, Theorem 5]) Let $\alpha \in \Lambda_{(1)}$ and let $\widehat{\alpha}(T) = \sum a_i(T-1)^i$ be the associated power series. Let η be a fixed $(p-1)^{th}$ root of unity in $\mathbb{Z}_p$. Given a non-negative integer k, let m be the integer such that $mp \leq k < (m+1)p$, and put $k = mp + k_0$. Let $\eta_0 < p$ be the positive integer such that $\eta \equiv \eta_0 \pmod p$. Then the coefficient of $(T-1)^k$ in $\widehat{\alpha|_{\eta U}}(T)$ is $e_{k,\eta}$, where, modulo p, we have*

$$e_{k,\eta} \equiv \binom{\eta_0}{k_0} \sum_{j=0}^{p-\eta_0-1} \binom{j+\eta_0}{j} (-1)^j a_{pm+\eta_0+j}. \tag{5.7}$$

Let $\alpha \in \Lambda_{(2)}$ and $\eta, \nu \in V$. Let us fix a primitive p^{th} root of unity ζ. The characteristic function of $\eta U \times \nu U$ is $\left[\frac{1}{p}\sum_{j_1=1}^{p} \zeta^{j_1(x_1-\eta)}\right] \times \left[\frac{1}{p}\sum_{j_2=1}^{p} \zeta^{j_2(x_2-\nu)}\right]$. Using this and the above result, we have the following result.

Theorem 5.2.1. *Let $\alpha \in \Lambda_{(2)}$ and let $\widehat{\alpha}(T_1, T_2) = \sum\sum a_{i_1,i_2}(T_1-1)^{i_1}(T_2-1)^{i_2}$ be the associated power series. Let η and ν be fixed $(p-1)^{th}$ root of unity in $\mathbb{Z}_p$. Given non-negative integers k_1, k_2, let m_1, m_2 be the integers such that $m_1 p \leq k_1 < (m_1+1)p$ and $m_2 p \leq k_2 < (m_2+1)p$. Put $k_1 = m_1 p + k_1^0$ and $k_2 = m_2 p + k_2^0$. Let $\eta_0 < p$ and $\nu_0 < p$ be the positive integers such that $\eta \equiv \eta_0 \pmod p$ and $\nu \equiv \nu_0 \pmod p$. Then the coefficient of $(T_1-1)^{k_1}(T_2-1)^{k_2}$ in*

$\widehat{\alpha|_{\eta U\times\nu U}}(T_1,T_2)$ *is* $e^{\eta,\nu}_{k_1,k_2}$, *where, modulo* $p\mathcal{O}$, *we have*

$$e^{\eta,\nu}_{k_1,k_2} \equiv \binom{\eta_0}{k_1^0}\binom{\nu_0}{k_2^0}\sum_{j_1=0}^{p-\eta_0-1}\sum_{j_2=0}^{p-\nu_0-1}\binom{j_1+\eta_0}{j_1}\binom{j_2+\nu_0}{j_2}(-1)^{j_1+j_2}a_{pm_1+\eta_0+j_1,pm_2+\nu_0+j_2}. \tag{5.8}$$

Now, we note that $\widehat{\alpha\circ(\eta,\nu)}(T_1,T_2)=\widehat{\alpha}(T_1^{\overline{\eta}},T_2^{\overline{\nu}})$, where $\overline{\eta}=\eta^{-1}$ and $\overline{\nu}=\nu^{-1}$. Also, $(\alpha\circ(\eta,\nu))|_{U^2}=(\alpha|_{\eta U\times\nu U})\circ(\eta,\nu)$. Therefore,

$$\widehat{\beta}(T_1,T_2)=\sum_{\eta\in V}\sum_{\nu\in V}\widehat{\alpha|_{\eta U\times\nu U}}(T_1^{\overline{\eta}},T_2^{\overline{\nu}}). \tag{5.9}$$

In case $\alpha\in\Lambda_{(1)}$, Childress in her paper [13] proved certain congruences modulo p amongst the coefficients of $\widehat{\alpha}(T)$ and $\widehat{\beta}(T)$. Using her approach, we shall prove Theorem 5.2.2 below. Let us now state a useful lemma (see [13, p.p. 255, Lemma 6]) and one can give a proof of the lemma by induction on k.

Lemma 5.2.1. *For any positive integer* k,

$$\left[\sum_{j=1}^{\infty}\binom{\eta}{j}Y^j\right]^k=\sum_{j=k}^{\infty}\rho_\eta(j,k)Y^j,$$

where $\rho_\eta(j,k)$ *is defined by:* $\rho_\eta(j,1)=\binom{\eta}{j}$, $\rho_\eta(j,k)=\sum_{i=1}^{j-1}\binom{\eta}{i}\rho_\eta(j-i,k-1)$.

For notational convenience, we set $\rho_\eta(j,0)=\rho_\eta(0,k)=0$ when $jk\neq 0$ and $\rho_\eta(0,0)=1$.

Childress proved the following useful result in [13, p.p. 255, Theorem 7].

Result 5.2.3. *If* $\widehat{\alpha}(T)=\sum a_i(T-1)^i$ *and* $\widehat{\beta}(T)=\sum b_i(T-1)^i$, *then*

$$b_{pj}\equiv\sum_{\eta\in V}\sum_{i=\eta_0}^{p-1}\binom{i}{\eta_0}(-1)^{i-\eta_0}\sum_{r=0}^{j}a_{pr+i}\sum_{k=0}^{\eta_0}\binom{\eta_0}{k}\rho_{\overline{\eta}}(pj,pr+k)\pmod{p\mathcal{O}}.$$

Following her approach, we shall now give a brief proof of the following result.

Theorem 5.2.2. *For $j_1 \geq 0, j_2 \geq 0$,*

$$b_{j_1p,j_2p} \equiv \sum_{\eta\in V}\sum_{\nu\in V}\sum_{i_1=\eta_0}^{p-1}\sum_{i_2=\nu_0}^{p-1}(-1)^{i_1+i_2-\eta_0-\nu_0}\binom{i_1}{\eta_0}\binom{i_2}{\nu_0}\sum_{r_1=0}^{j_1}\sum_{r_2=0}^{j_2}a_{pr_1+i_1,pr_2+i_2}\times$$
$$\sum_{t_1=0}^{r_1}\sum_{t_2=0}^{r_2}(-1)^{r_1+t_1+r_2+t_2}\binom{r_1}{t_1}\binom{r_2}{t_2}\binom{\overline{\eta}(t_1+\frac{\eta_0-\eta}{p})}{j_1}\binom{\overline{\nu}(t_2+\frac{\nu_0-\nu}{p})}{j_2} \pmod{p\mathcal{O}}. \tag{5.10}$$

Proof. Note that

$$\widehat{\beta}(T_1,T_2) = \sum_{\eta\in V}\sum_{\nu\in V}\widehat{\alpha|_{\eta U\times\nu U}}(T_1^{\overline{\eta}},T_2^{\overline{\nu}})$$
$$= \sum_{\eta\in V}\sum_{\nu\in V}\sum_{k_1=0}^{\infty}\sum_{k_2=0}^{\infty}e_{k_1,k_2}^{\eta,\nu}(T_1^{\overline{\eta}}-1)^{k_1}(T_2^{\overline{\nu}}-1)^{k_2}$$
$$= \sum_{\eta\in V}\sum_{\nu\in V}\sum_{k_1=0}^{\infty}\sum_{k_2=0}^{\infty}e_{k_1,k_2}^{\eta,\nu}\left[\sum_{j_1}^{\infty}\binom{\overline{\eta}}{j_1}(T_1-1)^{j_1}\right]^{k_1}\left[\sum_{j_2}^{\infty}\binom{\overline{\nu}}{j_2}(T_2-1)^{j_2}\right]^{k_2}$$
$$= \sum_{\eta\in V}\sum_{\nu\in V}\sum_{k_1=0}^{\infty}\sum_{k_2=0}^{\infty}e_{k_1,k_2}^{\eta,\nu}\sum_{j_1=k_1}^{\infty}\sum_{j_2=k_2}^{\infty}\rho_{\overline{\eta}}(j_1,k_1)\rho_{\overline{\nu}}(j_2,k_2)(T_1-1)^{j_1}(T_2-1)^{j_2} \tag{5.11}$$

To obtain (5.11), we applied Lemma 5.2.1. From (5.11), we finally obtain

$$\widehat{\beta}(T_1,T_2)$$
$$= \sum_{j_1=0}^{\infty}\sum_{j_2=0}^{\infty}(T_1-1)^{j_1}(T_2-1)^{j_2}\left[\sum_{k_1=0}^{j_1}\sum_{k_2=0}^{j_2}\sum_{\eta\in V}\sum_{\nu\in V}e_{k_1,k_2}^{\eta,\nu}\rho_{\overline{\eta}}(j_1,k_1)\rho_{\overline{\nu}}(j_2,k_2)\right]. \tag{5.12}$$

Modulo $p\mathcal{O}$, we have

$$\begin{aligned} b_{0,0} &\equiv \sum_{\eta\in V}\sum_{\nu\in V} e_{0,0}^{\eta,\nu} \\ &\equiv \sum_{\eta_0=1}^{p-1}\sum_{\nu_0=1}^{p-1}\sum_{j_1=0}^{p-1-\eta_0}\sum_{j_2=0}^{p-1-\nu_0}\binom{j_1+\eta_0}{j_1}\binom{j_2+\nu_0}{j_2}(-1)^{j_1+j_2}a_{\eta_0+j_1,\nu_0+j_2} \\ &\equiv \sum_{j_1=0}^{p-2}\sum_{j_2=0}^{p-2}(-1)^{j_1+j_2}\sum_{\eta_0=1}^{p-1-j_1}\sum_{\nu_0=1}^{p-1-j_2}\binom{j_1+\eta_0}{j_1}\binom{j_2+\nu_0}{j_2}a_{\eta_0+j_1,\nu_0+j_2} \\ &\equiv \sum_{k_1=1}^{p-1}\sum_{k_2=1}^{p-1}a_{k_1,k_2}\sum_{i_1=0}^{k_1-1}\sum_{i_2=0}^{k_2-1}\binom{k_1}{i_1}\binom{k_2}{i_2}(-1)^{i_1+i_2} \\ &\equiv \sum_{k_1=1}^{p-1}\sum_{k_2=1}^{p-1}(-1)^{k_1+k_2}a_{k_1,k_2}. \end{aligned} \tag{5.13}$$

Similarly, if j_1 or $j_2 \geq 1$, then following the proof of Result 5.2.3 (see [13, p.p. 255, Theorem 7]), we have

$$\begin{aligned} b_{pj_1,pj_2} \equiv \sum_{\eta\in V}\sum_{\nu\in V}\sum_{i_1=\eta_0}^{p-1}\sum_{i_2=\nu_0}^{p-1}\binom{i_1}{\eta_0}\binom{i_2}{\nu_0}(-1)^{i_1+i_2-\eta_0-\nu_0}\sum_{r_1=0}^{j_1}\sum_{r_2=0}^{j_2}a_{pr_1+i_1,pr_2+i_2}\times \\ \sum_{k_1=0}^{\eta_0}\sum_{k_2=0}^{\nu_0}\binom{\eta_0}{k_1}\binom{\nu_0}{k_2}\rho_{\overline{\eta}}(pj_1,pr_1+k_1)\rho_{\overline{\nu}}(pj_2,pr_2+k_2) \pmod{p\mathcal{O}}. \end{aligned} \tag{5.14}$$

From the definition of ρ, we find that $\sum_{k_1=0}^{\eta_0}\binom{\eta_0}{k_1}\rho_{\overline{\eta}}(pj_1,pr_1+k_1)$ is the coefficient of $Y_1^{j_1p}$ in $\sum_{k_1=0}^{\eta_0}\binom{\eta_0}{k_1}\left[\sum_{t_1}^{\infty}\binom{\overline{\eta}}{t_1}Y_1^{t_1}\right]^{r_1p+k_1}$ and hence it is the coefficient of $Y_1^{j_1p}$ in $(1+Y_1)^{\overline{\eta}\eta_0}\left((1+Y_1)^{\overline{\eta}}-1\right)^{r_1p}$. Let $x_1 = \frac{\overline{\eta}(\eta_0-\eta)}{p}$ and clearly $x_1 \in \mathbb{Z}_p$. Then we

have

$$\sum_{k_1=0}^{\eta_0}\binom{\eta_0}{k_1}\rho_{\overline{\eta}}(pj_1, pr_1+k_1)$$

$$= \text{coefficient of } Y_1^{pj_1} \text{ in } (1+Y_1)^{px_1+1}\left((1+Y_1)^{\overline{\eta}}-1\right)^{r_1 p}$$

$$\equiv \text{coefficient of } Y_1^{pj_1} \text{ in } (1+Y_1)(1+Y_1^p)^{x_1}\left((1+Y_1^p)^{\overline{\eta}}-1\right)^{r_1}$$

$$\equiv \text{coefficient of } Y_1^{j_1} \text{ in } (1+Y_1)^{x_1}\left((1+Y_1)^{\overline{\eta}}-1\right)^{r_1}$$

$$\equiv \sum_{t_1=0}^{r_1}(-1)^{r_1+t_1}\binom{r_1}{t_1}\binom{x_1+\overline{\eta}t_1}{j_1} \pmod{p}. \tag{5.15}$$

From (5.13)-(5.15), we complete the proof of the theorem. □

5.3 An application to λ-invariants

In this section we give criteria for the value of the λ-invariant of the power series $\widehat{\beta}(T_1, T_2)$ in terms of the coefficients of $\widehat{\alpha}(T_1, T_2)$. If $\alpha \in \Lambda_{(1)}$, then the λ-invariant of $\widehat{\beta}(T)$ is p times the λ-invariant of the Iwasawa series of G as in [2, 10, 14, 25]. In Chapter 4, we proved the following theorem. Also see [16].

Theorem 5.3.1. *If $\lambda(G(T_1, \cdots, T_n)) \leq 2p$, then $\lambda(\beta) = p\lambda(G(T_1, \cdots, T_n))$.*

Suppose that

$$G(T_1, \cdots, T_n) = \sum_{m_1=0}^{\infty}\cdots\sum_{m_n=0}^{\infty} g_{m_1,\cdots,m_n}(T_1-1)^{m_1}\cdots(T_n-1)^{m_n}. \tag{5.16}$$

If $\lambda(G(T_1, \cdots, T_n)) = k$, then for a partition $k_1 + \cdots + k_n$ of k, $g_{k_1,\cdots,k_n}$ is a unit in $\mathcal{O}$. In the proof of the Theorem 5.3.1, we showed that $b_{pk_1,\cdots,pk_n}$ is also a unit in $\mathcal{O}$. Using this and Theorem 5.2.2, we will give criteria for the λ-invariant of the power series $\widehat{\beta}(T_1, T_2)$ in terms of the coefficients of $\widehat{\alpha}(T_1, T_2)$. Let $\eta \in V \subseteq \mathbb{Z}_p^{\times}$. Let $\eta_0 < p$ be the positive integer such that $\eta \equiv \eta_0 \pmod{p}$.

It easily follows from Hensel's lemma that $\eta \equiv \eta_0^p \pmod{p^2}$. Given a prime p, we use this fact to evaluate the expression of Theorem 5.2.2.

Example 5.3.1. *Let $p = 3$ and $\alpha \in \Lambda_{(2)}$ be such that $\mu(G(T_1, T_2)) = 0$. Then we have:*

1. *$\lambda(G) = 0$ if and only if $a_{1,1} + a_{2,2} \not\equiv a_{1,2} + a_{2,1} \pmod{\pi}$.*
2. *If $\lambda(G) > 0$, then $\lambda(G) = 1$ if and only if either $a_{2,1} + a_{4,1} \not\equiv a_{2,2} + a_{4,2} \pmod{\pi}$ or $a_{1,2} + a_{1,4} \not\equiv a_{2,2} + a_{2,4} \pmod{\pi}$.*
3. *If $\lambda(G) > 1$, then $\lambda(G) = 2$ if and only if any one of the following is true:*
   (a) $a_{2,2} + a_{4,4} \not\equiv a_{2,4} + a_{4,2} \pmod{\pi}$
   (b) $a_{2,2} + a_{5,1} + a_{7,2} + a_{8,1} \not\equiv a_{2,1} + a_{5,2} + a_{7,1} + a_{8,2} \pmod{\pi}$
   (c) $a_{2,2} + a_{1,5} + a_{2,7} + a_{1,8} \not\equiv a_{1,2} + a_{2,5} + a_{1,7} + a_{2,8} \pmod{\pi}$.
4. *If $\lambda(G) > 2$, then $\lambda(G) = 3$ if and only if any one of the following is true:*
   (a) $a_{5,1} + a_{10,1} \not\equiv a_{5,2} + a_{10,2} \pmod{\pi}$
   (b) $a_{1,5} + a_{1,10} \not\equiv a_{2,5} + a_{2,10} \pmod{\pi}$
   (c) $a_{2,2} + a_{4,5} + a_{4,8} \not\equiv a_{4,2} + a_{2,7} + a_{4,7} + a_{2,8} \pmod{\pi}$
   (d) $a_{2,2} + a_{5,4} + a_{8,4} \not\equiv a_{2,4} + a_{7,2} + a_{7,4} + a_{8,2} \pmod{\pi}$.

In this way, in case $p = 3$, we can find criteria for the λ invariant of $G(T_1, T_2)$ in terms of the coefficients of $\widehat{\alpha}(T_1, T_2)$ if $\lambda(G) \leq 6$.

We may produce similar results for any prime p. The number of coefficients of $\widehat{\alpha}(T_1, T_2)$ which are involved increases with p.

Example 5.3.2. *Let $p = 3$ and consider the measure $\alpha \in \Lambda_{(2)}$ given by the power series $\sum_{k=1}^{\infty} T_1^{4^k} T_2$. We now find the Iwasawa series of the Γ-transform of α. Using* (5.2) *and* (5.3)*, we find that*

$$\begin{aligned}\Gamma_\alpha(s_1, s_2) &= \lim_{k_1,k_2} \int_{\mathbb{Z}_p^2} x_1^{k_1} x_2^{k_2} d\alpha(x_1, x_2) \\ &= \lim_{k_1,k_2} \left(T_1 \frac{d}{dT_1}\right)^{k_1} \left(T_2 \frac{d}{dT_2}\right)^{k_2} \widehat{\alpha}(T_1, T_2)|_{T_1=T_2=1} \\ &= \lim_{k_1,k_2} \left(T_1 \frac{d}{dT_1}\right)^{k_1} \left(T_2 \frac{d}{dT_2}\right)^{k_2} \sum_{k=1}^{\infty} T_1^{4^k} T_2|_{T_1=T_2=1}, \end{aligned} \tag{5.17}$$

where for $s_1, s_2 \in \mathbb{Z}_p$, each of k_1, k_2 vary through a sequence of positive integers satisfying $k_j \to s_j$ p-adically and $k_j \equiv 0 \pmod{p-1}$. From (5.17)*, we find that $G(T_1, T_2) = \sum_{k=1}^{\infty} T_1^k$, where, for $s_1, s_2 \in \mathbb{Z}_p$, $G((1+p)^{s_1}, (1+p)^{s_2}) = \Gamma_\alpha(s_1, s_2)$. Clearly $\lambda(G) = 1$ and this can also be verified using (1) and (2) of Example 5.3.1.*

Chapter 6

Conclusions and Future Research

Throughout this dissertation, we focused on Iwasawa μ-invariants of elliptic curves defined over $\mathbb{Q}$ and Iwasawa λ-invariants of p-adic measure on $\mathbb{Z}_p^n$ and their Γ-transforms.

- Let us first review the main result of Chapter 2. We considered two elliptic curves defined over $\mathbb{Q}$ and having good ordinary reduction at any odd prime p. We showed that $\mu(E_1) = \mu(E_2)$ if both $E_1(\mathbb{Q})[p]$ and $E_2(\mathbb{Q})[p]$ are trivial and $E_1[p^i] \cong E_2[p^i]$ as $G_{\mathbb{Q}}$-modules, where $i = \mu(E_1) + 1$. It will be interesting to investigate the above question for elliptic curves with supersingular reduction. In [3], B. D. Kim studied the Iwasawa μ and λ-invariants of the plus/minus Selmer groups of elliptic curves with isomorphic residual representation using ideas of [21]. Let E_1, E_2 be elliptic curves defined over $\mathbb{Q}$ with supersingular reduction at a prime p and $E_1[p] \cong E_2[p]$ as Galois modules. Then Kim proved that the Iwasawa μ-invariant $\mu^{\pm}(E_1)$ of $Sel_p^{\pm}(E_1/\mathbb{Q}_\infty)$ is zero if and only if $\mu^{\pm}(E_2) = 0$. Using the ideas of Chapter 2, we would like to study Iwasawa μ and λ-invariants of the plus/minus Selmer groups of elliptic curves.

- Let u be a topological generator of $1+p\mathbb{Z}_p$. Let us consider the continuous functions $f_m : \mathbb{Z}_p \to \mathbb{Z}_p$ and $f_{m_1,\cdots,m_n} : \mathbb{Z}_p^n \to \mathbb{Z}_p$ defined by $f_m(x) = \binom{u^x}{m}$ and $f_{m_1,\cdots,m_n}(x_1,\cdots,x_n) = f_{m_1}(x_1)\cdots f_{m_n}(x_n)$, respectively. Using the classical theorem of Mahler, we find that

$$f_m(x) = \binom{u^x}{m} = \sum_{j=0}^{\infty} a_j(f_m)\binom{x}{j}$$

and

$$f_{m_1,\cdots,m_n}(x_1,\cdots,x_n) = \sum_{j_1=0}^{\infty}\cdots\sum_{j_n=0}^{\infty} a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n})\binom{x_1}{m_1}\cdots\binom{x_n}{m_n}.$$

In Chapter 3, we discussed certain p-adic properties of the Mahler coefficients $a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n})$ for any $n \geq 1$. But, we were able to derive the p-adic properties only for a few of them. It will be interesting to classify all the Mahler coefficients according to their p-adic properties. In Chapter 4, using p-adic properties of the Mahler coefficients $a_{j_1,\cdots,j_n}(f_{m_1,\cdots,m_n})$, we proved that if $\lambda(G(T_1,\cdots,T_n)) \leq 2p$, then $\lambda(\beta) = p\lambda(G(T_1,\cdots,T_n))$. Hence, if we know p-adic properties of more Mahler coefficients, we can improve the condition of the above theorem.

- Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Let $f(T) \in \mathcal{O}[[T]]$. The λ-invariant of f is nothing but the $\mathbb{Z}_p$-rank of $\mathcal{O}[[T]]/(\pi^{-\mu(f)}f)$. Thus the λ-invariant has an important algebraic significance. We have defined Iwasawa invariants of a power series in n-variables with coefficients in $\mathcal{O}$ for $n \geq 1$. It will be interesting to know whether there is any algebraic significance of λ-invariant of such a multivariable power series over $\mathcal{O}$. It is already known that the above algebraic significance of a formal power series in one variable does not extend to more than one variable. However,

when the power series of more than one variable has finite order (so that the Weierstrass Preparation Theorem in several variables can be applied to it), it would be interesting to see if there is a connection between their λ-invariants and invariants arising via the Weierstrass Preparation Theorem.

References

[1] A. Nichifor, *Iwasawa Theory for Elliptic Curves with Cyclic Isogenies*, PhD Thesis, submitted at the Department of Mathematics, University of Washington, 2004.

[2] A. Saikia and R. Barman, *Iwasawa λ-invariants and Γ-transforms*, J. Ramanujan Math. Soc. **24** (2009), no. 2, 199–209.

[3] B. D. Kim, *The Iwasawa invariants of the plus/minus Selmer groups of elliptic curves for supersingular primes*, Asian J. Math. **13** (2009), no. 1, 181–190.

[4] B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.

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

[6] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251.

[7] J. Coates and R. Sujatha, *Galois Cohomology of Elliptic Curves*, Lecture notes in Mathematics, TIFR, Narosa Publishing House, 2004.

[8] J. Cremona, *Elliptic curve data*, http://www.warwick.ac.uk/ J. E. Cremona/ ftp/ data/ INDEX.html.

[9] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Comprehensive Studies in Math., Springer, vol. 323, 2008.

[10] J. Satoh, *Iwasawa λ-invariants of Γ-Transforms*, J. Number Theory **41** (1992), 98–101.

[11] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., Springer-Verlag, vol. 106, 2009.

[12] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math., Springer-Verlag, vol. 83, 1982.

[13] N. Childress, *The coefficients of a p-adic measure and its Γ-transform*, Manuscripta math. **64** (1989), 359–375.

[14] _____, *λ-invariants and Γ-transforms*, Manuscripta math. **64** (1989), 359–375.

[15] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Text in Mathematics, Springer-Verlag, vol. 58, 1984.

[16] R. Barman and A. Saikia, *Iwasawa λ-invariants and Γ-transforms of p-adic measures on $\mathbb{Z}_p^n$*, to appear in Int. J. Number Theory.

[17] R. Greenberg, *Topics in Iwasawa theory*, http://www.math. washington.edu/ $\sim$ greenber/ personal.html.

[18] _____, *Iwasawa theory for elliptic curves*, Lecture notes in Math., Springer-Verlag (1999), 53–144.

[19] _____, *Introduction to Iwasawa theory for elliptic curves*, IAS/Park City Mathematicas Series **9** (2001), 409–464.

[20] _____, *Iwasawa theory- Past and Present*, Advanced Studies in Pure Mathematics **30** (2001), 335–385.

[21] R. Greenberg and V. Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), 17–63.

[22] S. Lang, *Cyclotomic Fields I and II*, Graduate Texts in Math., Springer-Verlag, vol. 121, 1990.

[23] S. Rosenberg, *On the Iwasawa invariants of the Γ-transform of a rational function*, J. Number Theory **109** (2004), 89–95.

[24] W. Sinnott, *On the μ-invariant of the Γ-transform of a rational function*, Invent. Math. **75** (1984), 273–282.

[25] Y. Kida, *The λ-invraints of p-adic measures on $\mathbb{Z}_p$ and $1+q\mathbb{Z}_p$*, Sci. Rep. Kanazawa Univ. **30** (1986), 33–38.

List of Publications/Communicated

Journals

1. A. Saikia and R. Barman, *Iwasawa λ-invariants and Γ-Transforms*, J. Ramanujan Math. Soc. 24, No. 2, 199-209 (2009).

2. R. Barman and A. Saikia, *Iwasawa λ-invariants and Γ-transforms of p-adic measures on $\mathbb{Z}_p^n$*, to appear in Int. J. Number Theory.

3. R. Barman and A. Saikia, *A note on Iwasawa μ-invariants of elliptic curves*, to appear in Bull. Braz. Math. Soc. (N.S.)

4. R. Barman and A. Saikia, *Coefficients of a p-adic measure on $\mathbb{Z}_p^n$ and Iwasawa λ-invariants of its Γ-transform*, communicated.