P-ADIC L-FUNCTIONS ATTACHED TO DIRICHLET'S CHARACTER

Mohammadhossein Shahabi

A Thesis
in The Department of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
For the Degree of
Master of Science (Mathematics)

at Concordia University
Montreal, Quebec, Canada

September 2023

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: Mohammadhossein Shahabi

Entitled: p-Adic L-functions attached to Dirichlet's character
and submitted in partial fulfillment of the requirements for the degree of

Master of Science (Mathematics)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality. Signed by the final Examining Committee:

____________________ Chair
Dr. Giovanni Rosso

____________________ Examiner
Dr. Giovanni Rosso

____________________ Examiner
Dr. Carlo Pagano

____________________ Thesis Supervisor
Dr. Adrian Iovita

Approved by ____________________
Dr. Lea Popovic (Graduate Program Director)

____
Dr. Pascale Sicotte (Dean of Faculty)

____
Date 2023-09-12

Abstract for MSc

p-Adic L-functions attached to Dirichlet's character

Mohammadhossein Shahabi

This thesis aims to extend and elaborate on the initial sections of Neal Koblitz's article titled "A New Proof of Certain Formulas for p-Adic L-Functions." Koblitz's article focuses on the construction of p-adic L-functions associated with Dirichlet's character and the computation of their values at $s = 1$. He employs measure-theoretic methods to construct the p-adic L-functions and compute the Leopoldt formula $L_p(1,\chi)$.

To begin, we devote the first section (1.1) to providing comprehensive proof of Dirichlet's theorem for prime numbers. This is done because the theorem serves as a noteworthy example of how Dirichlet L-functions became relevant in the field of Number Theory.

In the second chapter, we introduce the complex version of Dirichlet L-functions and Riemann Zeta functions. We explore their analytical properties, such as functional equations and analytic continuation. Subsequently, we construct the field of p-adic numbers and equip it with the p-adic norm to facilitate analysis. We introduce measures and perform p-adic integrations.

Finally, we delve into the concept of p-adic interpolation for the Riemann Zeta function, aiming to establish the p-adic Zeta function. To accomplish this, we employ Mazur's measure-theoretic approach, utilizing the tools introduced in the third chapter. The thesis concludes by incorporating Koblitz's work on this subject.

Acknowledgements

I would like to express my deep gratitude to my supervisor, Professor Adrian Iovita, for his exceptional guidance and mentorship throughout this program. Not only has he been an outstanding teacher, but he has also shown genuine care and support, akin to that of a grandfather to his grandson. I am truly thankful for the incredible opportunity he has given me to be his student. It is a privilege to have a supervisor of his caliber, and I am honored to be under his guidance. I sincerely wish to convey my heartfelt appreciation to Adrian, even if words alone may not suffice.

I would also like to extend my thanks to Professor Giovanni Rosso and Carlo Pagano for their invaluable discussions, comments, and the courses I had the privilege of taking with Giovanni during this program.

To my parents and my brother, I want to express my gratitude for their unwavering support and love, despite being separated by 12000 km during this journey. I hope to make them proud.

Lastly, I want to thank my uncle Shahab and my roommate, Shahaboddin. Without their presence, these two years of being away from my family would have been incredibly challenging to endure.

Contents

Chapter 1

Introduction

1.1 An overview on Dirichlet's theorem for prime numbers

In this section, we present Dirichlet's theorem for prime numbers, which serves as an illustration of how L-functions are used in number theory.

Theorem 1.1.1. *If q and $\mathfrak{l}$ are relatively prime positive integers, then there are infinitely many primes of the form $\mathfrak{l} + kq$ with $k \in \mathbb{Z}$.*

Dirichlet proved this theorem by showing that the series

$$\sum_{p \equiv \mathfrak{l} \ (mod\ q)} \frac{1}{p^s}$$

diverges, where the sum is over all primes congruent to $\mathfrak{l}$ modulo q. Once q is fixed and no confusion is possible, we write $p \equiv \mathfrak{l}\ (mod\ q)$ to denote a prime congruent to $\mathfrak{l}$ modulo q.
Let us introduce Dirichlet characters.
A Dirichlet character is a multiplicative homomorphism $\chi : (\mathbb{Z}/n\mathbb{Z})^{\times} \to S^1$ where S^1 is the multiplicative group of the unit circle in $\mathbb{C}$ i.e., $\{z \in \mathbb{C} \mid |z| = 1\ \}$. We can extend any character to a function $\chi : \mathbb{Z} \to \mathbb{C}$ by putting $\chi(a) = 0$ for $(a,n) \neq 1$. If $n \mid m$, then χ induces a homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^{\times} \to S^1$ by composition with the natural map $(\mathbb{Z}/m\mathbb{Z})^{\times} \to (\mathbb{Z}/n\mathbb{Z})^{\times}$. Therefore, we could regard χ as being defined mod m or mod n, since both are essentially the same map. It is convenient to choose n minimal and call it the conductor of χ, denoted f or f_χ (or d).
We also define characters of any finite abelian groups G with the multiplicative map $\chi : G \to S^1$.

We denote by $\widehat{G}$ the set of all characters of G, and we then notice that this set inherits an abelian group structure.

Lemma 1.1.2. *The set $\widehat{G}$ is an abelian group under multiplication defined by*

$$(\chi_1.\chi_2)(a) = \chi_1(a).\chi_2(a)$$

with the trivial character as the unit.

Proof. The proof is straightforward. ☐

We call the $\widehat{G}$ the dual group of G.
Let $\mathbb{Z}(N)$ denote the set of all Nth roots of unity in $\mathbb{C}$.

$$\mathbb{Z}(N) = \left\{1, e^{2\pi i/N}, e^{2\pi i 2/N}, ..., e^{2\pi i(N-1)/N}\right\}.$$

Remark 1.1.3. *All the characters over $\mathbb{Z}(N)$ are of the form:*

$$\chi_L(k) = e^{2\pi i Lk/N}, 0 \leq L \leq N-1.$$

Remark 1.1.4. *Let $\widehat{\mathbb{Z}(N)}$ be the dual group of $\mathbb{Z}(N)$, then $\widehat{\mathbb{Z}(N)}$ is isomorphic to $\mathbb{Z}(N)$ with the map:*

$$\varphi \ : \ L \to \chi_L.$$

Proof. Let $L_1, L_2 \in \mathbb{Z}(N)$, then $\varphi(L_1+L_2) = \chi_{L_1+L_2} = e^{2\pi i L_1 k/n}.e^{2\pi i L_2 k/n} = \varphi(L_1).\varphi(L_2)$. For injectivity, let $\varphi(L_1) = \varphi(L_2)$, then $\chi_{L_1} = \chi_{L_2}$ which implies that $L_1 = L_2$. Finally, if we take χ_{L_1} for some $L_1 \in \mathbb{Z}(N)$, then L_1 is the only candidate in the domain that is mapped to χ_{L_1}. ☐

An observation is that since $\mathbb{Z}/N\mathbb{Z}$ is isomorphic to $\mathbb{Z}(N)$, therefore $\widehat{\mathbb{Z}(N)}$ is also the dual group of $\mathbb{Z}/N\mathbb{Z}$.
The proof of Dirichlet's theorem consists of several steps, one of which requires Fourier analysis on the group $(\mathbb{Z}/q\mathbb{Z})^{\times}$. Before delving into the theorem in its entirety, let us first provide an overview of the solution to a specific question: whether there exists an infinite number of prime numbers in the form of $4k+1$. This example, which consists of the special case $q = 4$ and $\mathfrak{l} = 1$ in the Theorem (1.1.1), illustrates all the important steps in the proof of the theorem.
We begin with the character on $(\mathbb{Z}/4\mathbb{Z})^{\times}$ defined by $\chi(1) = 1$ and $\chi(3) = -1$. We extend this character to all of $\mathbb{Z}$ as follows:

$$\chi(n) = \begin{cases} 0 & \text{if } n \textit{ is even} \\ 1 & \text{if } n = 4k+1 \\ -1 & \text{if } n = 4k+3. \end{cases} \tag{1.1}$$

Let $L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)/n^s$, so that

$$L(s,\chi) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots .$$

Then $L(1,\chi)$ is the convergent series given by

$$L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots .$$

Since the terms in the series are alternating and their absolute values decrease to zero, we have $L(1,\chi) \neq 0$. Because χ is multiplicative, the Euler product for zeta function generalizes to give

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \quad primes} \frac{1}{1 - \chi(p)p^{-s}},$$

(as we will prove later).
Taking the logarithm of both sides, we find that

$$log(L(s,\chi)) = \sum_{p} \frac{\chi(p)}{p^s} + O(1).$$

Letting $s \to 1^+$, it could be noticed that if $L(1,\chi) \neq 0$, which indeed is equal to $\pi/4$, then $\sum_p \chi(p)/p^s$ remains bounded. Hence,

$$\sum_{p\equiv 1} \frac{1}{p^s} - \sum_{p\equiv 3} \frac{1}{p^s}$$

is bounded as $s \to 1^+$. Also, $\sum_p 1/p$ diverges. So putting these two facts together, we find that

$$2\sum_{p\equiv 1} \frac{1}{p^s}$$

is unbounded as $s \to 1^+$. Hence $\sum_{p\equiv 1} 1/p$ diverges and as a consequence, there are infinitely many primes of the form $4k + 1$. The rest of this chapter gives the full proof of Dirichlet's theorem.
We begin with the Fourier analysis (which is actually the last step in the example given above), and reduce the theorem to the non-vanishing of L-functions.
Let's have a brief discussion regarding Fourier analysis. In the subsequent discussion, we consider the abelian group G to be represented by $(\mathbb{Z}/q\mathbb{Z})^{\times}$. The formulas presented below incorporate the order of G, which represents the number of integers within the range of $0 \leq n < q$ that are relatively prime to q. This number defines the Euler phi-function $\varphi(q)$, $|G| = \varphi(q)$.
Consider the function $\delta_{\mathfrak{l}}$ on G, which we think of as the characteristic function of $\mathfrak{l}$; if

$n \in (\mathbb{Z}/q\mathbb{Z})^{\times}$,

$$\delta_{\mathfrak{l}}(n) = \begin{cases} 1 & \text{if } n \equiv \mathfrak{l} \quad (mod \quad q) \\ 0 & otherwise. \end{cases} \tag{1.2}$$

We can expand this function in a Fourier series as follows:

$$\delta_{\mathfrak{l}}(n) = \sum_{e \in \widehat{G}} \hat{\delta}_{\mathfrak{l}}(e) e(n)$$

where

$$\hat{\delta}_{\mathfrak{l}}(e) = \frac{1}{|G|} \sum_{m \in G} \delta_{\mathfrak{l}}(m) \overline{e(m)} = \frac{1}{|G|} \overline{e(\mathfrak{l})}.$$

We can extend the function δ to encompass all integers $\mathbb{Z}$, by defining $\delta(m) = 0$ whenever m and q are not relatively prime. Similarly, the characters $e \in \widehat{G}$ can also be extended to cover all integers $\mathbb{Z}$ by defining:

$$\chi(m) := \begin{cases} \chi_L(m) & \text{if } (m,q) = 1 \\ 0 & otherwise. \end{cases} \tag{1.3}$$

With $|G| = \varphi(q)$ and $0 \leq L < q$, we may restate the above results as follows:

Lemma 1.1.5.

$$\delta_{\mathfrak{l}}(m) = \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi(\mathfrak{l})} \chi(m)$$

where the sum is over all Dirichlet characters.

By using the above lemma, we have successfully initiated the first step in the process of proving the theorem, since this lemma shows that

$$\sum_{p \equiv \mathfrak{l}} \frac{1}{p^s} = \sum_{p} \frac{\delta_{\mathfrak{l}}(p)}{p^s}$$

$$= \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi(\mathfrak{l})} \sum_{p} \frac{\chi(p)}{p^s}.$$

Thus it suffices to understand the behavior of $\sum_p \chi(p)/p^s$ as $s \to 1^+$. Indeed, we divide the aforementioned sum into two parts based on whether or not χ is trivial.

$$\sum_{p \equiv \mathfrak{l}} \frac{1}{p^s} = \frac{1}{\varphi(q)} \sum_{p} \frac{\chi_0(p)}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(\mathfrak{l})} \sum_{p} \frac{\chi(p)}{p^s}$$

$$= \frac{1}{\varphi(q)} \sum_{p \nmid q} \frac{1}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(\mathfrak{l})} \sum_{p} \frac{\chi(p)}{p^s}.$$

Since there is a finite numbers of prime numbers that divide q, the statement of Euler's theorem, which asserts that the sum of reciprocals $\sum_p 1/p$ goes to infinity, suggests that the initial sum on the right side also goes to infinity when s approaches 1. These observations demonstrate that Dirichlet's theorem can be derived from the following statement.

Theorem 1.1.6. *If χ is a nontrivial Dirichlet character, then the sum*

$$\sum_p \frac{\chi(p)}{p^s}$$

remains bounded as $s \to 1^+$.

The proof of (1.1.6) necessitates the introduction of L-functions, which we will focus on now. In the next section, we will provide proofs for all the properties of L-functions that we are going to mention here.

Now let us define L-functions.

Definition 1.1.7. *Let χ be a character modulo q. If s is a complex number $Re(s) > 1$, then the sum,*

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

converges absolutely for $Re(s) > 1$. Moreover, the function $L(s,\chi)$ is a holomorphic function in this half plane.

Note that in the case of the trivial character, up to some factors, we get the Riemann zeta function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

which we will state and prove later.

Theorem 1.1.8 (Dirichlet)**.** *If Re(s)>1, then*

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \quad primes} \frac{1}{1-\chi(p)p^{-s}}$$

Proof. See Theorem 2.2.1. □

It is worth noting that Euler was the first to observe the product formula for the zeta function.

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \quad primes} \frac{1}{1-p^{-s}}$$

Assuming the validity of this theorem for the time being, we can formally follow Euler's argument. By taking the logarithm of the product and using the fact that $\log(1+x) =$

$x + O(x^2)$, when x is sufficiently small, we would obtain the following result:

$$log(L(s,\chi)) = -\sum_p log(1 - \frac{\chi(p)}{p^s})$$

$$= -\sum_p \left[\frac{\chi(p)}{p^s} + O(\frac{1}{p^{2s}})\right]$$

$$= \sum_p \frac{\chi(p)}{p^s} + O(1).$$

If $L(1, \chi)$ is finite and non-zero, then $log(L(s, \chi))$ is bounded as $s \to 1^+$, and we can conclude that the sum

$$\sum_p \frac{\chi(p)}{p^s}$$

is bounded as $s \to 1^+$. We now make several observations about the above formal argument.

Since the Dirichlet characters χ take complex values, we will extend the logarithm to complex numbers w of the form

$$w = \frac{1}{1-z} \tag{1.4}$$

where $|z| < 1$. This extension will be accomplished using a power series.

The second aspect we need to address is the interpretation of taking the logarithm of both sides of the product formula. However, the challenge arises when $\chi(p)$ is a complex number since the complex logarithm is not uniquely defined. Specifically, the logarithm of a product is not equal to the sum of logarithms.

Third, it remains to prove that whenever $\chi \neq \chi_0$, then $log(L(s, \chi))$ is bounded as $s \to 1^+$. Since $L(s,\chi)$ is continuous at $s = 1$, it suffices to show that

$$L(1,\chi) \neq 1.$$

This is the non-vanishing we mentioned earlier, which corresponds to the alternating series being non-zero in the previous example.

So we will focus on three main parts,

1) Complex logarithm and infinite product.

2) Study of $L(s,\chi)$.

3) Proof that $L(1,\chi) \neq 0$ if $\chi \neq \chi_0$.

To address the first concern, we introduce two logarithmic functions. The first logarithm, denoted as log_1, is defined for complex numbers of the form $w = 1/(1-z)$ with $|z| < 1$. The second logarithm, denoted as log_2, is defined specifically for the L-function $L(s, \chi)$. For the first logarithm, we define,

$$log_1(\frac{1}{1-z}) = \sum_{k=1}^{\infty} \frac{z^k}{k} \quad for \quad |z| < 1$$

Note that $log_1 w$ is then defined if $Re(w) > 1/2$.

Proposition 1.1.9. *The logarithm function log_1 satisfies the following properties:*

i) If $|z| < 1$, then

$$e^{log_1(\frac{1}{1-z})} = \frac{1}{1-z}$$

ii) If $|z| < 1$, then

$$log_1\left(\frac{1}{1-z}\right) = z + E_1(z)$$

where the error E_1 satisfies $|E_1(z)| \leq |z|^2$ if $|z| < 1/2$

iii) if $|z| < 1/2$, then

$$\left|log_1\left(\frac{1}{1-z}\right)\right| \leq 2|z|$$

Proof. See [5], ch 8, proposition 3.1, p 258. □

By using these outcomes, we can establish a sufficient condition that ensures the convergence of infinite products of complex numbers. The proof of this condition follows the same approach as in the real case, with the distinction that we would need to employ the logarithm log_1.

Proposition 1.1.10. *If $\sum |a_n|$ converges, and $a_n \neq 1$ for all n, then*

$$\prod_n \left(\frac{1}{1-a_n}\right)$$

converges. Moreover, this product is non-zero.

Proof. For n large enough, $|a_n| < 1/2$, so we may assume without loss of generality that this inequality holds for all $n \geq 1$. Then

$$\prod_{n=1}^{N} \left(\frac{1}{1-a_n}\right) = \prod_{n=1}^{N} e^{log_1(\frac{1}{1-a_n})} = e^{\sum_{n=1}^{N} log_1(\frac{1}{1-a_n})}.$$

But we know from the previous proposition that

$$\left|log_1\left(\frac{1}{1-z}\right)\right| \leq 2|z|$$

so the fact that the series $\sum |a_n|$ converges, immediately implies that the limit

$$\lim_{N\to\infty}\sum_{n=1}^{N} log_1\left(\frac{1}{1-a_n}\right) = A$$

exists. Since the exponential function is continuous, we conclude that the product converges to e^A, which is clearly non-zero. □

The subsequent step involves gaining a deeper comprehension of the L-functions. Their behavior as functions of s, particularly near $s = 1$, relies on whether χ is trivial or not. In the case where χ is trivial as we said, $L(s, \chi_0)$ is essentially equal, up to some factors, to the zeta function.

Proposition 1.1.11. *Suppose χ_0 is the trivial Dirichlet character modulo q, and $q = p_1^{a_1}...p_n^{a_N}$ is the prime factorization of q. Then,*

$$L_(s{,}\chi_0) = (1 - p_1^{-s})(1 - p_2^{-s})...(1 - p_N^{-s})\zeta(s).$$

Therefore, $L(s{,}\chi_0) \to \infty$ as $s \to 1^+$

Proof. See proposition (2.2.2). □

The behavior of the remaining L-functions, where $\chi \neq \chi_0$, is more subtle. A notable characteristic is that these functions are now defined and continuous for $s > 0$. In fact, even more can be asserted.

Proposition 1.1.12. *i) The function $L(s{,}\chi)$ is continuously differentiable for $0 < s < \infty$.*

ii) There exist constants c and $c' > 0$ so that

$$L(s{,}\chi) = 1 + O(e^{-cs}) \quad as \quad s \to \infty, and$$

$$L'(s{,}\chi) = O(e^{-c's}) \quad as \quad s \to \infty.$$

Proof. See proposition (2.2.3). □

Based on the information we have gathered thus far about L-functions, we can now proceed to define the logarithm of L-functions. This is accomplished by integrating their logarithmic derivatives. In other words, if χ is a non-trivial Dirichlet character and $s > 1$, we define:

$$log_2(L(s,\chi)) = -\int_s^\infty \frac{L'(t,\chi)}{L(t,\chi)}dt.$$

We know that $L(t,\chi) \neq 0$ for every $t > 1$ since it is given by a product, and the integral is convergent because

$$\frac{L(t,\chi)}{L'(t,\chi)} = O(e^{-ct})$$

which follows from the behavior at infinity of $L(t,\chi)$ and $L'(t,\chi)$ recorded earlier.

The following links the two logarithms.

Proposition 1.1.13. *If $s > 1$, then*

$$e^{log_2(L(s,\chi))} = L(s,\chi).$$

Moreover,

$$log_2(L(s,\chi)) = \sum_p log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right).$$

Proof. See [5] ch 8, proposition 3.6, p 264. □

By combining the progress we have made thus far, we can provide a rigorous interpretation of the earlier formal argument. In fact, the properties of log_1 demonstrate that:

$$\sum_p log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right) = \sum_p \frac{\chi(p)}{p^s} + O(\sum_p \frac{1}{p^{2s}})$$
$$= \sum_p \frac{\chi(p)}{p^s} + O(1).$$

If $L(1,\chi) \neq 0$ for a non-trivial Dirichlet character, then according to its integral representation, $log_2(L(s,\chi))$ remains bounded as s approaches 1 from the right. Consequently, the equality between the logarithms implies that the sum $\sum_p(\chi(p)/p^s)$ remains bounded as s approaches 1 from the right, which is the desired result. Therefore, to complete the proof of Dirichlet's theorem, we need to establish that $L(1,\chi) \neq 0$ when χ is non-trivial. We now turn to a proof of the following deep result:

Theorem 1.1.14. *If $\chi \neq \chi_0$, then $L(1,\chi) \neq 0$.*

The proof is by contradiction, and we use two lemmas.

Lemma 1.1.15. *If $s > 1$, then*

$$\prod_\chi L(s,\chi) \geq 1$$

where the product is taken over all Dirichlet characters. In particular the product is real-valued.

Proof. See lemma (2.2.4). □

Lemma 1.1.16. *The following three properties hold:*

i) If $L(1,\chi) = 0$, then $L(1,\overline{\chi}) = 0$.

ii) If χ is non-trivial and $L(1,\chi) = 0$, then

$$|L(s,\chi)| \leq C|s-1| \quad when \quad 1 \leq s \leq 2.$$

iii) For the trivial Dirichlet character χ_0, we have

$$|L(s,\chi_0)| \leq \frac{C}{|s-1|} \quad when \quad 1 < s \leq 2.$$

Proof. See lemma (2.2.5). □

We can now conclude the proof that $L(1, \chi) \neq 0$ for χ a non-trivial complex Dirichlet character. So by contradiction say $L(1,\chi) = 0$. Then $L(1,\overline{\chi}) = 0$, and since $\chi \neq \chi_0$, there are at least two terms in the product

$$\prod_{\chi} L(s,\chi),$$

that vanish like $|s-1|$ as $s \to 1^+$. Since only the trivial character contributes a term that exhibits growth, and this growth is bounded by $O(1/1-s)$, we can conclude that the product tends to 0 as $s \to 1^+$, contradicting by (1.1.15) and indeed, the proof of Dirichlet's theorem is now complete.

Chapter 2

The Riemann zeta and L-functions of Dirichlet characters

2.1 Bernoulli numbers and polynomials

In this section, we provide an overview of various forms of Bernoulli numbers that will be extensively used.
The Bernoulli numbers are defined by the following generating function of variable t,

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

So the first few B_k's are:

$$B_0 = 1 \quad B_1 = -1/2$$
$$B_2 = 1/6 \quad B_3 = 0, \quad B_4 = -1/30, \quad B_5 = 0 \quad B_6 = 1/42.$$

Again we use a generating function to define Bernoulli polynomials:

$$\frac{te^{tx}}{e^t - 1} = (\sum_{k=0}^{\infty} B_k \frac{t^k}{k!})(\sum_{k=0}^{\infty} x^k \frac{t^k}{k!})$$

$$= \sum_{k=0}^{\infty} B_k(x) \frac{t^k}{k!}$$

where $B_k(x)$ is the kth Bernoulli polynomial. The first few Bernoulli polynomials are:

$$B_0(x) = 1, \quad B_1(x) = x - 1/2$$
$$B_2(x) = x^2 - x + 1/2 \quad B_3(x) = x^3 - 3/2x^2 + 1/2$$

Given a Dirichlet character of conductor d, generalised Bernoulli numbers $B_{k,\chi}$ are defined in a similar way,

$$\sum_{k=0}^{\infty} B_{k,\chi} \frac{t^k}{k!} = \frac{t}{e^{td}-1} \sum_{a=1}^{d} \chi(a) e^{at}.$$

Since we have the expansion

$$\frac{te^{at}}{e^{dt}-1} = \frac{1}{d} + \left(\frac{a}{d} - \frac{1}{2}\right)t$$
$$+\left(\frac{a^2}{d} - a + \frac{d}{6}\right)\frac{t^2}{2} + \left(\frac{a^3}{d} - \frac{3a^2}{2} + \frac{ad}{2}\right)\frac{t^3}{6} + \cdots ,$$

and

$$\sum_{a=0}^{d} \chi(a) = \begin{cases} \phi(d) & \text{if } \chi \neq \chi_0 \\ 0 & \textit{otherwise}, \end{cases} \tag{2.1}$$

it follows that

$$B_{0,\chi} = 0$$
$$B_{1,\chi} = \frac{1}{d} \sum_{a=1}^{d} \chi(a) a$$
$$B_{2,\chi} = \frac{1}{d} \sum_{a=1}^{d} \chi(a) a^2 - \sum_{a=1}^{d} \chi(a) a$$
$$B_{3,\chi} = \frac{1}{d} \sum_{a=1}^{d} \chi(a) a^3 - \frac{3}{2} \sum_{a=1}^{d} \chi(a) a^2 + \frac{1}{d} \sum_{a=1}^{d} \chi(a) a.$$

For a natural number d, let $\phi(d)$ be the number of integers from 1 to d which are relatively prime to d.
A similar formula for $B_{n,\chi}$

$$B_{n,\chi} = d^{n-1} \sum_{a=1}^{d} \chi(a) B_n(a/d)$$

where $B_n(x)$ is the Bernoulli polynomial.

2.2 Properties of Riemann zeta and L-functions- The Mellin transform

Let's proceed with proving the properties of L-functions that were used in the first chapter to establish Dirichlet's theorem.

Theorem 2.2.1 (Dirichlet)**.** *If Re(s)>1, then*

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p\ primes} \frac{1}{1-\chi(p)p^{-s}}$$

and the similar argument by Euler for the zeta function:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\ primes} \frac{1}{1-p^{-s}}$$

Proof. For simplicity of notation, let L denote the left-hand side of the above equation and define

$$S_N = \sum_{n\leq N} \chi(n)n^{-s}$$

and

$$\Pi_N = \prod_{p\leq N} \frac{1}{1-\chi(p)p^{-s}}.$$

The infinite product $\Pi = \lim_{N\to\infty} \prod_N = \prod_p 1/(1-\chi(p)p^{-s})$ converges by (1.1.10). Indeed, if we set $a_n = \chi(p_n)p_n^{-s}$, where p_n is the nth prime, we note that if $s > 1$, then $\sum |a_n| < \infty$.
Also, define

$$\Pi_{N,M} = \prod_{p\leq N} \left(1 + \frac{\chi(p)}{p^s} + ... + \frac{\chi(p^M)}{p^{Ms}}\right).$$

Now, fix $\varepsilon > 0$ and choose N so large that

$$|S_N - L| < \varepsilon \quad and \quad |\Pi_N - \Pi| < \varepsilon.$$

We can next select M large enough so that

$$|S_N - \Pi_{N,M}| < \varepsilon \quad and \quad |\Pi_{N,M} - \Pi_N| < \varepsilon.$$

To see the first inequality, one uses the fundamental theorem of arithmetic and the fact that the Dirichlet characters are multiplicative. The second inequality follows merely because each series $\sum_{n=1}^{\infty} \chi(p^n)/p^{ns}$ converges.
Therefore,

$$|L - \Pi| \leq |L - S_N| + |S_N - \Pi_{N,M}| + |\Pi_{N,M} - \Pi_N| + |\Pi_N - \Pi| < 4\varepsilon,$$

as was to be shown. □

Proposition 2.2.2. *Suppose χ_0 is the trivial Dirichlet character modulo q, and $q =$*

$p_1^{a_1}...p_n^{a_N}$ *is the prime factorization of* q*. Then,*

$$L(s,\chi_0) = (1-p_1^{-s})(1-p_2^{-s})...(1-p_N^{-s})\zeta(s).$$

Therefore, $L(s,\chi_0) \to \infty$ *as* $s \to 1^+$

Proof. By the previous theorem,

$$L(s,\chi_0) = \prod_{p \text{ primes}} \frac{1}{1-\chi_0(p)p^{-s}}$$

$$= \prod_{p\nmid q} \frac{1}{1-p^{-s}}$$

$$= \prod_{p|q}(1-p^{-s}) \prod_{p \text{ primes}} (1-p^{-s})^{-1}$$

$$= \prod_{p|q}(1-p^{-s})\zeta(s) = (1-p_1^{-s})(1-p_2^{-s})...(1-p_N^{-s})\zeta(s).$$

The second statement follows because $\zeta(s) \to \infty$ as $s \to 1^+$. □

Proposition 2.2.3. *If* χ *is a non-trivial Dirichlet character, then the associated L-function converge for* $s > 0$*. Moreover,*

i) The function $L(s,\chi)$ *is continuously differentiable for* $0 < s < \infty$*.*

ii)There exist constants c *and* $c' > 0$ *so that*

$$L(s,\chi) = 1 + O(e^{-cs}) \quad as \quad s \to \infty, and$$

$$L'(s,\chi) = O(e^{-c's}) \quad as \quad s \to \infty$$

Proof. For the first two statements see [5] proposition 3.3. For ii), by using triangular inequality, observe that for all s large,

$$|L(s,\chi) - 1| \leq 2^{-s} \sum_{n=2}^{\infty} \frac{1}{n^s}$$

$$\leq 2^{-s} O(1),$$

and by taking $c = log2$, we get that $L(s,\chi) = 1 + O(e^{-cs})$. A similar argument also shows that $L'(s,\chi) = O(e^{-c's})$ as $s \to \infty$ with in fact $c = c'$. □

Lemma 2.2.4. *If* $s > 1$*, then*

$$\prod_{\chi} L(s,\chi) \geq 1$$

where the product is taken over all Dirichlet characters. In particular the product is real-valued.

Proof. By employing the second point stated in (1.1.13):

$$L(s,\chi) = \exp\left(\sum_p log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right).$$

Hence,

$$\begin{aligned}\prod_\chi L(s,\chi) &= \exp\left(\sum_\chi \sum_p log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right) \\ &= \exp\left(\sum_\chi \sum_p \sum_{k=1}^{\infty} \frac{1}{k}\frac{\chi(p^k)}{p^{-sk}}\right) \\ &= \exp\left(\sum_p \sum_{k=1} \sum_\chi \frac{1}{k}\frac{\chi(p^k)}{p^{-sk}}\right).\end{aligned}$$

Because of (1.1.5) (with $\mathfrak{l} = 1$) we have $\sum_\chi \chi(p^k) = \varphi(q)\delta_1(p^k)$, and hence

$$\prod_\chi L(s,\chi) = \exp\left(\varphi(q) \sum_p \sum_{k=1}^{\infty} \frac{1}{k}\frac{\delta_1(p^k)}{p^{-sk}}\right) \geq 1,$$

since the term in exponent is non-negative. □

Lemma 2.2.5. *The following three properties hold:*

i) If $L(1,\chi) = 0$*, then* $L(1,\overline{\chi}) = 0$.

ii) If χ *is non-trivial and* $L(1,\chi) = 0$*, then*

$$|L(s,\chi)| \leq C|s-1| \quad \textit{when} \quad 1 \leq s \leq 2.$$

iii) For the trivial Dirichlet character χ_0*, we have*

$$|L(s,\chi_0)| \leq \frac{C}{|s-1|} \quad \textit{when} \quad 1 < s \leq 2.$$

Proof. The first statement is immediate because $L(1,\overline{\chi}) = \overline{L(1,\chi)}$.

The second statement follows from the mean-value theorem. Since $L(s,\chi)$ is continuously differentiable for $s > 0$ when χ is non-trivial. So we have:

$$|L(s,\chi) - L(1,\chi)| < |s-1|C$$

for some constant C. Since $L(1,\chi) = 0$ we get the desired bound. Finally, the last statement follows because by (2.2.2),

$$L(s,\chi_0) = (1 - p_1^{-s})(1 - p_2^{-s})...(1 - p_N^{-s})\zeta(s)$$

and ζ satisfies the similar estimate as in iii) since

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \leq 1 + \sum_{n=2}^{\infty} \int_{n-1}^{n} \frac{dx}{x^s}$$
$$= 1 + \int_{1}^{\infty} \frac{dx}{x^s},$$

and therefore,

$$\zeta(s) \leq 1 + \frac{1}{s-1} \quad for \quad s > 1$$

□

Let's now start the topic of the Mellin transform. The Mellin transform is a mathematical operation that extends the concept of the Fourier transform to a more general setting. It involves transforming a function defined on the positive real numbers into a new function defined on the complex plane.

Definition 2.2.6. *Let $f : \mathbb{R}_{\geq 0} \to \mathbb{C}$ be a continuous function of rapid decay (i.e. $|f(t)| \ll t^{-N}, \forall N \geq 0$). Then the Mellin transform of f is the function:*

$$F(s) = M[f(x)](s) = \int_0^{\infty} x^{s-1} f(x) dx$$

where s is a complex variable and the integral is taken over the positive real line.

The Mellin transform provides a useful tool for studying the properties of functions, especially those defined on the positive real line. It allows us to analyze the behavior of a function in terms of its transform, and vice versa.
In relation to the Riemann zeta function and L-functions, the Mellin transform is used to obtain their functional equations. These equations establish connections between the function values at different complex points and often exhibit symmetries, which aid in comprehending the characteristics and properties of these functions.
For example, the functional equation of the Riemann zeta function relates its values at s and $1 - s$, where s is a complex variable. It can be obtained by using the Mellin transform techniques and plays a crucial role in understanding the behavior of the zeta function and its connection to prime numbers.
As an example, let $f = 1/(e^x - 1)$ and let $Re(s) > 1$,

$$M[f](s) = \int_0^{\infty} \frac{1}{e^x - 1} x^{s-1} dx$$

$$= \int_0^\infty \sum_{n=1}^\infty e^{-nx} x^{s-1} dx$$
$$= \sum_{n=1}^\infty \int_0^\infty e^{-nx} x^{s-1} dx$$
$$= \sum_{n=1}^\infty \int_0^\infty e^{-t} (\frac{t}{n})^{s-1} \frac{dt}{n},$$

by change of variable $nx = t$

$$= \sum_{n=1}^\infty n^{-s} \int_0^\infty e^{-t} t^{s-1} dt = \zeta(s)\Gamma(s).$$

So, we have:

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{1}{e^x - 1} x^{s-1} dx$$

where

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$$

is the Mellin transform of the function e^{-t}, called Gamma function.

2.3 Functional equations and Analytic continuation

First, we will present the functional equations for the Riemann zeta function and L-functions. These equations establish relationships between the function values at different points in the complex plane and help us understand their properties.
Next, we can use these functional equations to extend the Zeta, respectively L-functions to the entire complex plane. This is called analytic continuation. By applying analytic continuation, we can define the values of these functions beyond their original regions of definition and explore their behavior in the broader context of the complex plane.

Theorem 2.3.1. *Let*

$$\Lambda(s) = \pi^{-s/2} \Gamma(\frac{s}{2}) \zeta(s).$$

Then $\Lambda(s)$ is invariant under replacing s by $1-s$:

$$\Lambda(s) = \Lambda(1-s) \ \forall s \text{ with } Re(s) > 1.$$

That is , $\zeta(s)$ satisfies the functional equation

$$\pi^{-s/2} \Gamma(\frac{s}{2}) \zeta(s) = \pi^{-(1-s)/2} \Gamma(\frac{1-s}{2}).$$

We will present Riemann's proof of (2.3.1), which can be extended to various other cases. The proof makes use of the theta function $\theta : \mathbb{R}_{\geq 0} \to \mathbb{C}$ given by:

$$\theta(t) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t}.$$

Our intention is to perceive this function in the form of a Mellin transform. In the proof of the theorem, the fundamental idea is that $\Lambda(s)$ essentially represents the Mellin transform of θ. The transformation properties of θ are then reflected in the functional equation of Λ through the Mellin transform. An immediate problem with this idea is that θ is not a function of rapid decay, since the constant term in the series is not of rapid decay. We then replace θ by:

$$\omega(t) = \sum_{n=1}^{\infty} e^{-\pi n^2 t}$$

which is related to θ by:

$$\theta(t) = 1 + 2\omega(t), \quad \omega(t) = \frac{\theta(t) - 1}{2}.$$

The function $\omega(t)$ is of rapid decay, and therefore we can take its Mellin transform.

Theorem 2.3.2.

$$M[\omega](s) = \pi^{-s}\Gamma(s)\zeta(2s) = \Lambda(2s)$$

Proof. By definition we have:

$$M[\omega](s) = \int_0^{\infty} \omega(t) t^s \frac{dt}{t} = \int_0^{\infty} \left(\sum_{n=1}^{\infty} e^{-\pi n^2 t} \right) t^s \frac{dt}{t}.$$

Since all the terms in the infinite series have rapid decay, we can interchange the order of integration,

$$\int_0^{\infty} \left(\sum_{n=1}^{\infty} e^{-\pi n^2 t} \right) t^s \frac{dt}{t} = \sum_{n=1}^{\infty} \int_0^{\infty} e^{-\pi n^2 t} t^s \frac{dt}{t}.$$

By changing the variable $u = \pi n^2 t$ we obtain,

$$\sum_{n=1}^{\infty} \int_0^{\infty} e^{-\pi n^2 t} t^s \frac{dt}{t} = \sum_{n=1}^{\infty} \int_0^{\infty} e^{-u} \pi^{-s} n^{-2s} u^s \frac{du}{u}$$

$$= \pi^{-s} \left(\int_0^{\infty} e^{-u} u^s \frac{du}{u} \right) \left(\sum_{n=1}^{\infty} n^{-2s} \right)$$

$$= \pi^{-s}\Gamma(s)\zeta(2s).$$

□

The reason for expressing $\Lambda(s)$ as the Mellin transform of $\omega(t)$ is that ω possesses favorable transformation properties derived from those of θ.

Theorem 2.3.3. *(Functional equation for $\theta(t)$) For all $t > 0$*

$$\theta(1/t) = \sqrt{t}.\theta(t)$$

Proof. See [6], ch 4, theorem 2.4, p 118. □

Theorem 2.3.4. *(Functional equation for $\omega(t)$) For all $t > 0$*

$$\omega(1/t) = \sqrt{t}.\omega(t) + \sqrt{t}/2 - 1/2$$

Proof.

$$\begin{aligned}
\omega(1/t) &= \frac{\theta(1/t) - 1}{2} \\
&= \frac{\sqrt{t}.\theta(t) - 1}{2} \\
&= \frac{\sqrt{t}.(1 + 2\omega(t)) - 1}{2} \\
&= \sqrt{t}.\omega(t) + \sqrt{t}/2 - 1/2.
\end{aligned}$$

□

At this point, we are prepared to demonstrate the functional equation of $\zeta(s)$.

Proof. (Theorem (2.3.1)) By (2.3.2), we know that

$$\Lambda(s) = M[\omega](s/2) = \int_0^\infty \omega(t)t^{s/2}\frac{dt}{t}.$$

The convergence of this integral for all s near ∞ is guaranteed due to the rapid decay of ω. However, the convergence at 0 will be determined by the growth behavior of $\omega(t)$ near 0. Now, let's proceed with the proof,

$$\omega(t) \approx C.t^{-1/2} \quad as \quad t \to 0.$$

Hence, the integral converges as long as the real part of s is greater than 1. It is important to note that Λ has a pole at $s = 1$ originating from ζ, which implies that we cannot extend the convergence beyond that point solely based on the definition.
Next, we break down the integral into two pieces:

$$\int_0^\infty \omega(t)t^{s/2}\frac{dt}{t} = \int_0^1 \omega(t)t^{s/2}\frac{dt}{t} + \int_1^\infty \omega(t)t^{s/2}\frac{dt}{t}. \tag{2.2}$$

It is worth noting that the second integral converges for all s in the complex plane,

whereas the convergence of the first integral is limited to cases where the real part of s is greater than 1. Therefore, our goal is to transform the first integral into a form resembling the second integral, that is, with limits from 1 to ∞ and with ω included in the integrand.
Certainly, this can be achieved by making the substitution $t \to 1/t$ and using the functional equation for ω:

$$\int_0^1 \omega(t)t^{s/2}\frac{dt}{t} = \int_1^\infty \omega(1/t)t^{-s/2}\frac{dt}{t}$$

$$= \int_1^\infty \left(\sqrt{t}.\omega(t) + \sqrt{t}/2 - 1/2\right)t^{-s/2}\frac{dt}{t}$$

and substituting in (2.2) we have,

$$\Lambda(s) = \int_0^\infty \omega(t)t^{s/2}\frac{dt}{t} = \int_1^\infty \omega(t)t^{\frac{1-s}{2}}\frac{dt}{t} + \int_1^\infty \omega(t)t^{s/2}\frac{dt}{t}t + \int_1^\infty t^{\frac{-1-s}{2}}dt - \frac{1}{2}\int_1^\infty t^{-1-s/2}dt$$

$$= \int_1^\infty \omega(t)t^{\frac{1-s}{2}}\frac{dt}{t} + \int_1^\infty \omega(t)t^{s/2}\frac{dt}{t} - \frac{1}{1-s} - \frac{1}{s}.$$

From this expression, we can deduce that $\Lambda(s)$ can be analytically extended to the entire complex plane, $\mathbb{C}$ as a meromorphic function with simple poles at $s = 0$ and $s = 1$. Additionally, we see that Λ is invariant under replacing s by $1 - s$:

$$\Lambda(s) = \Lambda(1 - s).$$

Consequently, $\zeta(s)$ has a pole at $s = 1$ and it has the desired functional equation. □

Next, we will proceed with deriving the functional equation for L-functions which we follow Iwasawa's work in [2].

Theorem 2.3.5. *The functional equation of $L(s,\chi)$ is:*

$$L(s,\chi) = \frac{\tau(\chi)}{2i^\delta}(\frac{2\pi}{d})^s \frac{L(1-s,\overline{\chi})}{\Gamma(s)cos(\frac{\pi(s-\delta)}{2})}$$

Proof. Let χ be a character with conductor d and let

$$F(z) = \sum_{a=1}^{d} \frac{\chi(a)ze^{az}}{e^{dz} - 1}$$

$$G(z) = \sum_{a=1}^{d} \frac{\chi(a)e^{-az}}{1 - e^{-dz}}$$

And $F(z)$ is the generating function that defines the "generalized Bernoulli numbers"

$$F(z) = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}$$

Both F and G are meromorphic functions on the z-plane with possible poles at $z = 2\pi ik/d$, $k \in \mathbb{Z}$ and

$$F(-z) = zG(z)$$

$$G(t) = \sum_{n=1}^{\infty} \chi(n) e^{-nt}$$

for $t > 0$.
Fix a real number ε, $0 < \varepsilon < 2\pi/d$ and define a path C_ε on $\mathbb{C}$ by

$$C_\varepsilon = (-\infty, -\varepsilon) + K_\varepsilon + (-\varepsilon, -\infty)$$

Where K_ε denotes the circle $\{z \in \mathbb{C} \mid |z| = \varepsilon\}$. Let

$$H(s) = \int_{C_\varepsilon} F(z) z^{s-1} \frac{dz}{z}$$

Where $z^{s-1} = e^{(s-1)logz}$ with the principal value of $\log z$:

$$\log z = logt - \pi i \quad \text{for} \quad z = -t \in (-\infty, -\varepsilon)$$
$$\log z = logt + \pi i \quad \text{for} \quad z = -t \in (-\varepsilon, \infty).$$

The integral converges absolutely for every complex number s so that $H(s)$ defines an entire function on the $\mathbb{C}$; it is obvious that $H(s)$ does not depend upon the choice of $0 < \varepsilon < 2\pi/d$. By the change of variable from z to $-z$, we get

$$H(s) = \int_{-C_\varepsilon} F(-z)(-z)^{s-1} \frac{dz}{z}$$

$$= -e^{-\pi is} \int_{-C_\varepsilon} G(z) z^{s-1}\, dz$$

with $z^{s-1} = e^{(s-1)logz}$, $0 \le Im(logz) \le 2\pi$. Clearly

$$\int_{-C_\varepsilon} G(z) z^{s-1}\, dz = \int_{K_\varepsilon} G(z) z^{s-1}\, dz + (e^{2\pi is} - 1) \int_{\varepsilon}^{\infty} G(t) t^{s-1}\, dt$$

Let $Re(s) > 1$. Then

$$\int_{K_\varepsilon} G(z)z^{s-1}\,dz \longrightarrow 0$$

as $\varepsilon \longrightarrow 0$. Therefore, for $Re(s) > 1$,

$$H(s) = -(e^{\pi is} - e^{-\pi is})\int_0^\infty G(t)t^{s-1}\,dt$$

where $\int_0^\infty G(t)t^{s-1}\,dt$ is the Mellin transform of $G(t)$ and,

$$M[G](s) = \int_0^\infty G(t)t^{s-1}\,dt = \int_0^\infty \sum_{n=1}^{\infty} \chi(n)e^{-nt}t^{s-1}\,dt$$

$$= \sum_{n=1}^{\infty} \chi(n)\int_0^\infty e^{-nt}t^{s-1}\,dt$$

$$= \sum_{n=1}^{\infty} \chi(n)n^{-s}\Gamma(s) = L(s,\chi)\Gamma(s)$$

It follows that for s with $Re(s) > 1$,

$$H(s) = -2isin(\pi s)\Gamma(s)L(s,\chi)$$

$$= -\frac{2\pi i}{\Gamma(1-s)}L(s,\chi)$$

namely,

$$L(s,\chi) = -\frac{1}{2\pi i}\Gamma(1-s)H(s). \tag{2.3}$$

Just keep in mind that with n an integer, $n \geq 1$, and let $s = 1 - n$ in (2.3), we also obtain that

$$-\frac{L(1-n,\chi)}{\Gamma(n)} = \frac{1}{2\pi i}\int_C F(z)z^{-n}\,\frac{dz}{z} = \frac{1}{2\pi i}\int_{K_\varepsilon} F(z)z^{-n-1}\,dz = res_0(F(z)z^{-n-1}). \tag{2.4}$$

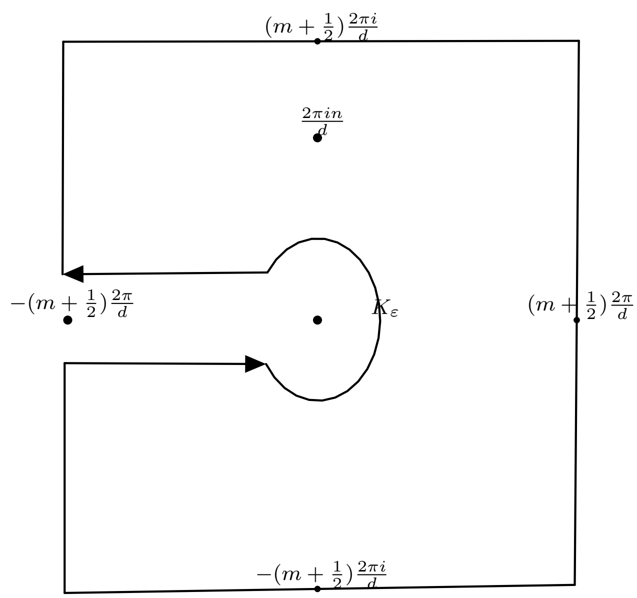
In Section (2.4), we will use this equality when expressing the special values of L-functions. Note that we are currently at a midway point in the computation of the functional equation for L-functions and the process of achieving analytic continuation. By employing the equation (2.3), it becomes evident that $L(s,\chi)$ can be analytically continued to a holomorphic function across the entire complex plane for non-trivial characters. Since $L(s,\chi)$ is holomorphic for $Re(s) > 1$ and $\Gamma(1-s)$ only has poles at

$s = 1, 2, 3, ...,$ the only possible location for a pole of $L(s,\chi)$ is at $s = 1$. However, it can be easily observed that for trivial character,

$$H(1) = \int_C F(z)\frac{dz}{z} = \int_{K_\varepsilon} F(z)\frac{dz}{z} = 2\pi i$$

otherwise it is zero.
Hence $L(s, \chi_0)$ has a simple pole with residue 1 at $s = 1$, and $L(s,\chi)$ for $\chi \neq \chi_0$ is also holomrphic at $s = 1$.

Now, for each integer $k \geq 1$, let D_m denote the path on $\mathbb{C}$ described below:



By the residue theorem,

$$\int_{D_k} F(z) z^{s-1}\frac{dz}{z} = -2\pi i \sum_{n=-k, n\neq 0}^{k} R_n$$

where R_n denotes the residue of the integrand at $z = 2\pi i n/d$. However, $|F(z)z^{-1}|$ is bounded on the outer square of the path D_k for all $k \geq 1$. Hence, if $Re(s) > 1$, then the integral over the outer square of D_k tends to zero as $k \longrightarrow \infty$. Therefore we obtain

$$H(s) = \int_C F(z)z^{s-1}\,\frac{dz}{z} = -2\pi i \sum_{n=-\infty, n\neq 0}^{\infty} R_n,$$

for $Re(s) > 1$.
Let $n \geq 1$. Then

$$R_n = \frac{1}{d}\sum_{a=1}^{d} \chi(a) e^{\frac{2\pi i a n}{d}} e^{s-1}(log(\frac{2\pi n}{d} + \frac{\pi i}{2}))$$
$$= \frac{1}{d}\overline{\chi}(n)\tau(\chi)(\frac{2\pi n}{d})^{s-1}e^{(s-1)\frac{\pi i}{2}}$$

with the Gaussian sum $\tau(\chi)$ defined as:

$$\tau(\chi) = \sum_{a=1}^{d} \chi(a) e^{\frac{2\pi i a}{d}}.$$

Similarly,

$$R_{-n} = \frac{1}{d}\chi(-1)\overline{\chi}(n)\tau(\chi)(\frac{2\pi n}{d})^{s-1}e^{-(s-1)\frac{\pi i}{2}}.$$

Hence it follows from the above that

$$H(s) = -\frac{2\pi i}{d}\tau(\chi)(\frac{2\pi}{d})^{s-1}(e^{(s-1)\frac{\pi i}{2}} + \chi(-1)e^{-(s-1)\frac{\pi i}{2}})\sum_{n=1}^{\infty}\overline{\chi}(n)n^{s-1}$$
$$= -\tau(\chi)(\frac{2\pi}{d})^{s}(e^{\pi i\frac{s}{2}} - \chi(-1)e^{-\pi i\frac{s}{2}})L(1-s,\overline{\chi}) \quad (2.5)$$

for $Re(s) < 0$. On the other hand,

$$L(s,\chi) = -\frac{1}{2\pi i}\Gamma(1-s)H(s).$$

By putting together (2.5) and this equation, we obtain the functional equation for $L(s,\chi)$.

$$L(s,\chi) = \frac{\tau(\chi)}{2i^{\delta}}(\frac{2\pi}{d})^{s}\frac{L(1-s,\overline{\chi})}{\Gamma(s)cos(\frac{\pi(s-\delta)}{2})}.$$

□

2.4 Special values

Initially we derive the formula :

$$\zeta(2k) = (-1)^k \pi^{2k}\frac{2^{2k-1}}{(2k-1)!}\left(-\frac{B_{2k}}{2k}\right) \text{ for } k = 1,2,3,.... \quad (2.6)$$

Recall the definition of the "hyperbolic *sine*," abbreviated

$$sinh(x) = \frac{e^x - e^{-x}}{2}.$$

It is equal to its Taylor series

$$sinhx = x + \frac{x^3}{3!} + \frac{x^5}{5!} + ... + \frac{x^{2k+1}}{(2k+)!} + ...,$$

obtained by averaging the series for e^x and e^{-x}. First, we prove the following proposition.

Proposition 2.4.1. *For all numbers x, the infinite product*

$$\pi x \prod_{n=1}^{\infty} \left(1 + \frac{x^2}{n^2}\right)$$

converges and equals $sinh(\pi x)$.

Proof. By using logarithm test, we obtain

$$\sum_{n=1}^{\infty} |log\left(1 + \frac{x^2}{n^2}\right)| \leq \sum_{n=1}^{\infty} \frac{x^2}{n^2} < \infty$$

□

For the equality we need the following lemma.

Lemma 2.4.2. *Let $n = 2k + 1$ be a positive odd integer. Then we can write*

$$sin(nx) = P_n(sinx)$$

$$cos(nx) = cosxQ_{n-1}(sinx)$$

where P_n (respectively Q_{n-1}) is a polynomial of degree at most n (respectively $n - 1$) with integer coefficients.

Proof. We use induction on k. The lemma is trivial for $k = 0$. Suppose it holds for $k - 1$. Then

$$\begin{aligned} sin[(2k+1)x] &= sin[(2k-1)x + 2x] \\ &= sin[(2k-1)x]cos(2x) + cos[(2k-1)x]sin(2x) \\ &= P_{2k-1}(sinx)(1 - 2sin^2x) \\ &+ cosxQ_{2k-2}(sinx)2sin(x)cos(x), \end{aligned}$$

which is of the required form $P_{2k+1}(sinx)$. The proof of $cos(2k+1)x = cosxQ_{2k}(sinx)$ is completely similar. □

Let's go back to the proof of the proposition. It's important to observe that when we substitute x with 0 in the equation $sin(nx) = P_n(sinx)$, we discover that the polynomial P_n has a zero constant term. Following that, we differentiate both sides of the equation $sin(nx) = P_n(sinx)$ with respect to x.

$$ncos(nx) = P_n'(sinx)cosx.$$

Setting $x = 0$ here gives: $n = P_n'(0)$, i.e., the first coefficient of P_n is n. Thus,

$$\frac{sin(nx)}{nsin(x)} = \widetilde{P}_{2k}(sinx) = 1 + a_1 sinx + a_2 sin^2x + ...$$

where the a_i are rational numbers. Please observe that when x takes values such as $\pm(\pi/n), ..., \pm(k\pi/n)$, the expression on the left side becomes zero. However, since the $2k$ values of namely $y = \pm sin(\pi/n), \pm sin(2\pi/n), ..., \pm sin(k\pi/n)$, represent different numbers where the polynomial $\widetilde{P}_{2k}$ has a degree of $2k$ and a constant term of 1, it is necessary to conclude that:

$$\widetilde{P}_{2k}(y) = \left(1 - \frac{y}{sin(\pi/n)}\right)\left(1 - \frac{y}{-sin(\pi/n)}\right)\left(1 - \frac{y}{sin(2\pi/n)}\right)$$
$$\left(1 - \frac{y}{-sin(2\pi/n)}\right)...\left(1 - \frac{y}{sin(k\pi/n)}\right)\left(1 - \frac{y}{-sin(k\pi/n)}\right)$$
$$= \prod_{r=1}^{k}\left(1 - \frac{y^2}{sin^2 r\pi/n}\right).$$

Thus,

$$\frac{sin(nx)}{nsin(x)} = \widetilde{P}_{2k}(sinx) = \prod_{r=1}^{k}\left(1 - \frac{sin^2x}{sin^2 r\pi/n}\right).$$

Replacing x by $\pi x/n$ gives:

$$\frac{sin(\pi x)}{n.sin(\pi x/n)} = \prod_{r=1}^{k}\left(1 - \frac{sin^2\pi x/n}{sin^2 r\pi/n}\right).$$

Now take the limit of both sides as $n = 2k + 1 \to \infty$. The left-hand side approaches $(sin\pi x)/\pi x$. For r small relative to n the rth term in the product approaches $1 - ((\pi x/n)/(\pi r/n))^2 = 1 - (x^2/r^2)$. It then follows that the product converges to $\prod_{r=1}^{\infty}(1 - (x^2/r^2))$. We conclude that:

$$\prod_{n=1}^{\infty}\left(1 - \frac{x^2}{n^2}\right) = \frac{sin(\pi x)}{\pi x} = 1 - \frac{\pi^2x^2}{3!} + \frac{\pi^4x^4}{5!} - \frac{\pi^6x^6}{7!} + \frac{\pi^8x^x}{9!} - ...,$$

using the Taylor series for the sine. But

$$\frac{sin(\pi x)}{\pi x} = 1 + \frac{\pi^2 x^2}{3!} + \frac{\pi^4 x^4}{5!} + \frac{\pi^6 x^6}{7!} + \frac{\pi^8 x^x}{9!} + ...$$

When we expand the infinite product for $sin(\pi x)/(\pi x)$, we observe that a negative sign appears exactly in those terms that contain an odd number of x^2/n^2 terms. In other words, the terms in the Taylor series for $sin(\pi x)/(\pi x)$ that have a negative sign correspond to these terms. Consequently, by changing the sign in the infinite product, we effectively transform all the minus signs on the right side of the equation into plus signs, thus obtaining the intended product expansion as stated in the proposition.

Theorem 2.4.3.

$$\zeta(2k) = (-1)^k \pi^{2k} \frac{2^{2k-1}}{(2k-1)!}\left(-\frac{B_{2k}}{2k}\right).$$

Proof. First take the logarithm of both sides of

$$sinh(\pi x) = \pi x \prod_{n=1}^{\infty} 1 + \frac{x^2}{n^2} \quad for\ x > 0.$$

On the left we get

$$log[sinh(\pi x)] = log[(e^{\pi x} - e^{-\pi x})/2] = log[(e^{\pi x}/2)(1 - e^{-2\pi x})]$$

$$= log(1 - e^{-2\pi x}) + \pi x - log2.$$

On the right we get (for $0 < x < 1$)

$$log\pi + logx + \sum_{n=1}^{\infty} log(1 + x^2/n^2) = log\pi + logx + \sum_{n=1}^{\infty}\sum_{k=1}^{\infty}(-1)^{k+1}\frac{x^{2k}}{kn^{2k}}$$

by the Taylor series for $log(l + x)$. Since this double series is absolutely convergent for $0 < x < 1$, we can interchange the order of summation and obtain the equality:

$$log(1 - e^{-2\pi x}) + \pi x - log2 = log\pi + logx + \sum_{k=1}^{\infty}\left[(-1)^{k+1}\frac{x^{2k}}{k}\sum_{n=1}^{\infty}\frac{1}{n^{2k}}\right]$$

$$= log\pi + logx + \sum_{k=1}^{\infty}\left[(-1)^{k+1}\frac{x^{2k}}{k}\zeta(2k)\right].$$

We now take the derivative of both sides with respect to x. On the right we may differentiate term-by-term, since the resulting series is uniformly convergent in $0 < x < 1 - \varepsilon$ for any $\varepsilon > 0$. Thus,

$$\frac{2\pi e^{-2\pi x}}{1 - e^{-2\pi x}} + \pi = \frac{1}{x} + 2\sum_{k=1}^{\infty}(-1)^{k+1}x^{2k-1}\zeta(2k).$$

Multiplying through by x and then substituting $x/2$ for x gives:

$$\frac{\pi x}{e^{\pi x}-1}+\frac{\pi x}{2}=1+\sum_{k=1}^{\infty}\frac{(-1)^{k+1}\zeta(2k)}{2^{2k-1}}x^{2k}.$$

So we have

$$(\pi x)/2+\sum_{k=0}^{\infty}B_k(\pi x)^k/k!=1+\sum_{k=1}^{\infty}\frac{(-1)^{k+1}\zeta(2k)}{2^{2k-1}}x^{2k}.$$

and by comparing coefficients of even powers of x gives:

$$\pi^{2k}B_{2k}/2k!=((-1)^{k+1}/2^{2k-1})\zeta(2k)$$

which gives us the theorem. □

Theorem 2.4.4.

$$\zeta(1-k)=-\frac{B_k}{k},\quad k\geq 2$$

Proof. Through using the properties of the gamma function (Γ) namely,

$$\Gamma(s)\Gamma(1-s)=\frac{\pi}{sin(\pi s)}$$

by restructuring the functional equation, we have

$$\zeta(1-s)=\frac{(2\pi)^s}{2\Gamma(s)cos(\frac{\pi s}{2})}\zeta(s)$$

for $s=2k$ and integer k we observe that:

$$\zeta(1-2k)=\frac{2(2k-1)!cos(\pi k)}{(2\pi)^{2k}}\zeta(2k)$$

$$=\frac{2(2k-1)!cos(\pi k)}{(2\pi)^{2k}}\times\frac{(-1)^{2k}2^{2k-1}(\pi)^{2k}}{(2k-1)!}.\left(-\frac{B_{2k}}{2k}\right)\quad by\ (2.4.3)$$

$$=-\frac{B_{2k}}{2k}.$$

On the other hand, the right-hand side of the functional equation vanishes if s is an odd integer higher than 1, because $cos(\pi s/2)=0$. $\zeta(1-s)$ therefore vanishes and so $\zeta(1-k)=-\frac{B_k}{k}$. □

The term $-B_k/k$ is the term that we wish to interpolate when we are constructing the p-adic zeta function in chapter 4.

Finally, in section (2.3), in the proof of the functional equation of the L-function, it was shown that

$$-\frac{L(1-n,\chi)}{\Gamma(n)} = \frac{1}{2\pi i}\int_C F(z)z^{-n}\,\frac{dz}{z} = \frac{1}{2\pi i}\int_{K_\varepsilon} F(z)z^{-n-1}\,dz = res_0(F(z)z^{-n-1}).$$

Moreover, $res_0(F(z)z^{-n-1}) = B_{n,\chi}/n!$. Then we observe that

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}, \tag{2.7}$$

for $n \geq 2$.

Chapter 3

p-Adic Analysis

3.1 p-Adic numbers

To introduce p-adic numbers, it is necessary to define a norm on the field of rational numbers.
Let us fix a prime integer p. We can define the function $ord_p : \mathbb{Z} \to \mathbb{Z}$, where $ord_p(a)$ represents the highest power of the prime number p that divides the non-zero integer a, called the p-adic valuation of a. This function counts the exponent of p in the prime factorization of a.
To extend this function to the rational numbers $\mathbb{Q}$, we define $ord_p(n/m) = ord_p(n) - ord_p(m)$ for any non-zero rational number n/m, where n and m are integers and $m \neq 0$. This definition takes into account the cancellation of common factors between the numerator and denominator when expressing a rational number in lowest terms. The ord_p satisfies the following properties for x,$y \in \mathbb{Q}$:
1)$ord_p(xy) = ord_p(x) + ord_p(y)$.
2)$ord_p(x + y) \geq min\{ord_p(x),ord_p(y)\}$.
3)Moreover, if $ord_p(x) \neq ord_p(y)$, then $ord_p(x + y) = min\{ord_p(x),ord_p(y)\}$

By extending the function in this way, we can determine the p-adic valuation or p-adic order of rational numbers, which provides a measure of divisibility by the prime number p.
Then the following function makes a norm on $\mathbb{Q}$.

$$|x|_p = \begin{cases} p^{-ord_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases} \tag{3.1}$$

Proposition 3.1.1. $|.|_p$ *is a norm on* $\mathbb{Q}$.

Proof. It follows directly from the properties of the norm namely,
1) $|x + y|_p \leq |x|_p + |y|_p$ for $x, y \in \mathbb{Q}$.

2) $|x|_p = 0$ iff $x = 0$.
3)$|x.y|_p = |x|_p|y|_p$ □

Observe that the absolute value $|.|_p$ is a non-Archimedean norm defined on the field of rational numbers $\mathbb{Q}$. To put it differently, a non-Archimedean norm exhibits the property known as the ultrametric property,

$$|x-y|_p \leq Max\{|x_p|,|y|_p\}.$$

Note that if $|x|_p \neq |y|_p$, then $|x-y|_p = Max\{|x|_p,|y|_p\}$.
In order to prove this assertion, assume that $|x|_p > |y|_p$, and we already know that $|x-y|_p \leq Max\{|x|_p,|y|_p\}$. Moreover, take $x = (x-y)+y$ and,

$$|x|_p \leq Max\{|x-y|_p, |y|_p\}.$$

Since we know that $|x|_p > |y|_p$, this inequality can hold only if

$$Max\{|x-y|_p, |y|_p\} = |x-y|_p.$$

This gives the reverse inequality $|x|_p \leq |x-y|_p$, and from it (using our first inequality) we can conclude that $|x-y|_p = |x|_p$.
The entire purpose of an absolute value is to give us a sense of "size." In other words, once we have an absolute value, we can use it to establish a metric for our field by measuring the distances between numbers. We may define open and closed sets and generally explore what is referred to as the topology of our field thanks to the metric.

Definition 3.1.2. *Define* $d(x,y) = |x-y|_p$ *for* $x,y \in \mathbb{Q}$.

We can prove the usual properties of a metric.

Proposition 3.1.3. *1)* $d(x,y) > 0$ *for any* $x,y \in \mathbb{Q}$ *and* $d(x,y) = 0$ *iff* $x = y$.

2) $d(x,y) = d(y,x)$ *for any* $x,y \in \mathbb{Q}$.

3) $d(x,y) \leq d(x,z) + d(z,y)$ *for any* $x,y,z \in \mathbb{Q}$. *In particular,*

4) $d(x,y) \leq max\{d(x,z), d(z,y)\}$ *for any* $x,y,z \in \mathbb{Q}$.

Having a metric gives us a topology with a base for open sets given by the family:

$$B(a,r) = \{x \in \mathbb{Q} \mid |a-x|_p < r\}$$

for $r \in \mathbb{R}^+$ and $a \in \mathbb{Q}$ and the closed balls are:

$$\overline{\mathrm{B}}(a,r) = \{x \in \mathbb{Q} \mid |a-x|_p \leq r\}$$

Now let us introduce the field of p-adic numbers.
From this point forward, we fix a prime integer p. Let S be the set of all Cauchy sequences of rational numbers $\{a_i\}$, meaning that for any given $\varepsilon > 0$, there exists an N such that $|a_i - a_j|_p < \varepsilon$ whenever both i and j are greater than N. We say that two such Cauchy sequences $\{a_i\}$ and $\{b_i\}$ are equivalent, denoted as $\{a_i\} \sim \{b_i\}$, if the p-adic norm $|a_i - b_i|_p$ approaches zero as i tends to infinity.

It can be observed that this establishes an equivalence relation on the set S, and we define the set of p-adic numbers, $\mathbb{Q}_p = S/\sim$ as the set of equivalence classes of Cauchy sequences with respect to the p-adic norm $|.|_p$. In other words, $\mathbb{Q}_p$ consists of all Cauchy sequences in $\mathbb{Q}$ that converge to the same p-adic limit, considered as distinct elements in the quotient set $\mathbb{Q}_p$.

We define the norm $|.|_p$ of an equivalence class $\bar{\mathrm{a}}_i$ to be $\lim_{i\to\infty} |a_i|_p$ where $\{a_i\}$ is any representative of $\bar{\mathrm{a}}_i$ and it can be checked that this limit exists for all $a_i \in \mathbb{Q}$. In another saying, p-adic absolute value extends to $\mathbb{Q}_p$. From the next lemma, this follows naturally.

Lemma 3.1.4. *Let $\{x_n\} \in S$ such that $\lim_{n\to\infty} |x_n|_p \neq 0$. Then, the sequence of real numbers $|x_n|_p$ is eventually stationary.*

Proof. Since $\{x_n\}$ is a Cauchy sequence which does not tend to zero, we can find c and N_1 such that

$$n > N_1 \implies |x_n|_p \geq c > 0.$$

On the other hand, there exists N_2 for which

$$m,n \geq N_2 \implies |x_n - x_m|_p < c.$$

So by taking $N = Max\{N_1,N_2\}$ we have,

$$m,n \geq N \implies |x_n - x_m|_p < Max\{|x_n|_p,|x_m|_p\},$$

which gives $|x_n|_p = |x_m|_p$. □

Now we can have the following definition.

Definition 3.1.5. *If $\lambda \in \mathbb{Q}_p$ and (x_n) be any Cauchy sequence representing λ, we define*

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p$$

It can be checked that $|\lambda|_p = p^{-n}$ for some integer n.
Given any two equivalence classes $\overline{a}$ and $\overline{b}$ of Cauchy sequences in $\mathbb{Q}_p$, we can select representatives $(a_i) \in \overline{a}$ and $(b_i) \in \overline{b}$ from each class. We define the product of these equivalence classes, denoted as $\overline{a} \cdot \overline{b}$, to be the equivalence class represented by the Cauchy sequence $\{a_i \cdot b_i\}$. In a similar manner, we define the sum of two equivalence classes by selecting a Cauchy sequence from each class, adding the corresponding terms

together, and demonstrating that the resulting equivalence class of the sum is independent of the choice of representatives. This allows us to define the additive inverse of an equivalence class in the expected way.
Defining the multiplicative inverse in $\mathbb{Q}_p$ requires some care due to the potential presence of zero terms in a Cauchy sequence. However, it is possible to demonstrate that every Cauchy sequence is equivalent to one that contains no zero terms. This allows us to define the multiplicative inverse in $\mathbb{Q}_p$.

With this in mind, we can show that the set $\mathbb{Q}_p$ of equivalence classes of Cauchy sequences forms a field when equipped with the operations defined as above. The addition and multiplication of equivalence classes are well-defined, as it can be shown by their independence from the choice of representatives. The additive and multiplicative identity can be easily defined using the appropriate Cauchy sequences.
There exists an inclusion map from the rational numbers $\mathbb{Q}$ to the p-adic numbers $\mathbb{Q}_p$. This inclusion map sends an element $x \in \mathbb{Q}$ to the equivalence class $\{x\} \in \mathbb{Q}_p$ represented by the constant Cauchy sequence $x, x, x, \cdots$.

In other words, each rational number $x \in \mathbb{Q}$ can be naturally identified with its equivalence class in $\mathbb{Q}_p$ consisting of all constant Cauchy sequences that converge to x. This inclusion map provides a way to view rational numbers as a subset of p-adic numbers.

Let us now prove that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ or more precisely, the image of $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Proposition 3.1.6. *The image of $\mathbb{Q}$ under the inclusion $\mathbb{Q} \to \mathbb{Q}_p$ is a dense subset of $\mathbb{Q}_p$.*

Proof. We need to show that any open ball around an element $\lambda \in \mathbb{Q}_p$ contains an element of (the image of) $\mathbb{Q}$, i.e., a constant sequence. So for a fixed radius ε, we will show that there is a constant sequence belonging to the open ball $B(\lambda,\varepsilon)$.
First of all, let $\{x_n\}$ be a Cauchy sequence representing λ, and let ε' be a number slightly smaller than ε. By the Cauchy property, there exists a number N such that $|x_n - x_m|_p < \varepsilon'$ whenever $n, m \geq N$. Let $y = x_N$ and consider the constant sequence $\{y\}$. We claim that $\{y\} \in B(\lambda,\varepsilon)$ which means that $|\lambda - \{y\}|_p < \varepsilon$. We know that $\lambda - \{y\}$ is represented by $\{x_n - y\}$ and we have $|\{x_n - y\}|_p = lim_{n\to\infty}|x_n - y|_p$. But, for any $n \geq N$ we have

$$|x_n - y|_p = |x_n - x_N|_p < \varepsilon'.$$

Therefore,

$$\lim_{n\to\infty} |x_n - y|_p \leq \varepsilon' < \varepsilon.$$

So that $\{y\} \in B(\lambda,\varepsilon)$. □

It is important to verify that $\mathbb{Q}_p$, equipped with the properties mentioned above, is unique up to isomorphism that preserves the absolute values. This means that any other complete field with the same properties and absolute value is isomorphic to $\mathbb{Q}_p$. The uniqueness up to isomorphism guarantees that the p-adic field $\mathbb{Q}_p$ is essentially the only field that satisfies these properties, ensuring its special role among complete fields with respect to the p-adic norm.

Now, by using the following theorem, our objective is to alter our perspective on $\mathbb{Q}_p$. Then, it would be wise to shift towards using more concrete terminology and promptly disregard the notion of "equivalence classes of Cauchy sequences."

Theorem 3.1.7. *Every equivalence class $\overline{a}$ in $\mathbb{Q}_p$ for which $|\overline{a}| \leq 1$ has exactly one representative Cauchy sequence of the form $\{a_i\}$ for which:*

1) $0 \leq a_i < p^i$, *for* $i = 1,2,3,...$

2) $a_i \equiv a_{i+1} \pmod{p^i}$, *for* $i = 1,2,3,....$

We need the following lemma for the proof.

Lemma 3.1.8. *Given any $x \in \mathbb{Q}_p$ and $n \geq 1$ with $|x|_p \leq 1$, there exists $\alpha \in \mathbb{Z}, 0 \leq \alpha \leq p^n - 1$, such that $|x - \alpha|_p < p^{-n}$. The integer α with these properties is unique.*

Proof. (Lemma (3.1.8))
suppose we have an element $x = a/b \in \mathbb{Z}_p$, where a and b are integers in lowest terms. Since $|x|_p \leq 1$, this implies that b is not divisible by p, and therefore not divisible by any power of p, such as p^n. Consequently, there exist integers m and k such that $mb + kp^n = 1$. Let $\alpha = ma$ be the element obtained by multiplying a by m. Then,

$$|\alpha - x|_p = |am - (a/b)|_p = |a/b|_p|mb - 1|_p \leq |mb - 1|_p = |kp^n|_p = \frac{|k|_p}{p^n} \leq p^{-n}.$$

□

Now we return to the proof of the theorem.

Proof. (Theorem (3.1.7)) Let's denote $\overline{a}$ simply as a. To establish uniqueness, we begin by assuming the existence of another sequence, denoted as $\{a'_i\}$, that satisfies conditions (1) and (2). If there exists an index i_0 such that $a_{i_0} \neq a'_{i_0}$, we observe that a_{i_0} and a'_{i_0} both fall within the range of values from 0 to p^{i_0}. Consequently, we can conclude that $a_{i_0} \not\equiv a'_{i_0} \pmod{p^{i_0}})$.

However, this equivalence relationship implies that for all indices $i \geq i_0$, $a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i \pmod{p^{i_0}}$. Thus

$$|a_i - a'_i|_p > p^{-i_0}$$

for all $i \geq i_0$ and $\{a_i\} \not\sim \{a'_i\}$.
So suppose $\{b_i\}$ be Cauchy sequence, a representative in a . We want to find an equivalent sequence $\{a_i\}$ satisfying (1) and (2). For every positive integer j, we define $N(j)$ as the natural number such that $|b_i - b_{i'}|_p \leq p^{-j}$ whenever both i and i' are greater than or equal to $N(j)$. It is important to note that if i is larger than $N(1)$, then $|b_i|_p < 1$. Since

$$|b_i|_p \leq Max\{|b_{i'}|_p, |b_i - b_{i'}|_p\} \leq Max\{|b_{i'}|_p, 1/p\}$$

and $|b_{i'}|_p \to |a| \leq 1$ as $i' \to \infty$. Now, by the lemma, we find a sequence of integers a_j, where $0 \leq a_j < p^j$ such that $|a_j - b_{N(j)}|_p \leq p^j$. We claim that $\{a_j\}$ is the desired sequence. It remains to show that $a_j \equiv a_{j+1} \pmod{p^j}$ and $\{a_j\} \sim \{b_j\}$. First follows because:

$$|a_{j+1} - a_j|_p = |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p$$

$$\leq Max\{|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |(a_j - b_{N(j)})|_p\}$$
$$= Max\{1/p^{j+1}, 1/p^j, 1/p^j\} = 1/p^j.$$

The second follows because:

$$|a_i - b_i|_p \leq |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p$$

$$\leq Max\{|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_i - b_{N(j)}|_p\}$$
$$= Max\{1/p^j, 1/p^j, 1/p^j\} = 1/p^j.$$

Hence, $|a_i - b_i|_p \to 0$ as $i \to \infty$ and the theorem is proved. □

We proved the theorem for $|a|_p \leq 1$. What if our p-adic number a is not satisfied by $|a|_p \leq 1$? Then, The p-adic number $a' = ap^m$ obtained by multiplying a by a power p^m of p (i.e., by the power of p equal to $|a|_p$), does fulfil $|a'|_p \leq 1$. Then, a' is represented by a sequence $\{a'_i\}$ as in the theorem and, $a = a'p^{-m}$ is represented by the sequence $\{a_i\}$ in which $a_i = a'_i p^{-m}$. It is now convenient to write all the a'_i in the sequence for a' to the base p, i.e.,

$$a'_i = b_0 + b_1 p + b_2 p^2 + \cdots + b_{i-1} p^{i-1}$$

where all b_i's are all "digits", i.e., integers in $\{0,1,\cdots,p-1\}$. Our condition $a'_i \equiv a'_{i+1} \pmod{p^i}$ precisely means that,

$$a'_{i+1} = b_0 + b_1 p + b_2 p^2 + \cdots + b_{i-1} p^{i-1} + b_i p^i$$

where the digits b_o through b_{i-1} are all the same as for a'_i. Consequently, a' can be understood as a number represented in base p, where the digits extend infinitely to the right, progressively adding a new digit each time we transition from a'_i to a'_{i+1}

Our initial value a can be viewed as a decimal number in base p with a finite number of digits "to the right of the decimal point" (representing negative powers of p, but written from the left), while having an infinite number of digits for positive powers of p:

$$a'_i = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \cdots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + b_{m+2} p^2 + \cdots .$$

We will soon observe that this equality holds in a precise and meaningful manner.

Definition 3.1.9. *The ring of p-adic integer is the valuation ring*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

with the maximal ideal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p < 1\}$ and $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p \mid |x|_p = 1\}$.

We have the similar inclusion $\mathbb{Z} \to \mathbb{Z}_p$ and we can prove that the image of $\mathbb{Z}$ in $\mathbb{Z}_p$ is dense.

Let $\{b_i\}_{i=-m}^{\infty}$ be any sequence of p-adic integers. Consider the sum,

$$S_N = \frac{b_{-m}}{p^m} + \frac{b_{-m+1}}{p^{m-1}} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots + b_N p^N.$$

The sequence of partial sums is evidently a Cauchy sequence. For any indices M and N where $M > N$, the p-adic absolute value of the difference between S_M and S_N is less than $1/p^N$. Consequently, this sequence converges to an element within $\mathbb{Q}_p$. As in the case of infinite series of real numbers, we define $\sum_{i=-m}^{\infty} b_i p^i$ to be this limit in $\mathbb{Q}_p$. More generally, if $\{c_i\}$ is any sequence of p-adic numbers such that $|c_i|_p \to 0$ as $i \to \infty$, the sequence of partial sums $S_N = c_1 + c_2 + ... + c_N$ converge to a limit which we denote $\sum_{i=1}^{\infty} c_i$. This is because $|S_M - S_N|_p = |c_{N+1} + c_{N+2} + ... + c_M|_p \leq Max\{|c_{N+1}|_p, |c_{N+2}|_p, ..., |c_M|_p\}$ which $\to 0$ as $N \to \infty$.

Hence, determining the convergence of p-adic infinite series is simpler compared to infinite series of real numbers. A series converges in $\mathbb{Q}_p$ if and only if its terms approach zero.

Now, focusing on p-adic expansions, we can observe that the infinite series on the right-hand side of the p-adic expansion definition,

$$\frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \cdots + \frac{b_{m-1}}{p} + b_m + b_{m+1}p + b_{m+2}p^2 + \cdots ,$$

(where b_i are elements from the set $0,1,\cdots,p-1$), converges to our a. Therefore, the equality can be understood as the sum of an infinite series. This equality is commonly referred to as the "p-adic expansion" of a.

One observation is that $\mathbb{Z}_p$ serves as the completion of $\mathbb{Z}$ concerning the p-adic absolute value. The sets of the form $a + p^n\mathbb{Z}_p$, where $a \in \mathbb{Q}$ and $n \in \mathbb{Z}$, represent the closed balls within $\mathbb{Q}_p$ (with a as the center and p^{-n} as the radius). Since $\mathbb{Q}$ is densely embedded in $\mathbb{Q}_p$, these closed balls cover the entirety of $\mathbb{Q}_p$. As we have nearly demonstrated, $\mathbb{Q}_p$ is a completely disconnected space since it is a non-Archimedean division ring. Furthermore, for any two points, it is always possible to find separate balls around them that have no intersection.

Remark 3.1.10. *$\mathbb{Q}_p$ is a totally disconnected Hausdorff topological space.*

Remark 3.1.11. *$\mathbb{Z}_p$ is compact, and $\mathbb{Q}_p$ is locally compact.*

Proof. (3.1.11) The second conclusion follows from the fact that $\mathbb{Z}_p$ is a neighborhood of zero. Demonstrating the compactness of $\mathbb{Z}_p$ is indeed sufficient to establish that $\mathbb{Q}_p$ is locally compact. More specifically, the sets $p^n\mathbb{Z}_p$, where n ranges over all integers, form a fundamental system of neighborhoods of 0 in $\mathbb{Q}_p$. This means that every neighborhood of 0 in $\mathbb{Q}_p$ contains one of these sets.

Now, we will establish the compactness of $\mathbb{Z}_p$. Consider the set $A = \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$, endowed with the product topology. According to the Tychonoff Theorem, A is compact because each factor $\mathbb{Z}/p^n\mathbb{Z}$ is compact. Hence, to establish that $\mathbb{Z}_p$ is compact, it suffices to demonstrate its closedness in A. To do so, we can use the fact that $\mathbb{Z}_p$ is the inverse limit of the system $\varprojlim(A_n,\varphi_n)$ for specific A_n and φ_n. As an inverse limit, $\mathbb{Z}_p$ can be identified as a closed subset of A.

So let $A_n = \mathbb{Z}/p^n\mathbb{Z}$ and $\varphi_n : A_n \to A_{n-1}$ be the natural homomorphism and define

$$\mathbb{Z}_p = \varprojlim(A_n,\varphi_n)$$

whose elements are $(...,x_n...,x_1)$ with $x_n \in A_n$ and $\varphi_n(x_n) = x_{n-1}$ if $n \geq 2$. Also the projections, $\pi_n : A \to \mathbb{Z}/p^n\mathbb{Z}$ for $n \geq 1$ which are continuous by the definition of product topology. Then:

$$\mathbb{Z}_p = \cap_{n\in\mathbb{N}^\times}\{x = (x_n)_{n\geq 1} \in A \mid \varphi_n(x_n) = x_{n-1}\}$$

$$= \cap_{n\in\mathbb{N}^\times}\{x = (x_n)_{n\geq 1} \in A \mid \varphi_n(\pi_n(x)) = \pi_{n-1}(x)\}.$$

Indeed, each subset of A defined by $\{x = (x_n)_{n\geq 1} \in A \mid \varphi_n(\pi_n(x)) = \pi_{n-1}(x)\}$ is closed. This can be shown by leveraging the continuity of both the projection maps and the functions φ_n.

The continuity of the projection maps ensures that the pre-images of closed sets under the projections are closed. Additionally, since each φ_n is continuous, the pre-images of closed sets under these functions are also closed.

Therefore, $\mathbb{Z}_p$ is now expressed as the intersection of closed subsets in the product A, implying that $\mathbb{Z}_p$ itself is closed. □

To complete this section, we proceed to discuss briefly the construction of an algebraic closure of $\mathbb{Q}_p$, denoted as $\overline{\mathbb{Q}}_p$, and subsequently its completion.
$\overline{\mathbb{Q}}_p$ is a field that contains all the roots of every polynomial with coefficients in $\mathbb{Q}_p$. In other words, $\overline{\mathbb{Q}}_p$ is obtained by adjoining all the algebraic elements to $\mathbb{Q}_p$ in a systematic manner, ensuring that it includes every root of every polynomial in $\mathbb{Q}_p$. To construct $\overline{\mathbb{Q}}_p$, we simply take the union of all finite extensions of $\mathbb{Q}_p$. Once $\overline{\mathbb{Q}}_p$ is established, we can then consider its completion, which involves adjoining the limit points of Cauchy sequences within $\overline{\mathbb{Q}}_p$.
For any given element $x \in \mathbb{Q}_p$, the extension $\mathbb{Q}_p(x)$ is a finite extension, meaning that its degree is equal to the degree of the minimal polynomial of x over $\mathbb{Q}_p$. Since x resides in the finite extension $\mathbb{Q}_p(x)$, we can define $|x|_p$ by extending the p-adic absolute value

uniquely to $\mathbb{Q}_p(x)$. Interestingly, it can be demonstrated that this absolute value does not rely on the specific field in which it is taken. In other words, it only depends on x itself as a root of some polynomial over $\mathbb{Q}_p$. Consequently, it is meaningful to state that $|x|_p$ is the absolute value of the element $x \in \overline{\mathbb{Q}}_p$, and that $\overline{\mathbb{Q}}_p$ is infinte extension of $\mathbb{Q}_p$.

Theorem 3.1.12. *The algebraic closure $\overline{\mathbb{Q}}_p$ is not complete with respect to the (extended) p-adic absolute value.*

Proof. See [4], ch 5, theorem 5.7.4, p 165. □

Since the algebraic closure of $\mathbb{Q}_p$, is not a complete field, it becomes necessary to create its completion. The process of constructing the completion is similar to that of $\mathbb{Q}_p$ and involves manipulating the ring that consists of all Cauchy sequences within $\overline{\mathbb{Q}}_p$.
To form the completion of $\overline{\mathbb{Q}}_p$, we consider the entire set of Cauchy sequences within $\overline{\mathbb{Q}}_p$ and treat it as a ring. An equivalence relation is established among these sequences, whereby two sequences are considered equivalent if their difference approaches zero as the index tends to infinity. By using this equivalence relation and dividing the ring of Cauchy sequences accordingly, we obtain the completion $\mathbb{C}_p$.

Proposition 3.1.13. *There exists a field $\mathbb{C}_p$ and an absolute value $||_p$ on $\mathbb{C}_p$ such that:*

i) $\mathbb{C}_p$ contains $\overline{\mathbb{Q}}_p$ and the restriction of $||_p$ to $\overline{\mathbb{Q}}_p$ coincides with the p-adic absolute value.

ii) $\mathbb{C}_p$ is complete with respect to the p-adic absolute value, and

iii) $\overline{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$.

v) $\mathbb{C}_p$ is complete and is algebraically closed.

Proof. See [4], ch 5, proposition 5.7.6, p 167 for the first three, and proposition 5.7.8 for the last one. □

3.2 Continuous and analytic functions

Our current aim is to present the notion of continuity and subsequently focus on using power series to establish p-adic analytic functions that exhibit similarities to classical functions.

Definition 3.2.1. *A function $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ is called continuous at a point $\alpha \in \mathbb{Z}_p$, if $\forall \varepsilon > 0$, $\exists \delta > 0$ such that $|x - \alpha|_p < \delta$ implies that $|f(x) - f(\alpha)|_p < \varepsilon$, $\forall x \in \mathbb{Z}_p$.*

A function $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ is continuous if it is continuous at all points $\alpha \in \mathbb{Z}_p$.

Definition 3.2.2. *A function $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ is called locally constant if every point $x \in \mathbb{Z}_p$ has a neighborhood U_x such that $f(U_x)$ is a single element in $\mathbb{Q}_p$.*

Remark 3.2.3. *Locally constant functions are continuous.*

As an example, since the space $\mathbb{Z}_p$ is totally disconnected, the characteristic function of any open ball $U \subset \mathbb{Z}_p$ is continuous.

$$\delta_U(x) = \begin{cases} 1 & \text{if } x \in U \\ 0 & \text{if } x \in \mathbb{Z}_p - U. \end{cases} \tag{3.2}$$

Remember that in a metric space with a non-Archimedean norm, a sequence is called Cauchy if and only if the difference between consecutive terms tends to zero. Moreover, in a complete metric space, an infinite sum converges if and only if its general term approaches zero. So if we consider expressions of the form

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \; a_n \in \mathbb{Q}_p,$$

we can give a value $\sum_{n=0}^{\infty} a_n x^n$ to $f(x)$ whenever an x is substituted for X for which $|a_n x^n|_p \to 0$. Just as in the Archimedean case (power series over $\mathbb{R}$ or $\mathbb{C}$), we define the "radius of convergence"

$$r = \frac{1}{\limsup \sqrt[n]{|a_n|_p}}$$

where the terminology "$1/r = \limsup \sqrt[n]{|a_n|_p}$ means that $1/r$ is the least real number such that for any $C > 1/r$ there are only finitely many $\sqrt[n]{|a_n|_p}$ greater than C. Equivalently, $1/r$ is the greatest "point of accumulation," i.e., the greatest real number which can occur as the limit of a subsequence of $|a_n|_p^{1/n}$.

Lemma 3.2.4. *Every $f(X) \in \mathbb{Z}_p[[X]]$ converges in $B(0,1) = \{x \in \mathbb{Q}_p \mid |x - 0|_p < 1\}$*

Proof. Let $f(X) = \sum_{n=0}^{\infty} a_n X^n$, $a_n \in \mathbb{Z}_p$ and let $x \in B(0,1)$. Thus $|x|_p < 1$ and also $|a_n|_p \leq 1$ for all n. Hence $|a_n x^n|_p \leq |x^n|_p \to 0$ as $n \to \infty$. $\square$

Another easy lemma is,

Lemma 3.2.5. *Every power series $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Z}_p[[X]]$ which converges in an open or (closed disc) $B(a,r)$ or $(\overline{B}(a,r))$, is continuous on it.*

Proof. Suppose $|x - x'|_p < \delta$, where $\delta < |x|_p$ will be chosen later. Then, $|x|_p = |x'|_p$ (we are assuming $x \neq 0$). We write

$$|f(x) - f(x')|_p = |\sum_{n=0}^{\infty} (a_n x^n - a_n x'^n)|_p$$

$\leq Max_n\{|a_nx^n - a_n'x'^n|_p\} = Max_n\{(|a_n|_p|(x-x')(x^{n-1}+x^{n-2}x'+...+xx'^{n-2}+x'^{n-1}|_p)\}.$

But,

$$|x^{n-1} + x^{n-2}x' + ... + xx'^{n-2} + x'^{n-1}|_p \leq Max_i\{x^{n-i}x'^{i-1}\}$$
$$= |x|_p^{n-1}.$$

Hence,

$$|f(x) - f(x')|_p \leq Max_n\{|x - x'|_p|a_n|_p||x|_p^{n-1}\}$$
$$< \frac{\delta}{|x|_p} Max_n\{|a_n|_p||x|_p^n\}.$$

Since $|a_n|_p||x|_p^n$ is bounded as $n \to \infty$, $|f(x) - f(x')|_p \leq \varepsilon$ for suitable δ. □

Remark 3.2.6. *The lemma can be generalised for $f(x) \in \mathbb{Q}_p[[X]]$.*

We now continue by introducing p-adic variations of the exponential and logarithm functions. As one might expect, the p-adic theory demonstrates a significant resemblance to the classical version, with the exception that certain challenging aspects become significantly easier to manage.
We begin with the formal power series of logarithm:

$$f(X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n}.$$

Considering that the coefficients of this power series consist of rational numbers, it is logical to interpret the series as a power series in $\mathbb{Q}_p$ (where p is any prime number). The initial stage in comprehending the power series involves determining its radius of convergence. Before delving into the calculation of the limit, it is important to observe another contrast between the classical and p-adic contexts. In the classical scenario, the presence of integers in the denominators contributes to the convergence as they tend to reduce the size of the series terms. However, in the p-adic context, this situation is completely reversed: integers in the denominator either have no effect on the absolute value (when they are not divisible by p) or make it bigger (when they are divisible by p).
Now, to compute the radius of f, we observe that:

$$|a_n|_p = |\frac{1}{n}|_p = p^{v_p(n)}.$$

Therefore,

$$|\sqrt[n]{a_n}|_p = p^{v_p(n)/n} \to 1,$$

as $n \to \infty$. So the radius of convergence is 1. This distinction does not provide a conclusive answer regarding whether the convergence occurs within the open or closed ball of radius 1. To make this determination, we must examine the behavior when the absolute value of "x" is equal to 1. However, it becomes evident that in such a scenario,

$|a_n X^n|_p = |1/n|_p$ does not tend to zero. So we have:

Lemma 3.2.7. *The series*

$$f(X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} = X - \frac{X^2}{2} + \frac{X^3}{3} - \frac{X^4}{4} + \cdots$$

converges for $|x|_p < 1$.

The conclusion is that $f(X)$ defines a function on the open ball $B(0,1)$ of radius 1 and center 0.

Definition 3.2.8. *We define the p-adic logarithm of* $x \in B(1{,}1)$ *as*

$$\log_p(x) = \log(1 + (x-1)) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}.$$

One of the most appealing aspects of defining the logarithm in this manner is that it preserves the fundamental property of the logarithm which is an equality of formal power series.

$$\log(X+1) + \log(Y+1) = \log(1 + X + Y + XY).$$

It follows that for any x and $y \in 1 + p\mathbb{Z}_p$, we have

$$\log_p(x) + \log_p(y) = \log_p(xy).$$

Now that we have established a logarithm, the construction of exponentials is not far behind. In the classical context, the exponential function is defined by the series:

$$\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$$

In the classical case, the series for the exponential function converges for all $x \in \mathbb{R}$, because the coefficients $1/n!$ decrease rapidly as n increases, approaching zero with respect to the real absolute value. However, in the p-adic context, this situation undergoes a significant change. The factorial term $n!$ tends to zero, causing the coefficients $1/n!$ to become arbitrarily large as n increases. As a result, we cannot expect to have a large radius of convergence. To determine the specific radius, we need to analyze the growth rate of the coefficients $1/n!$, specifically how divisible $n!$ is by the prime number p.

Lemma 3.2.9. *Let p be a prime. Then*

$$v_p(n!) = \sum_{n=0}^{\infty} \lfloor \frac{n}{p^i} \rfloor \leq \frac{n}{p-1}$$

where $\lfloor . \rfloor$ *is the greatest integer function.*

Proof. The equality is a well known number theoretic fact. The inequality follows because we have $\lfloor x \rfloor \leq x$, so that,

$$v_p(n!) = \sum_{i=0}^{\infty} \lfloor \frac{n}{p^i} \rfloor \leq \sum_{i=0}^{\infty} \frac{n}{p^i} = \frac{n}{p-1}$$

□

Now we use this estimate to work out the convergence of the exponential.

Lemma 3.2.10. *Let*

$$g(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!} = 1 + X + \frac{X^2}{2!} + \frac{X^3}{3!} + \cdots$$

Then $g(x)$ converges if and only if $|x|_p \leq p^{-\frac{1}{p-1}}$.

Proof. Since

$$|a_n|_p < p^{\frac{n}{p-1}},$$

by the previous lemma, we get

$$r \geq p^{-\frac{1}{p-1}}$$

where r represents the radius of convergence. Thus, the series certainly converges for $|x|_p < p^{-1/p-1}$.

On the other hand, let $|x|_p = p^{-1/(p-1)}$, and let $n = p^m$ be a power of p. Then we first have;

$$v_p(n!) = v_p(p^m!) = 1 + p + \cdots + p^{m-1} = \frac{p^m - 1}{p-1},$$

and, then since $v_p(x) = 1/p - 1$,

$$v_p(\frac{x^n}{n!}) = v_p(\frac{x^{p^m}}{p^m!}) = \frac{p^m}{p-1} - \frac{p^m - 1}{p-1} = \frac{1}{p-1}.$$

The fact that the convergence of $x^n/n!$ does not depend on the variable m, implies that it cannot tend to zero. As we already know that the region of convergence is a disk, this observation serves as proof for the lemma. □

Definition 3.2.11. *The p-adic exponential is the function $exp_p : B(0,p^{-1/p-1}) \to \mathbb{Q}_p$ defined by,*

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

Similar to the logarithm, the formal property of the exponential function is preserved in this context. If x and y are in $B(0,p^{-1/p-1})$, we have $x + y \in B(0,p^{-1/p-1})$ and,

$$\exp_p(x + y) = \exp_p(x) + \exp_p(y)$$

Proposition 3.2.12. *The functions* $\log_p$ *and* $\exp_p$ *are inverse one to the other, acting as isomorphisms, connecting the multiplicative group within the open disc centered at 1 with a radius of* $p^{-1/(p-1)}$ *and the additive group within the open disc centered at 0 with the same radius.*

Proof. See [3], proposition, p 81. □

Remark 3.2.13. *Almost everything extends to* $\mathbb{C}_p$*. More precisely:*
let
$$\mathfrak{D} = \{x \in \mathbb{C}_p \mid |x|_p \leq 1\}.$$
A power series $\sum_{n=1}^{\infty} a_n X^n$ with coefficients $a_n \in \mathbb{C}_p$ defines a continuous function on an open ball of radius $r = 1/(\limsup \sqrt[n]{|a_n|_p})$; the function extends to the closed ball of radius r if $|a_n|_p r^n \to 0$ as $n \to \infty$.
The usual power series defines a p-adic logarithm function
$$\log_p \ : \ B \to \mathbb{C}_p$$
where
$$B = \{x \in \mathfrak{D} \mid |x - 1|_p < 1\}.$$
This function satisfies the usual functional equation of $\log_p$.
The usual power series defines an exponential function
$$\exp_p \ : \ D \to \mathbb{C}_p$$
where
$$D = \{x \in \mathfrak{D} \mid |x|_p < p^{-1/(p-1)}\}.$$
This function also satisfies the functional equation of exp_p.

Now, we wish to introduce the concept of derivatives for p-adic functions in a natural manner by defining them in the conventional way.

Definition 3.2.14. *Let* $U \subset \mathbb{C}_p$ *be an open set, and let* $f : U \to \mathbb{C}_p$ *be a function. We say* f *is differentiable at* $x \in U$ *if the limit*
$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$
exists. If $f'(x)$ *exists for every* x *in* U*, we say* f *is differentiable in* U*, and we write* $f' : U \to \mathbb{C}_p$ *for the function* $x \mapsto f'(x)$*.*

To a certain degree, the derivative behaves as expected in p-adic analysis. For instance, we can demonstrate that differentiable functions are continuous, just as we do in the real numbers or complex numbers. However, there are some intriguing aspects that warrant further explorations.

Proposition 3.2.15. *Let $\sum a_n X^n$ be a power series and suppose $f = \sum a_n(x-\alpha)^n$ converges for all x in the closed ball $\beta = \overline{B}(\alpha,r) \subset \mathbb{C}_p$. Then we have:*

i) For every $x \in \beta$, the derivative $f'(x)$ exists, and is given by

$$f'(x) = \sum n a_n (x-\alpha)^{n-1}.$$

ii) More generally, for every $x \in \beta$, the k-th derivative exists and is given by,

$$f^{(k)}(x) = \sum \binom{n}{k} a_n (x-\alpha)^{n-k},$$

in particular, we have

$$a_k = \frac{f^{(k)}(\alpha)}{k!}.$$

iii) $f(x)$ is infinitely differentiable.

iv) Let $\beta \in \overline{\mathrm{B}}(\alpha,r)$. Then there exists a series $\sum b_n X^n$ such that $f(x) = \sum b_n(x-\beta)^n$ for any $x \in \overline{\mathrm{B}}(\alpha,r) = \overline{\mathrm{B}}(\beta,r)$. The series $\sum a_n X^n$ and $\sum b_n X^n$ have exactly the same region of convergence.

Proof. See [4], proposition 4.2.3, p 91. □

Definition 3.2.16. *If a function can be expressed as a convergent power series within a small vicinity of every point in its defined region, it is referred to as being locally analytic.*

3.3 p-Adic measures and examples

We start with the metric space $\mathbb{Q}_p$. As previously mentioned, the collection of sets in this metric space consisting of all sets of the form $a+p^N\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x-a|_p \leq 1/p^N\}$, where a belongs to $\mathbb{Q}_p$ and N belongs to $\mathbb{Z}$, forms an open basis for the topology. Consequently, any open subset of $\mathbb{Q}_p$ can be expressed as a union of open subsets of this form.
Such sets of the form $a+p^N\mathbb{Z}_p$ will be referred to as "intervals," and we may sometimes abbreviate $a+p^N\mathbb{Z}_p$ as $a+(p^N)$. It is important to note that all intervals are both closed and open. This is due to the fact that the complement of $a+(p^N)$ is the union of intervals $a'+(p^N)$ for all a' belonging to $\mathbb{Q}_p$ such that a' is not in $a+(p^N)$.
Let us review the properties of $\mathbb{Z}_p$: it is both compact and sequentially compact, meaning that every sequence of p-adic integers has a convergent subsequence. From this, we can deduce that an open subset of $\mathbb{Q}_p$ is compact if and only if it can be expressed as a finite union of intervals. We refer to these specific open sets as "compact-open" sets.

Let's recall the definition of locally constant functions.

Definition 3.3.1. *A function $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ is called locally constant if every point $x \in \mathbb{Z}_p$ has a neighborhood U_x such that $f(U_x)$ is a single element in $\mathbb{Q}_p$.*

It is worth noting that a locally constant function is continuous. In our context, we consider X as a compact-open subset of $\mathbb{Q}_p$, typically either $\mathbb{Z}_p$ or $\mathbb{Z}_p^\times$.

When defining integrals using Riemann sums, locally constant functions in p-adic context serve a similar purpose to step functions in the real numbers ($X = \mathbb{R}$).

Now, let's consider X as a compact-open subset of $\mathbb{Q}_p$, such as $\mathbb{Z}_p$ or $\mathbb{Z}_p^\times$, and proceed to define distributions.

Definition 3.3.2. *A p-adic distribution μ on X is a $\mathbb{Q}_p$-linear map on the space of locally constant functions on X to $\mathbb{Q}_p$. Equivalently,*
a distribution on X is an additive map from the set of compact-opens in X to $\mathbb{Q}_p$. i.e, if $U \subset X$ is the disjoint union of compact-opens $U_1, U_2, \ldots, U_n$, then $\mu(U) = \sum_{i=1}^{n} \mu(U_i)$.

Proposition 3.3.3. *Every map μ from the set of intervals contained in X to $\mathbb{Q}_p$ for which*

$$\mu(a + (p^N)) = \sum_{b=0}^{p-1} \mu(a + bp^N + (p^{N+1})),$$

whenever $a + (p^N) \subset X$, extends uniquely to a p-adic distribution on X.

Proof. Every compact-open $U \subset X$ can be written as a finite disjoint union of intervals: $U = \bigcup_i I_i$. We then define $\mu(U) = \sum \mu(I_i)$. To check that $\mu(U)$ does not depend on the partitioning of U into intervals, we first note that any two partitions $U = \bigcup_i I_i$ and $U = \bigcup_i I'_i$ of U into a disjoint union of intervals have a common subpartition ("finer" than both) which is of the form $I_i = \bigcup_j I_{ij}$ where, if $I_i = a + (p^N)$, then the I_{ij}'s run through all intervals $a' + (p^N)$ for some fixed $N' > N$ and for variable a' which are $\equiv a \pmod{p^N}$. Then, by repeated application of the equality in the statement of the proposition, we have:

$$\mu(I_i) = \mu(a + (p^N)) = \sum_{j=0}^{p^{N'-N-1}} \mu(a + jp^N + (p^{N'})) = \sum_j \mu(I_{ij}).$$

□

Some examples of p-adic distributions are as follows:

1) The Haar distribution, denoted as μ_{Haar}, is defined as follows:

$$\mu_{haar}(a + (p^N)) = \frac{1}{p^N}.$$

2) The Dirac distribution μ_α, concentrated at $\alpha \in \mathbb{Z}_p$, is defined as follows: $\mu_\alpha(U) = 1$

if $\alpha \in U$ and $\mu_\alpha(U) = 0$ otherwise.

3) The Bernoulli distribution $\mu_{B,k}$ is related to the Bernoulli polynomials. Let's first recall the definition of the Bernoulli polynomials:

The k-th Bernoulli polynomial, denoted $B_k(x)$, is defined by the generating function:

$$\frac{te^{xt}}{e^t - 1} = \sum_{k=0}^{\infty} B_k(x) \frac{t^k}{k!}.$$

Based on this, we can define the Bernoulli distribution $\mu_{B,k}$ as follows:

$$\mu_{B,k}(a + (p^N)) = p^{N(k-1)} B_k(\frac{a}{p^N}).$$

Proposition 3.3.4. *$\mu_{B,k}$ extends to a distribution on $\mathbb{Z}_p$ (called the "kth Bernoulli distribution ").*

Proof. By the previous proposition, we must show that

$$\mu_{B,k}(a + (p^N)) = \sum_{b=0}^{p-1} \mu_{B,k}(a + bp^N + (p^{N+1})).$$

The right-hand side equals

$$\mu_{B,k}(a + (p^N)) = p^{(N+1)(k-1)} B_k(\frac{a + bp^N}{p^{N+1}}).$$

So, multiplying with $p^{-N(k-1)}$ and setting $\alpha = a/p^{N+1}$, we must show that

$$B_k(p\alpha) = p^{k-1} \sum_{b=0}^{p-1} B_k(\alpha + \frac{b}{p}).$$

The right-hand side is, by the definition of $B_k(x)$, equal to $k!$ times the coefficient of t^k in

$$p^{k-1} \sum_{b=0}^{p-1} \frac{te^{(\alpha+b/p)t)}}{e^t - 1} = \frac{p^{k-1} te^{\alpha t}}{e^t - 1} \sum_{b=0}^{p-1} e^{bt/p} = \frac{p^{k-1} te^{\alpha t}}{e^t - 1} \frac{e^t - 1}{e^{t/p} - 1}.$$

By summing the geometric progression $\sum_{b=0}^{p-1} e^{bt/p}$, this expression equals to

$$\frac{p^k (t/p) e^{p\alpha(t/p)}}{e^{t/p} - 1} = p^k \sum_{j=0}^{\infty} B_j(p\alpha) \frac{(t/p)^j}{j!},$$

again by the definition of $B_k(x)$. Hence, k times the coefficient of t^k is simply

$$p^k B_k(p\alpha)(1/p)^k = B_k(p\alpha)$$

as desired. □

Finally, we are ready to extend distributions to measures and do integrations.

Definition 3.3.5. *A p-adic distribution μ on X is a measure if its values on compact-opens $U \subset X$ are bounded by some constant $B \in \mathbb{R}$, i. e.,*

$$|\mu(U)|_p \leq B$$

for all compact open $U \subset X$

The Dirac distribution μ_α for a fixed $\alpha \in \mathbb{Z}_p$ is indeed a measure. However, the Bernoulli distributions, as initially defined, may not be measures. In order to convert the Bernoulli distributions into measures, a common approach called "regularization" can be used. Let's introduce some notation. Given $\alpha \in \mathbb{Z}_p$, we define $\{\alpha\}_N$ as the rational integer that lies between 0 and $p^N - 1$ and is congruent to α modulo p^N. If μ is a distribution and $\alpha \in \mathbb{Q}_p$, we define $\alpha\mu$ as the distribution whose value on any compact-open set is equal to α times the value of μ. In other words, for any compact-open set U, we have $(\alpha\mu)(U) = \alpha \cdot (\mu(U))$.

Lastly, let's define the multiplication of a compact-open set $U \subset \mathbb{Q}_p$ by a non-zero scalar $\alpha \in \mathbb{Q}_p$. We denote this operation as αU, and it is defined as the set $\{x \in \mathbb{Q}_p \mid x/\alpha \in U\}$. It can be easily verified that the sum (scalar multiplication) of distributions (or measures) results in another distribution (or measure). Specifically, given a distribution (or measure) μ and a scalar $\alpha \in \mathbb{Q}_p$, the distribution (or measure) $\alpha\mu$ is obtained by multiplying the values of μ by α.

Furthermore, if $\alpha \in \mathbb{Z}_p^\times$ and μ is a distribution (or measure) defined on $\mathbb{Z}_p$, the function μ' defined as $\mu'(U) = \mu(\alpha U)$ is also a distribution (or measure) on $\mathbb{Z}_p$.
Let α be any rational integer that is not equal to 1 and is not divisible by p. We introduce the notation $\mu_{k,\alpha}$ to represent the regularized Bernoulli distribution on $\mathbb{Z}_p$. The definition of this distribution is as follows:

$$\mu_{k,\alpha}(U) = \mu_{B,k}(U) - \alpha^{-k}\mu_{B,k}(\alpha U).$$

We will show that $\mu_{k,\alpha}$ is a measure. However, regardless of the proof, it is evident from the arguments presented in the previous paragraph that $\mu_{k,\alpha}$ is indeed a distribution.
If $k = 1$, we have:

$$\mu_{1,\alpha}(a + (p^N)) = \mu_{B,1}(a + (p^N)) - \alpha^{-1}\mu_{B,1}(a + (p^N)) = B_1(\frac{a}{p^N}) - \alpha^{-1}B_1(\frac{\alpha a}{p^N})$$

$$= \frac{a}{p^N} - \frac{1}{2} - \alpha^{-1}\left[\frac{\alpha a}{p^N} - \frac{1}{2}\right]$$

$$= \frac{1/(\alpha) - 1}{2} + \frac{a}{p^N} + \frac{1}{\alpha}\{\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\}$$

$$= \frac{1}{\alpha}\left[\frac{\alpha a}{p^N}\right] + \frac{1/(\alpha)-1}{2}$$

where [ ] means the greatest integer function.

Proposition 3.3.6. $|\mu_{1,\alpha}(U)|_p \leq 1$ *for all compact open* $U \subset \mathbb{Z}_p$.

Proof. Note that $1/\alpha \in \mathbb{Z}_p$ and $1/2 \in \mathbb{Z}_p$. Therefore, for $p \neq 2$, we have $1/\alpha - 1/2 \in \mathbb{Z}_p$. If $p = 2$, we have $\alpha^{-1} - 1 \equiv 0 \pmod 2$, which is also valid. Since $\left[\alpha a/p^N\right] \in \mathbb{Z}_p$, we can conclude that $\mu_{1,\alpha}(a + (p^N)) \in \mathbb{Z}_p$. Moreover, since every compact-open set U can be expressed as a finite disjoint union of intervals I_i, we can infer that

$$|\mu_{1,\alpha}(U)|_p \leq Max|\mu_{1,\alpha}(I_i)|_p \leq 1$$

□

We will shortly prove that $\mu_{k,\alpha}$ is a measure for all $k = 1, 2, 3, ...$ and $1 \neq \alpha \in \mathbb{Z}$, and $\alpha \notin p\mathbb{Z}$.

Consequently, $\mu_{1,\alpha}$ qualifies as a measure and represents the initial notable example of a p-adic measure that we have encountered. In fact, as we will soon observe, $\mu_{k,\alpha}$ plays a vital role in p-adic integration, akin to the significance of "dx" in actual integration. We then demonstrate a crucial congruence connecting $\mu_{1,\alpha}$ to $\mu_{k,\alpha}$. The demonstration of this congruence initially appears tediously computational, but it becomes clearer when we consider an identical circumstance in real calculus.

Theorem 3.3.7. *Let* d_k *be the least common denominator of the coefficients in* $B_k(x)$. *Therefore,* $d_1 = 2, d_2 = 6, d_3 = 2$ *and etc. Then,*

$$d_k\mu_{k,\alpha}(a + (p^N)) \equiv d_k k a^{k-1}\mu_{1,\alpha}(a + (p^N)) \pmod{p^N}$$

where both sides of this congruence lie in $\mathbb{Z}_p$.

Proof. We know that

$$B_k(x) = B_0x^k + kB_1x^{k-1} + ... = x^k - k/2x^{k-1} + ...$$

We also have,

$$d_k\mu_{k,\alpha}(a + (p^N)) = d_k p^{N(k-1)}\left(B_K(\frac{a}{p^N}) - \alpha^{-k}B_k(\frac{\{\alpha a\}_N}{p^N})\right).$$

The polynomial $d_K B_k(x)$ has integral coefficients and degree k. Consequently, we only need to take into account the leading two terms, $d_k x^k - d_k(k/2)x^{k-1}$, of $d_k B_k(x)$. This is because our variable x has a denominator of p^N, which ensures that the denominators in the lower terms of $d_k B_k(x)$ will be canceled out by $p^{N(k-1)}$, leaving us with at least

p^N remaining. We also note that,

$$\alpha a \equiv \{\alpha a\}_N \pmod{p^N}$$

and

$$\frac{\{\alpha a\}_N}{p^N} = \frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right].$$

Therefore,

$$d_k\mu_{k,\alpha}(a+(p^N)) \equiv d_k p^{N(k-1)}\left(\frac{a^k}{p^{Nk}} - \alpha^{-k}\left(\frac{\{\alpha a\}}{p^N}\right)^k\right.$$

$$\left.-\frac{k}{2}\left(\frac{a^{k-1}}{p^N(k-1)} - \alpha^{-k}\left(\frac{\{\alpha a\}}{p^N}\right)^{k-1}\right)\right) \pmod{p^N}$$

$$= d_k\left(\frac{a^k}{p^N} - \alpha^{-k}p^{N(k-1)}\left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right)^k - \frac{k}{2}\left(a^{k-1} - \alpha^{-k}p^{N(k-1)}\left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right)^{k-1}\right)\right)$$

$$\equiv d_k\left(\frac{a^k}{p^N} - \alpha^{-k}\left(\frac{\alpha^k a^k}{p^N} - k\alpha^{k-1}a^{k-1}\left[\frac{\alpha a}{p^N}\right]\right) - \right.$$

$$\left.\frac{k}{2}(a^{k-1} - \alpha^{-k}(\alpha^{k-1}a^{k-1})\right) \pmod{p^N}$$

$$= d_k k a^{k-1}\left(\frac{1}{\alpha}\left[\frac{\alpha a}{p^N}\right] + \frac{1/(\alpha) - 1}{2}\right)$$

$$= d_k k a^{k-1}\mu_{1,\alpha}(a+(p^N)).$$

□

Corollary 3.3.8. *$\mu_{k,\alpha}(a+(p^N))$ is a measure for all $k = 1,2,3,\cdots$, and any $\alpha \in \mathbb{Z}$ and $\alpha \notin p\mathbb{Z}, \alpha \neq 1$.*

Proof. We must show that $\mu_{k,\alpha}(a+(p^N))$ is bounded. By the previous theorem,

$$|\mu_{k,\alpha}(a+(p^N))|_p \le Max\left\{|\frac{p^N}{d_k}|_p, |ka^{k-1}\mu_{1,\alpha}(a+(p^N))|_p\right\} \le Max\left\{|\frac{1}{d_k}|_p, |\mu_{1,\alpha}(a+(p^N))|_p\right\}.$$

But, $|\mu_{1,\alpha}(a+(p^N))|_p \le 1$ and d_k is fixed. □

Why go to all this trouble to "regularise" Bernoulli distributions in order to obtain measures? The answer is that if f is locally constant for an unbounded distribution μ, then $\int f d\mu$ is defined by definition as long as f is locally constant. However, some problems arise when attempting to employ limits of Riemann sums to extend integration to continuous functions f.
For example, let $\mu = \mu_{Haar}$ and take the simple function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ given by

$f(x) = x$. Let's form the Riemann sums. Given f, for any N we divide up $\mathbb{Z}_p$ into $\bigcup_{a=0}^{p^N-1}(a + (p^N))$, and we let $x_{a,N}$ be an arbitrary point in the ath interval and define the Nth Riemann sum of f corresponding to $\{x_{a,N}\}$ as

$$S_{N,\{x_{a,N}\}} = \sum_{a=0}^{p^N-1} f(x_{a,N})\mu(a + (p^N)).$$

In our example, this sum equals to

$$\sum_{a=0}^{p^N-1} x_{a,N}\frac{1}{p^N}$$

For example, if we simply choose $x_{a,N} = a$ we obtain,

$$\sum_{a=0}^{p^N-1} a\frac{1}{p^N} = p^{-N}\frac{(p^N-1)p^N}{2} = \frac{p^N-1}{2}.$$

This sum has a limit in $\mathbb{Q}_p$ as $N \to \infty$, namely, $-1/2$. But if instead of $x_{a,N} = a \in a + (p^N)$ we change one of the $x_{a,N}$ to $a + a_0p^N \in a + (p^N)$ for each N, where a_0 is a fixed p-adic integer, then we obtain that

$$p^{-N}\left(\sum_{a=0}^{p^N-1} a + a_0p^N\right) = \frac{p^N-1}{2} + a_0$$

whose limit is $a_0 + \frac{1}{2}$. Consequently, the choice of points within the intervals does not determine the limit of the Riemann sums. If it is not possible to integrate continuous functions with respect to a "distribution," then it is of limited use and should not be considered as a measure. We now demonstrate how bounded distributions merit the word "measure" given to them.
Recall that X is a compact-open subset of $\mathbb{Q}_p$ like $\mathbb{Z}_p$ or $\mathbb{Z}_p^\times$ (for simplicity take $X \subset \mathbb{Z}_p$). The following theorem allows us to integrate the continuous functions.

Theorem 3.3.9. *Let μ be a p-adic measure on X, and let $f : X \to \mathbb{Q}_p$ be a continuous function. Then the Riemann sums*

$$S_{N,\{x_{a,N}\}} = \sum_{0\le a<p^N, a+(p^N)\subset X} f(x_{a,N})\mu(a + (p^N))$$

where $x_{a,N} \in a + (p^N)$, converge to a limit in $\mathbb{Q}_p$ as $N \to \infty$ which does not depend on the choice of $\{x_{a,N}\}$.

Proof. Suppose that $|\mu(U)|_p \le B$ for all compact-open $U \subset X$. We first estimate for $M > N$

$$|S_{N,\{x_{a,N}\}} - S_{M,\{x_{a,M}\}}|_p.$$

By writing X as a finite union of intervals, we can choose N large enough so that every $a+(p^N)$ is either $\subset X$ or is disjoint from X. We rewrite $S_{N,\{x_{a,N}\}}$ as follows, by using the additivity of μ,

$$S_{N,\{x_{a,N}\}} = \sum_{0\le a<p^M, a+(p^M)\subset X} f(x_{\overline{\mathrm{a}},N})\mu(a+(p^M))$$

(where $\overline{\mathrm{a}}$ denotes the least nonnegative residue of $a \pmod{p^N}$). We further assume that N is large enough so that $|f(x)-f(y)|_p \le \varepsilon$ whenever $x \equiv y \pmod{p^N}$. (Remember that since X is compact, continuity implies uniform continuity.). Then

$$\begin{aligned}|S_{N,\{x_{a,N}\}} - S_{M,\{x_{a,M}\}}|_p &= \left| \sum_{0\le a<p^M, a+(p^M)\subset X} \Big(f(x_{\overline{\mathrm{a}},N}) - f(x_{a,M})\Big)\mu(a+(p^M))\right|_p \\ &\le Max\{|f(x_{\overline{\mathrm{a}},N}) - f(x_{a,M})|_p.|\mu(a+(p^M))|_p\} \\ &\le \varepsilon.B\end{aligned}$$

□

Definition 3.3.10. *If $f: X \to \mathbb{Q}_p$ is a continuous function and μ is a measure on X, we define $\int f\mu$ to be the limit of the Riemann sums, the existence of which was just proved. (Note that if f is locally constant, this definition agrees with the earlier meaning of $\int f\mu\ \cdot$)*

The following simple but important facts follow immediately from this definition.

Proposition 3.3.11. *If $f: X \to \mathbb{Q}_p$ is a continuous function such that $|f(x)|_p \le A$ for all $x \in X$ and if $|\mu(U)|_p \le B$ for all compact-open $U \subset X$, then*

$$\left| \int f\mu \right|_p \le AB.$$

Proof. By writing the Riemann sum,

$$\begin{aligned}\left| \int_X f\mu \right|_p &= \left| \lim_{N\to\infty} \sum_{a=0}^{p^N-1} f(x)\mu(a+(p^N)) \right|_p \\ &\le Max\Big\{ |f(x)|_p.|\mu(a+(p^N))|_p \Big\} \le AB.\end{aligned}$$

□

Corollary 3.3.12. *If f,$g: X \to \mathbb{Q}_p$ are two continuous functions such that $|f(x)-$*

$g(x)|_p \leq \varepsilon$ for all $x \in X$ and if $|\mu(U)|_p \leq B$ for all compact-open $U \subset X$, then

$$\left| \int f\mu - \int g\mu \right|_p \leq \varepsilon B.$$

Proof. With similar calculation,

$$\left| \int_X f\mu - \int g\mu \right|_p = \left| \lim_{N\to\infty} \sum_{a=0}^{p^N-1} (f(x) - g(x))\mu(a + (p^N)) \right|_p$$

$$\leq Max\left\{ |f(x) - g(x)|_p . |\mu(a + (p^N))|_p \right\} \leq \varepsilon B.$$

□

Chapter 4

p-Adic zeta and L-functions

4.1 p-Adic interpolation of $f(s) = a^s$

Let's consider a positive real number a. The function $f(s) = a^s$ can be defined as a continuous function of a real variable by initially defining it for rational numbers s and then extending it by continuity to real numbers. This extension is accomplished by considering each real number as the limit of a sequence of rational numbers.

Consider the scenario where we have a fixed positive integer, denoted n, which we treat as an element belonging to the field of p-adic numbers. For any non-negative integer s, the value of n^s is an element of the p-adic integers. Furthermore, the non-negative integers are dense within the set of p-adic integers, similar to how the rational numbers are dense within the real numbers. In simpler terms, any p-adic integer can be expressed as the limit of a sequence of non-negative integers. Based on this understanding, we can try to extend the function $f(s) = n^s$ in a continuous manner from non-negative integers s to all p-adic integers s.
In order to achieve this extension, it is necessary to investigate whether n^s and $n^{s'}$ are close to each other when the non-negative integers s and s' are close. For instance, we can consider the case where $s' = s + p^N$ for a sufficiently large positive integer N. However, by examining a few examples, we can observe that this proximity does not always hold true,
(1) $n = p$, $s = 0$: $|n^s - n^{s'}|_p = |1 - p^N|_p = 1$.
(2)$1 < n < p$: by Fermat's little theorem, we have $n^p \equiv n$ and so $n \equiv n^p \equiv n^{p^2} \equiv n^{p^3} \equiv ... \equiv n^{p^N} \pmod{p}$, hence $n^s - n^{s+p^N} = n^s(1 - n^{p^N}) \equiv n^s(1-n) \pmod{p}$, thus $|n^s - n^{s'}|_p = 1$, no matter what N is.
However, the situation is not as unfavorable as the previous examples might suggest. let's choose n such that $n \equiv 1 \pmod{p}$. For instance, we can choose $n = 1 + mp$, where m is an integer. Now, let's consider the condition $|s' - s|_p \leq 1/p^N$, which implies that

$s' = s + s''p^N$ for some $s'' \in \mathbb{Z}$. Then we have (let $s' > s$)

$$|n^s - n^{s'}|_p = |n^s|_p |1 - n^{s'-s}|_p = |1 - n^{s'-s}|_p = |1 - (1+mp)^{s''p^N}|_p.$$

But by expanding $(1+mp)^{s''p^N}$, we notice that each term in $1-(1+mp)^{s''p^N}$ is divisible by at least p^{N+1}. Thus,

$$|n^s - n^{s'}|_p \leq |p^{N+1}|_p = \frac{1}{p^{N+1}}.$$

In other words, if $s - s'$ is divisible by p^N, then $n^s - n^{s'}$ is divisible by p^{N+1}. Hence, when n satisfies $n \equiv 1 \,(\mathrm{mod}\, p)$, it is justified to define the function $f(s) = n^s$ for any p-adic integer s as the p-adic integer that corresponds to the limit of the sequence n^{s_i}. Here, s_i represents a sequence of non-negative integers that converges to the p-adic integer s. In this manner, we extend the original function $f(s) = n^s$ defined on non-negative integers to encompass a broader domain of p-adic integers by considering the convergence behavior of the sequence n^{s_i}. (For example the partial sums of the p-adic expansion of (s)). Then, $f(s)$ is a continuous function from $\mathbb{Z}_p \to \mathbb{Z}_p$.

We can improve the situation by allowing any n that is not divisible by p, provided that we also impose congruence conditions on s and s' modulo $(p-1)$, in addition to a large power of p. Specifically, we choose a fixed s_0 from the set $0,1,2,\cdots,p-2$, and instead of considering n^s for all non-negative integers s, we consider n^s for all $s = s_0 + (p-1)s_1$, where s_1 is any non-negative integer. In this way, we examine $n^{s_0+(p-1)s_1}$ for different values of s_1. We can do this because then

$$n^s = n^{s_0}(n^{p-1})^{s_1},$$

and for any n not divisible by p we have $n^{p-1} \equiv 1 \pmod p$. Thus, we are in the situation of the last paragraph with n^{p-1} in place of n and s_1 in place of s.

Remark 4.1.1. *This p-adic interpolation applies word-by-word to the function $f(s) = n^{-s}$.*

The direct method for interpolating the Riemann zeta function, $\zeta(s)$, in the p-adic setting would involve interpolating each term of the series individually and then summing up the interpolated results. Nonetheless, this approach is not successful since the terms that are eligible for interpolation, which are those n such that p does not divide n, constitute an infinite series that diverges within the ring of p-adic integers.

The initial step is to extract the terms from the Riemann zeta function in a manner suitable for p-adic interpolation. As observed earlier, we need to exclude the terms where n is divisible by p. We do this as follows:

$$\zeta(s) = \sum_{n=1,\, p\nmid n}^{\infty} \frac{1}{n^s} + \sum_{n=1,\, p\mid n}^{\infty} \frac{1}{n^s} = \sum_{n=1,\, p\nmid n}^{\infty} \frac{1}{n^s} + \sum_{n=1}^{\infty} \frac{1}{p^s n^s}$$

$$= \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s} + \frac{1}{p^s}\zeta(s)$$

$$\zeta(s) = \frac{1}{1-(1/p^s)} \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s}.$$

It is this last sum

$$\zeta^*(s) = \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s} = (1-\frac{1}{p^s})\zeta(s)$$

which we will be dealing with later. This process is known as "taking out the p-Euler factor." The reason is that $\zeta(s)$ has the famous expansion

$$\zeta(s) = \prod_{\text{primes } q} \frac{1}{1-(1/q^s)}.$$

The factor $1/(1-1/q^s)$ is called the "q-Euler factor." Thus, multiplying $\zeta(s)$ by $(1-1/p^s)$ amounts to removing the p-Euler factor:

$$\zeta^*(s) = \prod_{\text{primes } q\neq p} \frac{1}{1-(1/q^s)}.$$

4.2 Definition of the p-Adic zeta function

Any measure μ on $\mathbb{Z}_p$ can be restricted to X if X is a compact-open subset of $\mathbb{Z}_p$. This means that we define a measure μ^* on X by setting $\mu^*(U) = \mu(U)$ whenever U is a compact open in X. In terms of integrating functions, we have

$$\int f\mu^* = \int f.(characteristic\ function\ of\ X).\mu$$

We shall use the notation $\int_X f\mu$ for the restricted integral $\int f\mu^*$.
We said that we want to interpolate $-B_k/k$. We have the following relation

$$\int_{\mathbb{Z}_p} 1.\mu_{B,k} = \mu_{B,k}(\mathbb{Z}_p) = B_k.$$

This equality is easy to be seen with having $N = 0$, $a = 0$ in $\mu_{B,k}(a+p^N\mathbb{Z}_p)$. Therefore, we want to interpolate the numbers

$$(-1/k)\int_{\mathbb{Z}_p} 1.\mu_{B,k}. \tag{4.1}$$

One question that might arise is if the distributions $\mu_{B,k}$ are connected in any obvious ways for different k? Not quite, however (3.3.7) shows that the regularised measure $\mu_{k,\alpha}$ is connected to $\mu_{1,\alpha}$. (3.3.7) and (3.3.9) have the following consequence, which is more precise:

Proposition 4.2.1. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be the function $f(x) = x^{k-1}$(k a fixed positive integer). Let X be a compact-open subset of $\mathbb{Z}_p$. Then*

$$\int_X 1.\mu_{k,\alpha} = k \int_X f \mu_{1,\alpha}$$

Proof. By (3.3.7), we have

$$d_k \mu_{k,\alpha}(a + (p^N)) \equiv d_k k a^{k-1} \mu_{1,\alpha}(a + (p^N)) \pmod{p^{N-ord_p(d_k)}}$$

Now, assuming that N is large enough so that X is a union of intervals of the form $a + (p^N)$, we have

$$\int_X 1.\mu_{k,\alpha} = \sum_{0 \le a < p^N,\, a+(p^N) \subset X} \mu_{k,\alpha}(a + (p^N))$$

$$\equiv \sum_{0 \le a < p^N,\, a+(p^N) \subset X} k a^{k-1} \mu_{1,\alpha}(a + (p^N)) \pmod{p^{N-ord_p(d_k)}}$$

$$= k \sum_{0 \le a < p^N,\, a+(p^N) \subset X} f(a) \mu_{1,\alpha}(a + (p^N)).$$

Taking the limit as $N \to \infty$ gives us $\int_X 1.\mu_{k,\alpha} = k \int_X f \mu_{1,\alpha}$. □

If we replace f by x^{k-1} in our notation, treating x as a variable of integration, we may write this proposition as

$$\int_X 1.\mu_{k,\alpha} = k \int_X x^{k-1} \mu_{1,\alpha} \tag{4.2}$$

From the perspective of p-adic interpolation, the right-hand side appears considerably better than the left-hand side because the k appearing doesn't occur strangely in the subscript of μ but rather in the exponent. The story for interpolating the integrand x^{k-1} for any fixed x is known from before. Namely, we are in business as long as $x \not\equiv 0 \pmod p$. To ensure that this property exists for all of our x's in the integration domain, we must take $X = \mathbb{Z}_p^\times$.
Thus, we claim that the expression $(-1/k) \int_{\mathbb{Z}_p^\times} 1.\mu_{B,k}$ can be interpolated. To accomplish this, we add the outcomes of interpolation discussion to (3.3.12).
That corollary tells us that if $|f(x) - x^{k-1}|_p \le \varepsilon$ for all $x \in \mathbb{Z}_p^\times$, then

$$\left| \int_{\mathbb{Z}_p^\times} f(x) \mu_{1,\alpha} - \int_{\mathbb{Z}_p^\times} x^{k-1} \mu_{1,\alpha} \right|_p \le \varepsilon.$$

(Recall that $|\mu_{1,\alpha}(U)|_p \le 1$ for all compact-open $U \subset X$).
Choose for f the function $x^{k'-1}$ where $k \equiv k' \pmod{p-1}$ and $k \equiv k' \pmod{p^N}$ or writing

these two as $k \equiv k' \,(\mathrm{mod}\,(p-1)p^N)$. By the interpolating discussion, we know that

$$|x^{k'-1} - x^{k-1}|_p \leq \frac{1}{p^{N+1}}.$$

Thus

$$\left| \int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha} - \int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} \right|_p \leq \frac{1}{p^{N+1}}.$$

We conclude that for any $s_0 \in \{\textit{Positive integers congruent to } s_0 \textit{ mod } (p-1)\}$, we can extend the function of k given by $\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}$ to a continuous function of p-adic integers s,

$$\int_{\mathbb{Z}_p^\times} x^{s_0+s(p-1)-1}\mu_{1,\alpha}.$$

However, we have slightly deviated from the numbers we started with ,i.e, $(-1/k)\int_{\mathbb{Z}_p^\times} 1.\mu_{B,k}$. We just saw that we can interpolate

$$\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} = 1/k \int_{\mathbb{Z}_p^\times} 1.\mu_{k,\alpha}.$$

Let us relate the numbers (4.1) and (4.2)

$$\frac{1}{k}\int_{\mathbb{Z}_p^\times} 1.\mu_{k,\alpha} = \frac{1}{k}\mu_{k,\alpha}(\mathbb{Z}_p^\times)$$

$$= \frac{1}{k}(1-\alpha^{-k})(1-p^{k-1})B_k$$

$$= (\alpha^{-k}-1)(1-p^{k-1})\left(-\frac{1}{k}\int_{\mathbb{Z}_p^\times} 1.\mu_{B,k}\right).$$

The second equality holds because first note that $\mathbb{Z}_p = \mathbb{Z}_p^\times \sqcup p\mathbb{Z}_p$, therefore

$$\mu_{k,\alpha}(\mathbb{Z}_p^\times) = \mu_{k,\alpha}(\mathbb{Z}_p) - \mu_{k,\alpha}(p\mathbb{Z}_p)$$

and

$$\frac{1}{k}\mu_{k,\alpha}(\mathbb{Z}_p^\times) = \frac{1}{k}\Big(\mu_{B,k}(\mathbb{Z}_p) - \alpha^{-k}\mu_{B,k}(\alpha\mathbb{Z}_p) - \mu_{B,k}(p\mathbb{Z}_p) + \alpha^{-k}\mu_{B,k}(p\alpha\mathbb{Z}_p)\Big)$$

$$= \frac{1}{k}\Big(\mu_{B,k}(\mathbb{Z}_p)(1-\alpha^{-k}) - p^{k-1}\mu_{B,k}(\mathbb{Z}_p)(\alpha^{-k}-1)\Big)$$

$$= -\frac{1}{k}\mu_{B,k}(\mathbb{Z}_p)(\alpha^{-k}-1)(1-p^{k-1}).$$

The term $1-p^{k-1}$ made its appearance because we had to restrict our integration from $\mathbb{Z}_p$ to $\mathbb{Z}_p^\times$. As we have discussed, n^s can not be interpolated when $p \mid n$. We must remove the "p-Euler factor" from the ζ-function before it can be interpolated. So we will interpolate the numbers $1-p^{k-1}(-B_k/k)$,

$$(1-p^{k-1})(-\frac{B_k}{k}) = \frac{1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}.$$

One slight deviation we would notice now is that the Euler term is $1-p^{k-1}$ and not $1-p^{-k}$ as you might think it should be from the discussion of interpolation. It is as though, instead of $\zeta(k)$, we were really interpolating $\zeta(1-k)$ (which we have not yet defined what this means for positive k). So we define our p-adic ζ-function to have the value $(1-p^{k-1})(-\frac{B_k}{k})$ at the integer $1-k$, not at k itself.

Definition 4.2.2. *If k is a positive integer, let*

$$\zeta_p(1-k) = (1-p^{k-1})(-\frac{B_k}{k})$$

so that by preceding paragraph,

$$\zeta_p(1-k) = \frac{1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}.$$

Note that the expression on the right is independent of α, i.e., if $\beta \in \mathbb{Z}$, $p \nmid \beta \neq 1$, then $(\beta^{-k}-1)^{-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} = (\alpha^{-k}-1)^{-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}$ since both equal $(1-p^{k-1})(-\frac{B_k}{k})$. This independence of α will be used later when we want to define $\zeta_p(s)$ for p-adic s.
We now prove several fundamental properties of Bernoulli numbers derived by Kummer, Clausen, and von staudt. Until their relationship with the Kubota-Leopoldt ζ_p and Mazur's measure theoretic was uncovered, these facts were regarded as sophisticated yet enigmatic curiosities. However, it was eventually revealed that they emerge naturally from basic "calculus-type" considerations.

Theorem 4.2.3. *(Kummer for (1) and (2), Clausen and von staudt for (3))*
(1) If $p-1 \nmid k$, then $|B_k/k|_p \leq 1$
(2)If $p-1 \nmid k$ and if $k \equiv k' \,(\mathrm{mod}\,(p-1)p^N)$, then

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B'_k}{k'}\,(\mathrm{mod}\,p^{N+1})$$

(3) If $p-1 \mid k$ (or if $p=2$ and k is even or $k=1$), then

$$pB_k \equiv -1\,(\mathrm{mod}\,p)$$

Proof. We assume $p>2$, and leave the proof of (3) when $p=2$.
Here we need the fact that the multiplicative group of nonzero residue classes of $\mathbb{Z}$ modulo p is a cyclic of order $p-1$, i.e,. there exists an $\alpha \in \{2,3,4,\cdots,p-1\}$ such that α^{p-1} is the lowest positive power of α which is congruent to 1 modulo p. In the proof

of part (1) and (2), we choose our "measure regularizer" α to be such a generator in $\{2,3,4,\cdots,p-1\}$. This means that, since $p-1 \nmid (-k)$, we have $\alpha^{-k} \not\equiv 1$ modulo p, so that $(\alpha^{-k}-1)^{-1} \in \mathbb{Z}_p^\times$
To prove (1), we are assuming $k>1$ (since for $k=1$ and $p>2$ we have $|B_1/1|_p = |-1/2|_p = 1$). We write

$$|B_k/k|_p = |1/(\alpha^{-k}-1)|_p |1/(1-p^{k-1})|_p| \int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}|_p$$

$$= |\int_{\mathbb{Z}_p^\times} x^{k-1} d\mu_{1,\alpha}|_p \leq 1,$$

by (3.3.11).
To prove (2), we rewrite the desired congruence as

$$\frac{1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} \equiv \frac{1}{\alpha^{-k'}-1}\int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha} \,(\operatorname{mod} p^{N+1}).$$

Notice that if for a, b , c, $d \in \mathbb{Z}_p$ we have $a \equiv c$ and $b \equiv d \,(\operatorname{mod} p^n)$, then we also have $ab \equiv cb \equiv cd \,(\operatorname{mod} p^n)$. Therefore, since $a = 1/(\alpha^{-k}-1)$, $b = \int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}$, $c = 1/(\alpha^{-k'}-1)$ and $d = \int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha}$ are in $\mathbb{Z}_p$, it only suffices to prove that $(\alpha^{-k}-1)^{-1} \equiv (\alpha^{-k'}-1)^{-1} \,(\operatorname{mod} p^{N+1})$ and $\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} \equiv \int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha} \,(\operatorname{mod} p^{N+1})$. The first reduces to $\alpha^k \equiv \alpha^{k'}$ (mod p^{N+1}) (by the corollary 3.3.12), and the second reduces to $x^{k-1} \equiv x^{k'-1} \,(\operatorname{mod} p^{N+1})$ for all $x \in \mathbb{Z}_p^\times$. But this all follows from the discussion in (4.1).
We conclude by demonstrating the Clausen-von Staudt congruence. Let $a = 1+p$ for this, and remember that we are proving it when $p>2$. We have

$$pB_k = -kp(-B_k/k) = \frac{-kp}{\alpha^{-k}-1}(1-p^{k-1})^{-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}.$$

First take the first of the three factors on the right. If we let $d = ord_p k$, then

$$\alpha^{-k}-1 = (1+p)^{-k}-1 \equiv -kp \,(\operatorname{mod} p^{d+2})$$

so that

$$1 \equiv \frac{-kp}{\alpha^{-k}-1} \,(\operatorname{mod} p).$$

Next, since k must be ≥ 2, we have $(1-p^{k-1})^{-1} \equiv 1 \,(\operatorname{mod} p)$. Thus,

$$pB_k \equiv \int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} \,(\operatorname{mod} p).$$

Again by using corollary (3.3.12), we obtain

$$pB_k \equiv \int_{\mathbb{Z}_p^\times} x^{-1}\mu_{1,\alpha} \pmod p.$$

But this integral is congruent to -1 $\pmod p$. □

We now return to p-adic interpolation.

Definition 4.2.4. *Fix $s_0 \in \{0,1,2,\cdots,p-2\}$. For $s \in \mathbb{Z}_p$ ($s \neq 0$ if $s_0 = 0$), we define*

$$\zeta_{p,s_0}(s) = \frac{1}{\alpha^{-(s_0+(p-1)s)} - 1}\int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)s-1}\mu_{1,\alpha}.$$

It should be now clear that this definition makes sense, namely, $\alpha^{-(s_0+(p-1)s)} = \alpha^{-s_0}(\alpha^{p-1})^{-s}$ and $x^{-(s_0+(p-1)s-1)}$ for any $x \in \mathbb{Z}_p^\times$ are defined for p-adic s by taking any sequence $\{k_i\}$ of positive integers which approach s p-adically. Another way to define $\zeta_{p,s_0}(s)$ is as follows: $-\lim_{k_i\to s}(1-p^{s_0+(p-1)k_i-1})B_{s_0+(p-1)k_i}/(s_0+(p-1)k_i)$.
We now see that if k is a positive integer congruent to s_0 (mod $p-1$), i.e., $k = s_0+(p-1)k_0$, then we have : $\zeta_p(1-k) = \zeta_{p,s_0}(k_0)$. We think of the ζ_{p,s_0} as p-adic "branches" of ζ_p, one for each congruence class mod $p-1$. (But note that the odd congruence classes -$s_0 = 1,3,5,...,p-2-$ give us the zero function, since for each s_0 always $B_{s_0+(p-1)k_i} = 0$, so we are only interested in even s_0).

We excluded the scenario where $s = 0$ and $s_0 = 0$ in the definition of ζ_{p,s_0}. The reason for this exclusion is that when $s = 0$ and $s_0 = 0$, the term $\alpha^{-(s_0+(p-1)s)}$ becomes equal to 1, causing the denominator to vanish. By expressing $\zeta_p(1-k)$ as $\zeta_{p,s_0}(k_0)$, where $k = s_0+(p-1)k_0$, we can associate this excluded case with $\zeta_p(1)$. Consequently, similar to the Archimedean Riemann zeta-function, the p-adic zeta-function has a pole at l.

Theorem 4.2.5. *For fixed p and fixed s_0, $\zeta_{p,s_0}(s)$ is a continuous function of s which does not depend on the choice of $\alpha \in \mathbb{Z}$, $p \nmid \alpha$, and $\alpha \neq 1$, which appears in its definition.*

Proof. The implication that the integral is a continuous function of s follows from two key points: section (4.1) and the corollary presented at the end of section (3.3). The factor $1/(\alpha^{-(s_0+(p-1)s)} - 1)$ can be considered a continuous function, given that we exclude the case where $s = 0$ when $s_0 = 0$. This exclusion is necessary because the term $\alpha^{-(s_0+(p-1)s)}$ is a continuous function, as stated in section (4.1). So $\zeta_{p,s_0}(s)$ is also continuous.
To demonstrate that $\zeta_{p,s_0}(s)$ does not depend on the choice of α, we can consider an alternative choice for α, denoted as β. Here, we assume that β belongs to the set of integers $\mathbb{Z}$, satisfies $p \nmid \beta$, and $\beta \neq 1$. The two functions

$$\frac{1}{\alpha^{-(s_0+(p-1)s)} - 1}\int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)s-1}\mu_{1,\alpha}$$

and

$$\frac{1}{\beta^{-(s_0+(p-1)s)}-1}\int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)s-1}\mu_{1,\alpha}$$

agree whenever $(s_0 + (p-1)s) = k$ is an integer greater than 0, i.e., whenever s is a non-negative integer ($s > 0$ if $s_0 = 0$), since in that case both functions equal $(1-p^{k-1})(-B_k/k)$. But the non-negative integers are dense in $\mathbb{Z}_p$, so that any two continuous functions which agree there are equal. Therefore, taking β instead of α does not affect the function. □

(4.2.5) gives us our p-adic interpolation of the "interesting factor $-B_{2k}/2k$ in $\zeta(1-2k)$ and we are done.

4.3 Definition of the p-Adic L-function

We will now begin building the p-adic L-function. We fix a primitive Dirichlet character modulo d,

$$\chi\ :\ (\mathbb{Z}/d\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$$

which can be considered as a function

$$\chi\ :\ \mathbb{Z} \to \overline{\mathbb{Q}}$$

by extending to n not prime to d.
Recall the equation (2.7) if $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ is analytically continued to the complex plane, we have:

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}$$

for $n \geq 2$.
Note that the $B_{n,\chi}$'s are in the field $\mathbb{Q}(\chi)$ obtained by adjoining the values of χ to $\mathbb{Q}$. The p-adic analogue of $L(s,\chi)$ for any prime is formed by these algebraic special values of $L(s,\chi)$, which can be studied arithmetically.
Now, let $\mathbb{Z}_p, \mathbb{Z}_p^\times, \mathbb{Q}_p, \mathbb{C}_p$ denote respectively the ring of p-adic integers, multiplicative group of $\mathbb{Z}_p$, the field of fractions of $\mathbb{Z}_p$ and the p-adic completion of an algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$. The functions $ord_p p$ and $|x|_p$ are normalised so that $ord_p p = 1$.

We establish a fixed embedding of the field $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$, also with embedding $\overline{\mathbb{Q}} \to \mathbb{C}$, then any algebraic number will be regarded as being both p-adic and complex number.

The same letter χ will specifically designate the character on $(\mathbb{Z}/d\mathbb{Z})^\times$ thought to take values in $\mathbb{C}$ or $\mathbb{C}_p$. For any $a \in \mathbb{Z}_p^\times$, let $\omega(a)$ be the unique $(p-1)$st root of 1 in $\mathbb{Z}_p^\times$ which reduces to a modulo p. It also can be seen that $\omega(a) = \lim_{n\to\infty} a^{p^n}$. Also note that $\mathbb{Z}_p^\times$ can be decomposed directly as $V \times D$ where V is the cyclic group of order $p-1$

consisting of $(p-1)$st roots of unity in $\mathbb{Q}_p$ and D is the interval in $\mathbb{Z}_p^\times$, $1+p\mathbb{Z}_p$ $(1+4\mathbb{Z}_p$, if $p=2)$. Then, each $a \in \mathbb{Z}_p^\times$ can be written uniquely as $a = \omega(a) \times \langle a \rangle$ where ω and $\langle\rangle$ denote the projections of a on V and D respectively.
Now, if we let $\overline{\mathbb{Q}}$ be the field of all algebraic numbers, i.e., the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, with an imbedding $\overline{\mathbb{Q}} \to \mathbb{C}$ and considering $\overline{\mathbb{Q}}$ as a subfield of $\mathbb{C}$, then V in $\mathbb{C}$ is identified with the group of roots of unity in $\overline{\mathbb{Q}}$ with order $p-1$, namely with a subgroup of $\mathbb{C}^\times$. Hence, defining $\omega(a) = 0$ for $a \in \mathbb{Z}$ that is not relatively prime to p, we obtain a character

$$\mathbb{Z} \to \mathbb{C}$$

$$a \mapsto \omega(a)$$

with the conductor p and this induces an isomorphism

$$(\mathbb{Z}/p\mathbb{Z})^\times \cong V \subset \mathbb{C}^\times$$

Note that for the case $p=2$ we have $V = \{1, -1\}$.
Finally, let χ_n denote the primitive character induced by $\chi\overline{\omega}^n$($\overline{\omega}$ denote the complex conjugate character $\overline{\omega} = \omega^{-1}$).
Now, we get to the proposition of Kubota- Leopoldt and Iwasawa.

Proposition 4.3.1. *(Kubota-Leopoldt [10] and Iwasawa [2]) There exists a unique p-adic meromorphic (analytic if $\chi \neq \chi_0$) function $L_p(s,\chi)$, $s \in \mathbb{Z}_p$ for which*

$$L_p(1-n,\chi) = (1-\chi_n(p)p^{n-1})L(1-n,\chi_n). \tag{4.3}$$

The measure-theoretic approach used by Mazur is slightly modified by us. one of the numerous ways to prove the claim that are now possible. One of the most important steps in the proof is the inclusion of the "twisted" L-function which is defined as $L(s,\chi,\xi) = \sum \frac{\chi(n)}{n^s}\xi^n$ where ξ is a rth root of unity such that $(r,pd) = 1$.
Such L-series (for $r = d$) are used classically to prove the formula for $L(1,\chi)$.
We now sketch a similar argument for the formula:

$$L(1-n,\chi,\xi) = -\frac{1}{n}B_{n,\chi,\xi} \tag{4.4}$$

where $B_{n,\chi,\xi}$'s are defined as follows:

$$F_\xi(z) = \sum_{0\leq a<d} \frac{\chi(a)\xi^a z e^{az}}{\xi^d e^{dz}-1} = \sum_{n=0}^{\infty} B_{n,\chi,\xi}\frac{z^n}{n!} \tag{4.5}$$

where χ is the character modulo d. Let $r > 1$ be an integer prime to pd and let $\xi^r = 1$ and $\xi \neq 1$.
Similarly, define

$$G_\xi(z) = \sum_{0 \le a < d} \frac{\chi(a)\xi^a e^{-az}}{1 - \xi^{-d} e^{-dz}}$$

We obtain that

$$F_\xi(-z) = zG_\xi(z)$$

and

$$H_\xi(s) = \int_{C_\varepsilon} F_\xi(z) z^{s-1} \frac{dz}{z}$$

and the contour C_ε is the same contour as in (2.3.5). With the similar calculations and assuming $t > 0$,

$$H_\xi(s) = -(e^{\pi i s} - e^{-\pi i s}) \int_0^\infty G_\xi(t) t^{s-1}\, dt$$

and

$$\begin{aligned} \int_0^\infty G_\xi(t) t^{s-1}\, dt &= \int_0^\infty \sum_{n=1}^\infty \chi(n) e^{-nt} t^{s-1} \xi^n \, dt \\ &= \sum_{n=1}^\infty \chi(n)\xi^n \int_0^\infty e^{-nt} t^{s-1}\, dt \\ &= \sum_{n=1}^\infty \chi(n)\xi^n n^{-s} \Gamma(s) = L(s,\chi,\xi)\Gamma(s) \end{aligned}$$

we get that

$$H_\xi(s) = L(s,\chi,\xi)\Gamma(s).$$

If we put $s = 1 - n$,

$$\begin{aligned} -\frac{L(1-n,\chi,\xi)}{\Gamma(n)} &= res_0(F_\xi(z) z^{-n-1}) = res_0(z^{-n-1} \sum_{n=0}^\infty B_{n,\chi,\xi} \frac{z^n}{n!}) \\ &= -\frac{1}{n} B_{n,\chi,\xi}. \end{aligned}$$

Note that by replacing n by $n+1$, we may write

$$L(-n,\chi,\xi) = -\frac{1}{n+1} B_{n+1,\chi,\xi} = \text{ coefficient } of\ \frac{t^{n+1}}{n!}\ in \sum_{0 \le a < d} \frac{\chi(a)\xi^a e^{at}}{1 - \xi^d e^{dt}}.$$

Now, define $X = \varprojlim (\mathbb{Z}/dp^N\mathbb{Z})$. Let $a + dp^N \mathbb{Z}_p, 0 \le a < dp^N$ denote the set of $x \in X$ such that $|x - a|_p \le \frac{1}{p^N}$ which also map to a under the natural map $X \to \mathbb{Z}/dp^N\mathbb{Z}$ and let $X^\times = \bigcup'_{0 \le a < dp} a + dp\mathbb{Z}_p$ be the unit group (where $'$ will always denote omission of indices divisible by p). The character χ can be pulled back to X via the map $X \to \mathbb{Z}/d\mathbb{Z}$.

We fix the following measure to begin working with the mazur's measure-theoretic strategy.

Definition 4.3.2. *Let $z \in \mathbb{C}_p$ be such that $z^{dp^N} \neq 1$ for all N, define:*

$$\mu_z(a + dp^N\mathbb{Z}_p) = \frac{z^a}{1 - z^{dp^N}}. \tag{4.6}$$

Proposition 4.3.3. *μ_z is finitely additive. Let $D_1 = \{x \in \mathbb{C}_p \mid |x-1|_p < 1\}$ and let $\overline{\mathrm{D_1}} = \mathbb{C}_p - D_1$ be the complement of the open unit disc around 1. Then,*

$$\mu_z, is, a, measure(i.e., is, bounded) \iff z \in \overline{\mathrm{D_1}}.$$

Proof. The verification of the additivity is as follows:

$$\sum_{j=0}^{p-1} \mu_z(a + jdp^N + dp^{N+1}\mathbb{Z}_p) = \sum_{j=0}^{p-1} \frac{z^{a+jdp^N}}{1 - z^{dp^{N+1}}}$$

$$= \frac{z^a}{1 - z^{dp^{N+1}}} \sum_{j=0}^{p-1} z^{jdp^N} = \frac{z^a}{1 - z^{dp^{N+1}}} \frac{1 - z^{(dp^N)^p}}{1 - z^{dp^N}}$$

$$= \frac{z^a}{1 - z^{dp^N}} = \mu_z(a + dp^N\mathbb{Z}_p).$$

Now, if $z \in D_1$, then z^{dp^N} goes to 1 p-adically and

$$|\mu_z(a + dp^N\mathbb{Z}_p)|_p = \frac{1}{|1 - z^{dp^N}|_p}$$

which is not bounded. For the opposite direction, if $z \in \overline{D_1}$ and $|z|_p > 1$, then $|1 - z^{dp^N}|_p = |z^{dp^N}|_p$ and $|\mu_z(a + dp^N\mathbb{Z}_p)|_p = |z^{a-dp^N}|_p < 1$ since $0 \leq a < dp^N$. Moreover, if $z \in \overline{D_1}$ and $|z|_p \leq 1$, then since $|1 - z^{dp^N}|_p \geq 1$, we have

$$|\mu_z(a + dp^N\mathbb{Z}_p)|_p \leq \frac{1}{|1 - z^{dp^N}|_p} \leq 1$$

□

The classical Haar measure, dx/x is virtually as significant a measure for $\mathbb{R}^\times$ as μ is for X. There can be no translation invariant measure on X that is not zero. However, μ makes as good an attempt at invariance as one can hope in the p-adic situation:

$$\mu_z(p\alpha) = \frac{z^{pa}}{1 - z^{dp^N}} = \mu_{z^p}(\alpha) \tag{4.7}$$

where α is an interval of the form $\alpha = a + dp^N\mathbb{Z}_p$.

Recall that a measure μ can be extended to a continuous function:

$$\int_X f\,d\mu = \lim_{N\to\infty} \sum_{0\le a<dp^N} f(a)\mu_z(a+dp^N\mathbb{Z}_p) \tag{4.8}$$

The most important μ_z are when $z=\xi$ is an rth root of 1, $\xi\neq 1$ and r relatively prime to pd. We observe that $\xi\in\overline{D_1}$.
Now, fix any $t\in\mathbb{C}_p$ with $ord_p t > 1/(p-1)$. Then the sum $\sum(tx)^n/n!$ converges to e^{tx} and we can show that:

$$\int_X e^{tx}\chi(x)\,d\mu_\xi = \sum_{0\le a<d} \frac{\chi(a)\xi^a e^{at}}{1-\xi^d e^{dt}}. \tag{4.9}$$

We can see this with the following calculations:

$$\int_X e^{tx}\chi(x)\,d\mu_\xi = \lim_{N\to\infty}\sum_{0\le a<dp^N} e^{ta}\chi(a)\frac{\xi^a}{1-\xi^{dp^N}} =$$

$$\lim_{N\to\infty}\Big(\sum_{0\le a<dp} e^{ta}\chi(a)\frac{\xi^a}{1-\xi^{dp^N}} + ... + \sum_{(p^N-1)d\le a<dp^N} e^{ta}\chi(a)\frac{\xi^a}{1-\xi^{dp^N}}\Big)$$

$$= \lim_{N\to\infty}\Big(\sum_{0\le a<d} e^{ta}\chi(a)\frac{\xi^a}{1-\xi^{dp^N}} + ... + \sum_{0\le a<d} e^{t(a+d(p^N-1))}\chi(a+d(p^N-1))\frac{\xi^{a+d(p^N-1)}}{1-\xi^{dp^N}}\Big)$$

$$= \lim_{N\to\infty}\sum_{0\le a<d} e^{ta}\chi(a)\frac{\xi^a}{1-\xi^{dp^N}} + ... + \sum_{0\le a<d} e^{ta}e^{td(p^n-1)}\chi(a)\frac{\xi^a\xi^{d(p^N-1)}}{1-\xi^{dp^N}}$$

$$= \lim_{N\to\infty}\Big(\sum_{0\le a<d}\frac{\chi(a)e^{ta}\xi^a}{1-\xi^{dp^N}}\Big(\sum_{j=0}^{p^N-1} e^{tdj}\xi^{dj}\Big)\Big) = \lim_{N\to\infty}\Big(\sum_{0\le a<d}\frac{\chi(a)e^{ta}\xi^a}{1-\xi^{dp^N}}.\frac{1-e^{tdp^N}\xi^{dp^N}}{1-\xi^d e^{td}}\Big)$$

$$= \Big(\sum_{0\le a<d}\frac{\chi(a)e^{ta}\xi^a}{1-\xi^d e^{td}}\Big).\lim_{N\to\infty}\frac{1-e^{tdp^N}\xi^{dp^N}}{1-\xi^{dp^N}}$$

We note that $\lim_{N\to\infty}\frac{1-e^{tdp^N}\xi^{dp^N}}{1-\xi^{dp^N}} = 1$ because:

$$\frac{1-e^{tdp^N}\xi^{dp^N}}{1-\xi^{dp^N}} = \frac{1-e^{tdp^N}\xi^{dp^N}+e^{tdp^N}-e^{tdp^N}}{1-\xi^{dp^N}}$$

$$= e^{tdp^N} + \frac{1-e^{tdp^N}}{1-\xi^{dp^N}}.$$

Then when we are taking the limit, the first term goes to 1 and the second term is zero because $\frac{1}{1-\xi^{dp^N}}$ is bounded.
Now since $ord_p t > 1/(p-1)$, then e^{tx} has the desired power series and we plug it into

the integral,

$$\sum_{n=0}^{\infty}\int_X \frac{(tx)^n}{n!}\chi(x)\,d\mu_\xi = \sum_{n=0}^{\infty}\frac{t^n}{n!}\int_X x^n\chi(x)\,d\mu_\xi \tag{4.10}$$

and by equating coefficients of $t^n/n!$ and comparing with (4.5) we have

$$L(-n,\chi,\xi) = \int_X x^n\chi(x)\,d\mu_\xi. \tag{4.11}$$

In another saying, a p-adic integral has been used to express the algebraic number $L(-n,\chi,\xi)$. We would like to interpolate these special values into the p-adic interpolating function $L_p(s,\chi,\xi)$. Just as the classical $L(s,\chi,\xi)$ interpolates these special values at negative integers, i.e., we would like to let $-n$ approach p-adic numbers $s \in \mathbb{Z}_p$. But, in order for (4.11) to approach a p-adic limit as $-n \to s$, we must modify the integral by replacing $\int_X$ by $\int_{X^\times}$ and then x by $\langle x\rangle = x/\omega(x)$ which is 1 modulo p. More precisely, by (4,6) and the fact that $X = X^\times \bigcup pX$, then:

$$\int_X x^n\chi(x)\,d\mu_\xi = \lim_{N\to\infty}\sum_{0\le a<dp^N} a^n\chi(a)\mu_\xi(a+dp^N\mathbb{Z}_p)$$

$$= \lim_{N\to\infty}\sideset{}{'}\sum_{0\le a<dp^N} a^n\chi(a)\mu_\xi(a+dp^N\mathbb{Z}_p) + \lim_{N\to\infty}\sum_{0\le a<dp^{N-1}}(pa)^n\chi(pa)\mu_\xi(pa+dp^N\mathbb{Z}_p)$$

$$= \lim_{N\to\infty}\sideset{}{'}\sum_{0\le a<dp^N} a^n\chi(a)\mu_\xi(a+dp^N\mathbb{Z}_p) + p^n\chi(p)\lim_{N\to\infty}\sum_{0\le a<dp^{N-1}} a^n\chi(a)\mu_{\xi^p}(a+dp^N\mathbb{Z}_p)$$

Then taking the limit over N,

$$\int_{X^\times} x^n\chi(x)\,d\mu_\xi = \int_X x^n\chi(x)\,d\mu_\xi - p^n\chi(p)\int_X x^n\chi(x)\,d\mu_{\xi^p}$$

$$= L(-n,\chi,\xi) - p^n\chi(p)L(-n,\chi,\xi^p) \tag{4.12}$$

Replacing n by $n-1$ and then χ by χ_n, we obtain:

$$\int_{X^\times}\langle x\rangle^{n-1}\chi_1(x)\,d\mu_\xi(x) = L(1-n,\chi_n,\xi) - p^{n-1}\chi_n(p)L(1-n,\chi_n,\xi^p) \tag{4.13}$$

To define $L_p(s,\chi,\xi)$, we let $1-n \to s \in \mathbb{Z}_p$ on the left of (4.13), (this makes sense because $\langle x\rangle$ is 1 modulo p so it can be raised to a p-adic power), and we set

$$L_p(s,\chi,\xi) = \int_{X^\times}\langle x\rangle^{-s}\chi_1(x)\,d\mu_\xi(x). \tag{4.14}$$

In order to recover the untwisted L-function and demonstrate the proposition 1, first we observe the following relation which follows naturally from the definitions:

$$\sum_{\xi,\xi^r=1} L(s,\chi,\xi) = (r^{1-s}\chi(r) - 1)L(s,\chi) \quad for\ s \in \mathbb{C}, \tag{4.15}$$

since on the left we have,

$$\begin{aligned}\sum_{\xi,\xi^r=1} L(s,\chi,\xi) &= \sum_{\xi,\xi^r=1}\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}\xi^n = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}\sum_{k=1}^{r-1}e^{2\pi ikn/r}\\ &= \sum_{r|n}\frac{\chi(n)}{n^s}\sum_{k=1}^{r-1}e^{2\pi ikn/r} + \sum_{r\nmid n}\frac{\chi(n)}{n^s}\sum_{k=1}^{r-1}e^{2\pi ikn/r}\\ &= \sum_{r|n}\frac{\chi(n)}{n^s}\sum_{k=1}^{r-1}e^{2\pi ikn/r} + \sum_{r\nmid n}\frac{\chi(n)}{n^s}e^{2\pi in/r}\frac{e^{2\pi ikn(r-1)/r}-1}{e^{2\pi in/r}-1}\\ &= \frac{\chi(r)(r-1)}{r^s}L(s,\chi) - \sum_{r\nmid n}\frac{\chi(n)}{n^s}\\ &= \frac{\chi(r)(r-1)}{r^s}L(s,\chi) - (\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} - \sum_{r|n}\frac{\chi(n)}{n^s})\\ &= \frac{\chi(r)(r-1)}{r^s}L(s,\chi) - L(s,\chi)(1-\frac{\chi(r)}{r^s})\\ &= (r^{1-s}\chi(r)-1)L(s,\chi).\end{aligned}$$

So, By using this for $s = 1-n$ and summing (4.15) over non-trivial rth roots of unity ξ, we have

$$\begin{aligned}\sum_{\xi,\xi^r=1} L_p(1-n,\chi,\xi) &= \sum_{\xi,\xi^r=1}(L(1-n,\chi,\xi) - \chi_n(p)p^{n-1}L(1-n,\chi_n,\xi^p))\\ &= (r^n\chi_n(r)-1)L(1-n,\chi_n) - \chi_n(p)p^{n-1}(r^n\chi_n(r)-1)L(1-n,\chi_n)\\ &= (\langle r\rangle^n\chi_n(r)-1)(1-\chi_n(p)p^{n-1})L(1-n,\chi_n).\end{aligned}$$

By the fact that $\langle x\rangle = x/\omega(x)$ and $\chi_n = \chi\overline{\omega}^n$,
So we have:

$$\sum_{\xi,\xi^r=1} L_p(1-n,\chi,\xi) = (\langle r\rangle^n\chi_n(r)-1)(1-\chi_n(p)p^{n-1})L(1-n,\chi_n) \tag{4.16}$$

$$r^n\chi_n(r) = \langle r\rangle^n\omega(r)\chi(r)\overline{\omega}(r) = \langle r\rangle^n\chi(r).$$

Therefore, by putting

$$\mu = \sum_{\xi,\xi^r=1}\mu_\xi,$$

we define

$$L_p(s,\chi) = \frac{1}{\langle r\rangle^{1-s}\chi(r)-1}\sum_{\xi\ ,\xi^r=1} L_p(s,\chi,\xi) \tag{4.17}$$

$$= \frac{1}{\langle r\rangle^{1-s}\chi(r)-1}\int_{X^\times}\langle x\rangle^{-s}\chi_1(x)\,d\mu(x)$$

We will prove the formula (4.13) in the Proposition (4.3.1) which is called interpolation property, in the final section.
Note that $\mu = \sum_{\xi,\xi^r=1}\mu_\xi$ is Mazur's measure with "regularisation" $1/r$. By (4.16) , also for $n \geq 2$, we have:

$$f(n) =$$

$$\frac{1}{\langle r\rangle^{n}\chi(r)-1}\sum_{\xi,\xi^r=1} L_p(1-n,\chi,\xi) - \frac{1}{\langle r\rangle^{n}\chi(r)-1}\sum_{\xi,\xi^r=1} L_p(1-n,\chi,\xi') = 0,$$

where ξ' is an r'th root of unity. It follows that f is an analytic function on $\mathbb{Z}_p$ which has infinite zeros, therefore it is the zero function. We conclude that $L_p(s,\chi)$ is independent of r, even though the use of rth root of unity was essential in its construction. The factor $(1-\chi_n(p)p^{n-1})$ can be interpolated as removing "the Euler factor", i.e., the type of function which can be interpolated p-adically is

$$(1-\chi(p)p^{n-1})L(s,\chi) = \prod_{q\neq p,prime}((1-\chi(q)q^{-s}))^{-1}$$

The only thing left in the proof is to show that $L_p(s,\chi)$ is analytic (meromorphic if $\chi = \chi_{triv}$). So, we need to write it as a power series in the following way. Note that $\langle x\rangle^s$ is an analytic function of $s \in \mathbb{Z}_p$ and can be written as a power series:

$$< x >^s = \exp_p(s\log_p < x >) = \sum_{n=0}^{\infty}\frac{s^n\,(\log_p\langle x\rangle)^n}{n!}$$

Then,

$$L_p(s,\chi) = \frac{1}{\langle r\rangle^{1-s}\chi(r)-1}\int_{X^\times}\sum_{n=0}^{\infty}\frac{s^n\,(\log_p\langle x\rangle)^n}{n!}\chi(x)\,d\mu$$

$$= \frac{1}{\langle r\rangle^{1-s}\chi(r)-1}\sum_{n=0}^{\infty}s^n\int_{X^\times}\frac{(\log_p\langle r\rangle)^n}{n!}\chi(x)\,d\mu$$

and by taking $a_n = \int_{X^\times}\frac{(\log_p\langle x\rangle)^n}{n!}\chi(x)\,d\mu$, we get the following power series,

$$L_p(s,\chi) = \frac{1}{\langle r\rangle^{1-s}\chi(r)-1}\sum_{n=0}^{\infty}a_n s^n$$

which means that $L_p(s,\chi)$ is analytic. And when $\chi = \chi_0$ we get a meromorphic function with pole at $s = 1$.
Now we can derive the Leopoldt formula for $L_p(1,\chi)$. The classical formula for $L(1,\chi)$

can be derived by fourier inversion on the group $G = \mathbb{Z}/d\mathbb{Z}$ (see [7]). Let ζ be a fixed primitive dth root of 1, and define

$$\hat{f}(a) = \sum_{b \in G} f(b)\zeta^{-ab}$$

for a function f on G. Then

$$f(b) = \frac{1}{d} \sum_{a \in G} \hat{f}(a)\zeta^{ab}. \tag{4.18}$$

Applying fourier inversion to $f_s(b) = \sum_{n \equiv b} n^{-s}$ (suppose $Re(s) > 1$) and using the definition of $L(s,\chi)$ and $L(s,\chi_{triv},\xi)$, we have

$$\begin{aligned} L(s,\chi) &= \sum_{0 \leq b < d} \chi(b) f_s(b) = \frac{1}{d} \sum_{a,b} \chi(b) \hat{f}_s(a) \xi^{ab} \\ &= \frac{1}{d} \sum_{j} \chi(j) \xi^{j} \sum_{a} \overline{\chi}(a) \hat{f}_s(a) \\ &= \frac{g_\chi}{d} \sum_{a} \overline{\chi}(a) L(s,\chi_{triv},\zeta^{-a}), \end{aligned}$$

where $j = ab$ and $g_\chi = \sum_j \chi(j)\zeta^j$ is the Gauss sum. Letting $s \to 1$ and noting that $L(1,\chi_0) = -\log(1-\xi)$, we obtain

$$L(1,\chi) = -\frac{g_\chi}{d} \sum_{0 \leq a < d} \overline{\chi}(a) \log(1 - \zeta^{-a}) \tag{4.19}$$

Now let's move on to the p-adic situation.

Theorem 4.3.4. *(Leopoldt [11])*

$$L_p(1,\chi) = -\left(1 - \frac{\chi(p)}{p}\right) \frac{g_\chi}{d} \sum_{0 \leq a < d} \overline{\chi}(a) \log_p(1 - \zeta^{-a}))$$

Here $\log_p : \mathbb{C}_p^\times \to \mathbb{C}_p$ is the Iwasawa p-adic logarithm, the unique function which
(1) is given by the usual series $\sum (-1)^{n+1}(x-1)^n/n$ when $|x-1|_p < 1$
(2) satisfies

$$\log_p(xy) = \log_p(x) + \log_p(y) \tag{4.20}$$

and (3) is normalised by the condition

$$\log_p p = 0 \tag{4.21}$$

Remark that $\log_p x$ is locally analytic on $\mathbb{C}_p^\times$ in the (Kranser) sense that it can be represented by a convergent power series in a neighborhood of any point in its region

of definition with the derivative $1/x$.
The two ways that theorem (4.3.4) varies from (4.19) are as follows: the anticipated "removal of the Euler factor," which results in the expression $(1 - \chi(p)/p)$; and the substitution of log by $\log_p$,
Since $\log(1-\xi^{-a})$ is replaced with $\log_p(1-\xi^{-a})$, the formal series for the former does not converge p-adically, so that (4.20)and (4.21) are needed to evaluate $\log_p(1-\xi^{-a})$, the validity of the p-adic formula in theorem (4.3.4) may initially seem odd. Contrary to initial perceptions, however, the proof of Lemma (4.3.5) below demonstrates that Leopoldt's formula is actually supported by the same formal series along with a unique analytic continuation.

Lemma 4.3.5. *If $z \in \overline{D}_1$ and μ_z on $\mathbb{Z}_p$ is the measure given by (4.6) with $d = 1$, then*

$$\int_{\mathbb{Z}_p^\times} \frac{1}{x}\, d\mu_z(x) = -\frac{1}{p}\log_p \frac{(1-z)^p}{1-z^p}$$

Proof. If $|z|_p < 1$, first note that $\frac{1}{1-z^{p^N}} = 1 + z^{p^N} + z^{2p^N} + ...$ which goes to 1 as $N \to \infty$. Then the left side is

$$\lim_{N\to\infty} \sum_{0<j<P^N}{}' \frac{z^j}{j}\frac{1}{1-z^{p^N}} = \lim_{N\to\infty} \Big(\sum_{0<j<P^N} \frac{z^j}{j} - \sum_{0<j<P^{N-1}} \frac{z^{pj}}{pj} \Big)$$

$$= -\frac{1}{p}(\log_p(1-z)^p - \log_p(1-z^p))$$

We now use analytic continuation to extend the equality from $|z|_p < 1$ to all $z \in \overline{D}_1$. Note from [8] that a function is Kranser analytic on $\overline{D}_1$ if it is a uniform limit of rational functions with poles in D_1. The fact we need about such functions is that if two Kranser analytic functions on $\overline{D}_1$ are equal on a disc in $\overline{D}_1$, then they are equal on all of $\overline{D}_1$.
Consider that by newton binomial expansion and assuming that $|z|_p \le 1$,

$$\frac{(1-z)^p}{1-z^p} = 1 + \frac{1}{1-z^p} \sum_{0<j<p} \binom{p}{j} (-z)^j.$$

It can be seen that if $z \in \overline{\mathrm{D}}_1$ then $(1-z)^p/(1-z^p) \in D_1$ because:

$$\left|\frac{(1-z)^p}{1-z^p} - 1\right|_p = \left|\frac{1}{1-z^p} \sum_{0<j<p} \binom{p}{j}(-z)^j\right|_p \le Max_j\left\{\left|\frac{\binom{p}{j}(-z)^j}{1-z^p}\right|_p\right\} \le 1,$$

since for each j, $\binom{p}{j}(-z)^j \in \mathbb{Z}_p$ and $|\frac{1}{1-z^p}| = |1 + z^p + z^{2p} + ...|_p \le Max_i\{|z^i|_p\} = 1$.

Moreover, if $|z|_p > 1$, then

$$\frac{(1-z)^p}{1-z^p} = 1 + \frac{1}{1-z^{-p}} \sum_{0<j<p} \binom{p}{j} (-z)^{-j}.$$

Similarly, $|\frac{(1-z)^p}{1-z^p} - 1|_p \leq 1$ and we conclude that if $z \in \overline{D}_1$ then $(1-z)^p/(1-z^p) \in D_1$. Hence, both sides of the equality in the lemma are Kranser analytic functions of z on $\overline{D}_1$. The left side is the uniform limit of the rational functions(with poles in D_1)

$$\sum_{0<j<P^N}{}' \frac{z^j}{j} \frac{1}{1-z^{p^N}}$$

and the right side is the uniform limit of the rational functions (with poles in D_1)

$$\frac{1}{p} \sum_{j=1}^{N} \frac{(-1)^j}{j} \left(\frac{(1-z)^p}{1-z^p} - 1 \right)^j.$$

Since they agree on $\{z \mid |z|_p < 1\}$, they agree on all of $\overline{D}_1$ □

Lemma (4.3.5) will be applied when z is a root (but not a p^Nth root) of unity.

Remark 4.3.6. *1. If z is a $(p-1)$st root of 1, the right side of lemma (4.3.5) becomes $-(1-1/p)\log_p(1-z) = -\log_p(1-z) - \log_p(1-z)^{1/p}$. For example, setting $z = -1$ gives the following p-adic limit for $\log_p 2$*

$$\log_p 2 = -\frac{p}{2(p-1)} \lim_{N\to\infty} \sum_{0<j<P^N}{}' \frac{(-1)^j}{j}$$

2. Lemma (4.3.5) is the key step in our proof of Leopoldt's formula for $L_p(1,\chi)$. As mentioned before, the subtly in Leopoldt's formula is that $\log_p(1-\xi)$ is not given by the same formal series as $\log(1-\xi)$, since ξ is outside the disc of convergence of $\log_p(1-z)$. However, Lemma (4.3.5) shows that if we "correct by the frobenius" in the Dwork style (see, e.g., [9]), i.e., replace (1-z) by $(1-z)^p/(1-z^p)$, the resulting series is globally analytic out to ξ. The effect of this step on the formula for $L_p(1,\chi)$ is to bring out the Euler factor $1-\chi(p)/p$, as we shall see soon in (4.22).

The other ingredient in the proof of Theorem (4.3.4) is the analog of the Fourier inversion(4.18) used in the classical case.

Lemma 4.3.7. *For χ a primitive character mod d, ζ a fixed primitive dth root of 1, $g_\chi = \sum_j \chi(j)\xi^j$, $\xi \neq 1$ an rth root of 1, $(r,pd) = 1$, we have for any continuous $f : X \to \mathbb{C}_p$*

$$\int_X \chi f \, d\mu_\xi = \frac{g_\chi}{d} \sum_{0\leq a<d} \overline{\chi}(a) \int_X f \, d\mu_{\zeta^{-a}\xi}.$$

Proof. To proof Lemma (4.3.7), by linearity and continuity it suffices to prove it for $f =$ characteristic function of $j + dp^N\mathbb{Z}_p$. Therefore, on the right side we have:

$$= \frac{g_\chi}{d} \sum_{0\le a<d} \overline{\chi}(a) \sum_{0<j<dp^N} \frac{\zeta^{-aj}\xi^j}{1-\zeta^{-adp^N}\xi^{dp^N}}$$

$$= \frac{g_\chi}{d} \sum_{0\le a<d} \overline{\chi}(a)(\sum_{0<j<d} \frac{\zeta^{-aj}\xi^j}{1-\zeta^{-adp^N}\xi^{dp^N}} \sum_{k=0}^{p^N-1} \zeta^{-adk}\xi^{dk})$$

$$= \frac{g_\chi}{d} \sum_{0\le a<d} \overline{\chi}(a) \sum_{0<j<d} \frac{\zeta^{-aj}\xi^j}{1-\zeta^{-ad}\xi^d} = \frac{g_\chi}{d} \sum_{0\le a<d} \overline{\chi}(a) \frac{\zeta^{-aj}\xi^j}{1-\zeta^{-ad}\xi^d}\chi(j)\overline{\chi}(j)$$

$$= \frac{g_\chi}{d} \sum_{j,a} \overline{\chi}(aj) \frac{\zeta^{-aj}\xi^j}{1-\zeta^{-ad}\xi^d}\chi(j) = \frac{g_\chi}{d} \sum_{T} \overline{\chi}(T)\zeta^{-T} \sum_{j} \xi^j\chi(j)\frac{1}{1-\xi^d},$$

where $T = aj$ and

$$= \frac{g_\chi g_{\overline{\chi}}}{d} \frac{g_\chi}{1-\xi^d} = \frac{g_\chi}{1-\xi^d}.$$

However, on the left side,

$$= \lim_{N\to\infty} \sum_{0<j<dp^N} \chi(j) \frac{\xi^j}{1-\xi^{dp^N}} = \lim_{N\to\infty} \sum_{0<j<d} \chi(j) \frac{\xi^j}{1-\xi^{dp^N}} \sum_{k=0}^{p^N-1} \xi^{dk}$$

$$= \sum_{0<j<d} \chi(j)\xi^j \frac{1}{\xi^d-1} = \frac{g_\chi}{1-\xi^d}.$$

□

Now we can prove Theorem ((4.3.4) for the twisted case.
Note that if $f : X \to \mathbb{C}_p$ comes from pulling back an $f : \mathbb{Z}_p \to \mathbb{C}_p$ via the projection $X \to \mathbb{Z}_p$, we can replace X by $\mathbb{Z}_p$ in $\int_X f\, d\mu_\xi$, where μ_ξ on $\mathbb{Z}_p$ is given by (4.5) with $d = 1$.
Applying lemma (4.3.7) and the preceding remark to $f = (1/x)$. *char fn* of $X^\times$, we have

$$L_p(1,\chi,\xi) = \int_{X^\times} \frac{\chi(x)}{x}\, d\mu_\xi = \frac{g_\chi}{d} \sum_{0\le a<d} \overline{\chi}(a) \int_{\mathbb{Z}_p^\times} \frac{1}{x}\, d\mu_{\zeta^{-a}\xi}$$

$$= -\frac{g_\chi}{d} \sum_{0\le a<d} \overline{\chi}(a) \frac{1}{p} \log_p \frac{(1-\zeta^{-a}\xi)^p}{1-(\zeta^{-a}\xi)^p}$$

$$= -\frac{g_\chi}{d}(1-\frac{\chi(p)}{p}) \sum_{0\le a<d} \overline{\chi}(a) \log_p(1-\zeta^{-a}\xi) \tag{4.22}$$

Since $r > 1$ is any integer prime to pd, we may choose r so that $\chi(r) \neq 1$ and then use (4.18) with $s = 1$ to express $L_p(1,\chi)$ in terms of the $L_p(1,\chi,\xi)$ for $\xi \neq 1$. We obtain,

$$L_p(1,\chi) = \frac{1}{\chi(r)-1}\sum_{\xi^r=1} L_p(1,\chi,\xi)$$

$$= -\frac{g_\chi}{d}(1-\frac{\chi(p)}{p})\left[\frac{1}{\chi(r)-1}\sum_{0<a<d}\overline{\chi}(a)\sum_{\xi^r=1}\log_p(1-\zeta^{-a}\xi)\right].$$

The inner summation is equal to $\log_p(1-\zeta^{-ar}) - \log_p(1-\zeta^{-a})$ because first note that

$$\sum_{\xi^r=1}\log_p(1-\zeta^{-a}\xi) = \log_p(\prod_{\xi^r=1} 1-\zeta^{-a}\xi),$$

and if we factorize the equation $Z^r = (\zeta^{-a}\xi)^r = \zeta^{-ar}$ into its root we have,

$$Z^r - \zeta^{-ar} = \prod_{\xi^r=1}\frac{Z-\zeta^{-ar}}{Z-\zeta^{-a}}$$

which gives us the equality for $Z = 1$. Therefore, the term in the square bracket is seen to equal $\sum_{0<a<d}\overline{\chi}(a)\log_p(1-\zeta^{-a})$ as desired.

4.4 The interpolation properties

The interpolation formula is the formula which would relate L_p to our classical L-function over negative integers, and is in the Proposition (4.3.1),

Proposition 4.4.1.

$$L_p(1-n,\chi) = (1-\chi_n(p)p^{n-1})L(1-n,\chi_n) \quad \forall n \text{ positive}, \tag{4.23}$$

and $\chi_n = \chi\overline{\omega}^n$ *with same* χ *and* ω *stated in the beginning of the section (4.3).*

Proof. The proof of this equality is easy. Recall that we define

$$L_p(s,\chi) = \frac{1}{\langle r\rangle^{1-s}\chi(r)-1}\sum_{\xi,\,\xi^r=1} L_p(s,\chi,\xi),$$

and we showed that,

$$\sum_{\xi,\xi^r=1} L_p(1-n,\chi,\xi)$$

$$= (\langle r\rangle^n\chi_n(r)-1)(1-\chi_n(p)p^{n-1})L(1-n,\chi_n).$$

Then,

$$L_p(1-n,\chi) = \frac{1}{\langle r\rangle^n\chi(r)-1}\sum_{\xi,\xi^r=1} L_p(1-n,\chi,\xi) = (1-\chi_n(p)p^{n-1})L(1-n,\chi_n)$$

which is what we wanted to prove. □

Bibliography

[1] Koblitz, Neal. "A new proof of certain formulas for p-adic L-functions." (1979): 455-468.

[2] Iwasawa, Kenkichi. Lectures on p-adic L-functions. No. 74. Princeton University Press, 1972.

[3] Koblitz, Neal, and Neal Koblitz. P-adic numbers. Springer New York, 1984.

[4] Gouvãea, Fernando Quadros. P-adic numbers: An introduction. Springer-Verlag, 1993.

[5] Stein, Elias M., and Rami Shakarchi. Fourier analysis: an introduction. Vol. 1. Princeton University Press, 2011.

[6] Stein, Elias M., and Rami Shakarchi. Complex analysis. Vol. 2. Princeton University Press, 2010.

[7] Borevich, Zenon Ivanovich, and Igor Rostislavovich Shafarevich. Number theory. Academic press, 1986.

[8] Krasner, M. "Prolongement analytique uniforme et multiforme dans les corps valués complets, Colloque Int."

[9] Dwork, Bernard. "p-adic cycles." Publications Mathématiques de l'IHÉS 37 (1969): 27-115.

[10] Leopoldt, Heinrich W., and Tomio Kubota. "Eine p-adische Theorie der Zetawerte. Teil I: Einführung der p-adischen Dirichletschen L-Funktionen." Journal für die reine und angewandte Mathematik (Crelles Journal) 1964.214-215 (1964): 328-339.

[11] Leopoldt, Heinrich Wolfgang. "Eine p-adische Theorie der Zetawerte. II." (1975): 224-239.