2022

Interpolating the Riemann Zeta Function in the p-adics

Rebecca Mamlet

SCRIPPS

THE WOMEN'S COLLEGE

• CLAREMONT •

Interpolating the Riemann Zeta Function in the p-adics

Becca Mamlet

Christopher Towse, Advisor

Anie Chaderjian, Reader

Submitted to Scripps College in Partial Fulfillment of the Degree of Bachelor of Arts

March 11, 2022

Department of Mathematics

Abstract

In this thesis, we develop the Kubota-Leopoldt Riemann zeta function in the p-adic integers. We follow Neil Koblitz's interpolation of Riemann zeta, using Bernoulli measures and p-adic integrals. The underlying goal is to better understand p-adic expansions and computations. We finish by connecting the Riemann zeta function to L-functions and their p-adic interpolations.

Contents

Abstract **iii**

Acknowledgments **ix**

1 Overture **1**

2 Classical Functions **3**
- 2.1 The Riemann Zeta Function 3
- 2.2 Zeta and the Bernoulli Numbers 9

3 A p-adic Primer **15**
- 3.1 The Basics 15
- 3.2 Finding Expansions 19
- 3.3 Sorting the Numbers 21
- 3.4 A Sketch of the Landscape 23
- 3.5 Continuity 25
- 3.6 Conceptualizing p-adic Topology: A Study in Indigo 27

4 DIY p-adic Zeta **31**
- 4.1 A Smaller Step 32
- 4.2 Interlude 38
- 4.3 Measures 39
- 4.4 Building the Integral 44
- 4.5 The Mellin-Mazur Integral 47

5 Finale **53**
- 5.1 Dirichlet Characters 53
- 5.2 p-adic L-functions 55

Bibliography **57**

List of Figures

2.1 Contour C 5

4.1 $A \cup B = A + B - (A \cap B)$? 40

Acknowledgments

This absolutely would never have happened without my incredible advisor, Professor Towse. Thanks for guiding me through this material and answering all my questions. You're a brilliant mathematician and a fantastic teacher.

Thank you also to my second reader, Professor Chaderjian. I appreciate all your generous support and instruction on this project, and (more importantly) throughout my time at Scripps.

Thank you to Will Geller for helping me with measures! (Did I get them right?)

Thanks to all my friends and family for providing food, love, and moral support. For those of you who don't like math, here's a bunny:

```
( \ _ / )
(  ' x ' )
c( " )( " )
```

For those of you who like math but only the boring kind, here's an equation which doubles as a heart:

$$d = \frac{m}{v}$$

Special thanks to Sarah and Mariam and Dan for answering questions at ungodly hours of the night, and thank you to Gabi for holding my hand while I waded through readings. Love you all! Carthago delenda est.

Chapter 1

Overture

When Kurt Hensel formally introduced the p-adic numbers in 1897, he probably was not thinking about how silly the name sounded. The p-adics are not actually a type of obscure vegetable or a swear someone might use in *Oklahoma*. Instead, they are all about prime numbers, which is what the p stands for.

The p-adic numbers, written $\mathbb{Q}_p$, are an entirely different number field from the reals or the complex numbers. In place of $\mathbb{Z}$ are the p-adic integers, $\mathbb{Z}_p$. Instead of decimals, we have p-adic expansions. Lots of things look like real numbers. Nothing acts like it.

Our goal is, ostensibly, to interpolate a function in the p-adics. The underlying hope is to understand how computations work in $\mathbb{Q}_p$. We will go through examples and see the connections between real numbers, modular arithmetic, and p-adic numbers.

Often, numbers in the p-adics are written like real numbers: $4, 83, \frac{6725601}{22}$, etc. The true form of a p-adic number, though, is the p-adic expansion–a number represented in powers of p. Most p-adic math is done with these expansions. For example, in $\mathbb{Q}_7$,

$$\frac{6725601}{22} = 1 + (5 \cdot 7) + (6 \cdot 7^2) + (1 \cdot 7^3) + \dots.$$

Chapter 3 will explain how to find these expansions.

Integer shorthand will be extended to rational numbers for this thesis. When we say $p \nmid k$, we mean that p does not divide the numerator or the denominator of k in its simplified form. When we say that $k \equiv j \pmod{p}$, we mean that $k = j + mp$ where $m \in \mathbb{Z}$. This way, any fractional parts of k and j remain fractions.

We will do our best to supply all necessary context, but this thesis is intended to be accessible to someone with a background in undergraduate number theory and analysis. For Chapter 2, familiarity with complex integrals will also be assumed.

The next section will provide some background on the Riemann zeta function, focusing on complex analysis. The third section is a more in-depth look at the p-adics, and the fourth section interpolates the Riemann zeta function into the p-adics.

Interpolation means taking a function in one field and making it work in another. For instance we will take the Riemann zeta function, defined on the complex plane, and manipulate it until it works in the p-adic integers. Sometimes this means substituting in analogous operations, sometimes it means changing the inputs, and sometimes it means completely rewriting parts of the function. We reserve the right to take creative liberties.

Chapter 2

Classical Functions

This chapter acts as an overview of the Riemann zeta function. The zeta function has several important uses, but we are most interested in its relation to Bernoulli numbers. We will p-adically interpolate the function in Chapter 4. For now, it is helpful to establish some major properties.

Before beginning, some notation is required. The following section takes place in the complex plane, so for complex variable $z = x + iy$, $\text{Re}(z)$ will denote the real part of the variable, x, and $\text{Im}(z)$ will denote the imaginary coefficient, y.

2.1 The Riemann Zeta Function

Definition 2.1.1 (Riemann Zeta Function). *The Riemann zeta function is defined for $z \in \mathbb{C}$ as*

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}. \tag{2.1}$$

Alternatively,

$$\zeta(z) = \prod_{\textit{prime } p} \left(1 - \frac{1}{p^z}\right)^{-1}. \tag{2.2}$$

Riemann zeta converges when $\text{Re}(z) > 1$:

$$\left|\frac{1}{n^z}\right| \leq \left|\frac{1}{n^{\text{Re}(z)}}\right| \leq \frac{1}{n^{1+\delta}}$$

for some $\delta > 0$, and a well-established fact from calculus is that infinite series

$$\sum_{n=1}^{\infty} \frac{1}{n^p}$$

converge for $p > 1$. By the comparison test, Riemann zeta converges when $\mathrm{Re}(z) > 1$.

Additional functions will be introduced throughout this section, but they are just a means to an end. What we really want is the following identity for natural number k:

$$\zeta(1-k) = -\frac{B_k}{k} \tag{2.3}$$

where B_k is the kth Bernoulli number. When we finally p-adically interpolate the Riemann zeta function, this is the equation we will work with. It is much simpler than an infinite sum or product, and Bernoulli numbers are surprisingly easy to work with in the p-adics. The appearance of Bernoulli numbers is a bit startling, so we will use this section to illustrate how they got in there.

The zeta function is often analyzed in tandem with the Gamma function, defined for $z \in \mathbb{C}$ with $\mathrm{Im}(z) > 0$, as

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

The Gamma function is a way to generalize factorials, because

$$\Gamma(n+1) = n! \tag{2.4}$$

for any nonnegative integer n.

Conventional analysis also establishes

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}. \tag{2.5}$$

One integral representation of $\zeta(z)$ for $\mathrm{Re}(z) > 1$ is

$$\Gamma(z)\zeta(z) = \int_0^{\infty} \frac{x^{z-1} e^{-x}}{1-e^{-x}}\, dx. \tag{2.6}$$

For a proof, consult Apostol (1998: p.251).

Define another function:

$$I(z) = \frac{1}{2\pi i} \int_C \frac{s^{z-1} e^s}{1-e^s}\, ds. \tag{2.7}$$

It can be shown that I(z) is an entire function of z. Again, see proof in Apostol (1998: p.253).

The contour over which I is defined, contour C, is illustrated in Figure 2.1. The contour goes around the negative real axis, consisting of C_1 and C_3 which move counterclockwise around the axis, and circle C_2 centered about the origin.

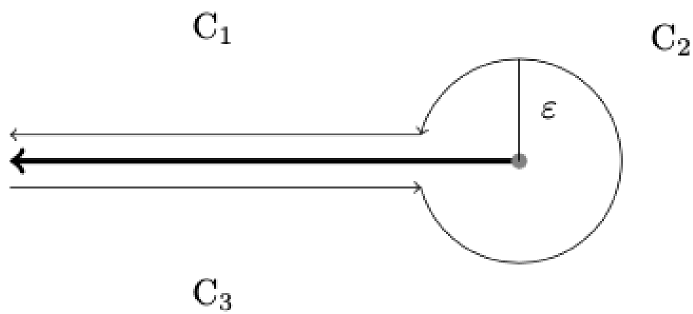

Figure 2.1 Contour C

To get to the Bernoulli numbers, we will need the following integral representation of Riemann zeta. Incidentally, this lemma also acts as an analytic continuation of $\zeta(z)$–which we will use–but it is not our primary motivation.

Lemma 2.1.1. *When Re*$(z) > 1$,

$$\zeta(z) = \Gamma(1-z)I(z). \tag{2.8}$$

Proof. The aim of I is to integrate over the nonnegative real axis, so we will eventually let the radius of C_2 go to 0 as the lines (C_1 and C_3) go to negative infinity. There are two issues. One, I has a pole at $s = 0$, and two, z^{s-1} is a multivalued function, which means simplifying too early could result in the wrong answer.

Isolate the multivalued part of the integral by letting

$$g(s) = \frac{e^s}{1-e^s}.$$

For most of the following calculations, $g(s)$ will not be important, so we can safely set it aside and write

$$2\pi i I(z) = \int_C s^{z-1} g(s)\, ds.$$

Parameterize C_1 as $s = re^{-\pi i}$ and C_3 as $s = re^{\pi i}$. As previously stated, r will eventually go to infinity, but by convention, instead we let r go from ε to ρ and take the limit as ρ goes to infinity.

Parameterize C_2 as $s = \varepsilon e^{i\theta}$ where $-\pi \leq \theta \leq \pi$. Eventually, we will take the limit as ε goes to 0, but not yet. In fact, note that

$$2\pi i I(z) = \lim_{\substack{\rho\to\infty \\ \varepsilon\to 0}} \left(\int_{C_1} + \int_{C_2} + \int_{C_3} \right).$$

By evaluating I with these limits, we will eventually reach Equation 2.8.

Start with C_1. Recall that $e^{-\pi i} = e^{\pi i} = -1$ by Euler's formula. In every case except s^{z-1}, simplifying $re^{-\pi i}$ to $-r$ is fine. As mentioned earlier, however, s^{z-1} will give a different answer if we simplify before plugging in. To change from s to $re^{-\pi i}$, we will need to change measures as well:

$$\begin{aligned} s &= -r \\ ds &= -dr. \end{aligned}$$

Thus, letting $s = -r$ for most of the integral,

$$\begin{aligned} -\int_{\rho}^{\varepsilon} (re^{-\pi i})^{z-1} g(-r)\, dr &= -\int_{\rho}^{\varepsilon} r^{z-1} e^{-\pi i z} e^{\pi i} g(-r)\, dr \\ &= \int_{\rho}^{\varepsilon} r^{z-1} e^{-\pi i z} g(-r)\, dr \\ &= \int_{\varepsilon}^{\rho} -r^{z-1} e^{-\pi i z} g(-r)\, dr. \end{aligned}$$

We switched bounds on the integral so that C_1 will have the same bounds as C_3 when we add them. The process for C_3 is nearly identical to that of C_1:

$$-\int_{\varepsilon}^{\rho} (re^{\pi i})^{z-1} g(-r)\, dr = \int_{\varepsilon}^{\rho} r^{z-1} e^{\pi i z} g(-r)\, dr.$$

Combining the two, we get

$$\begin{aligned} &\int_{\varepsilon}^{\rho} -r^{z-1} e^{-\pi i z} g(-r)\, dr + \int_{\varepsilon}^{\rho} r^{z-1} e^{\pi i z} g(-r)\, dr \\ &\qquad = \int_{\varepsilon}^{\rho} r^{z-1} g(-r)[-e^{-\pi i z} + e^{\pi i z}]\, dr \\ &\qquad = \int_{\varepsilon}^{\rho} r^{z-1} g(-r)[2i \sin(\pi z)]\, dr, \end{aligned}$$

by Euler's formula.

As a reminder, what we have so far is

$$2\pi i I(z) = \lim_{\substack{\rho\to\infty \\ \varepsilon\to 0}} 2i\sin(\pi z)\int_{\varepsilon}^{\rho} r^{z-1}g(-r)\,dr + \lim_{\substack{\rho\to\infty \\ \varepsilon\to 0}} \int_{C_2} (\text{something}).$$

Now take the limit of the first integral:

$$2i\sin(\pi z)\lim_{\substack{\rho\to\infty \\ \varepsilon\to 0}} \int_{\varepsilon}^{\rho} \frac{r^{z-1}e^{-r}}{1-e^{-r}}\,dr.$$

By Equation 2.6, the above limit is equivalent to

$$2i\sin(\pi z)\Gamma(z)\zeta(z),$$

which is quite similar to what we eventually want.

Before finishing up, we still need to take care of C_2, which is paramaterized by $s = \varepsilon e^{i\theta}$ with $-\pi \le \theta \le \pi$. For change of variables,

$$\begin{aligned} s &= \varepsilon e^{i\theta} \\ ds &= i\varepsilon e^{i\theta}\,d\theta. \end{aligned}$$

The integral is

$$\begin{aligned} &i\int_{-\pi}^{\pi} \varepsilon^{z-1}e^{(z-1)i\theta}g(\varepsilon e^{i\theta})\varepsilon e^{i\theta}\,d\theta \\ &= i\varepsilon^{z}\int_{-\pi}^{\pi} e^{iz\theta}g(\varepsilon e^{i\theta})\,d\theta. \end{aligned}$$

This integral will eventually go to 0, but to prove it, we will need a result from complex analysis.

Lemma 2.1.2. *If $f(z)$ is continuous on some complex contour Γ, and if $|f(z)| \le M$ for all $z \in \Gamma$, then*

$$\left|\int_{\Gamma} f(z)\,dz\right| \le M\cdot \text{ the arc length of } \Gamma.$$

Break up

$$|i\varepsilon^{z}e^{iz\theta}g(\varepsilon e^{i\theta})| = |i\varepsilon^{z}|\cdot|e^{iz\theta}|\cdot|g(\varepsilon e^{i\theta})|.$$

Let $z = x + iy$ for some real x and y. Then in a well-known result,

$$\begin{aligned} |i\varepsilon^{x+iy}| &= |i| \cdot |\varepsilon^x| \cdot |\cos(y) + i\sin(y)| \\ &= 1 \cdot |\varepsilon^x| \cdot \sqrt{\cos^2(y) + \sin^2(y)} \\ &= \varepsilon^x. \end{aligned}$$

Consider $|e^{iz\theta}|$. By the same argument as above, $|e^{iz\theta}| = e^{-y\theta}$. In the first case, if $y > 0$, this function is greatest at $\theta = \pi$. In the second case, if $y < 0$, then this function is greatest at $\theta = -\pi$, but the output is equal to that of the first case's maximum. If $y = 0$, then the function is 1 and θ does not matter. In every case,

$$e^{-y\theta} \leq e^{|y|\pi}.$$

The last term is $|g(\varepsilon e^{iz\theta})|$. Since $g(s)$ is analytic apart from a simple pole at $s = 0$, $zg(z)$ is analytic over all of C_2. Analytic over a bounded domain implies that $zg(z)$ is also bounded by a constant, say A. Thus

$$|z||g(z)| \leq A,$$

implying

$$|g(z)| \leq \frac{A}{|z|}.$$

As proven by an argument similar to that of $|i\varepsilon^z|$, $|\varepsilon e^{i\theta}| = \varepsilon$. Therefore, $|g(\varepsilon e^{i\theta})| \leq \frac{A}{\varepsilon}$.

Lastly, the arc length of C_2 is $2\pi\varepsilon$. Putting everything together, we find

$$\left|\int_{C_2} i\varepsilon^z e^{iz\theta} g(\varepsilon e^{i\theta})\, d\theta\right| \leq 2\pi\varepsilon \cdot i\varepsilon^x \cdot \frac{A}{\varepsilon} \cdot e^{|y|\pi} = 2A\pi i e^{|y|\pi}\varepsilon^x.$$

Finally, take the limit as $\varepsilon \to 0$. We said $\mathrm{Re}(z) > 1$, meaning $x > 1$. Therefore,

$$\lim_{\varepsilon \to 0} 2A\pi i e^{|y|\pi}\varepsilon^x = 0.$$

Finally, go back to $I(z)$:

$$2\pi i I(z) = 2i\sin(\pi z)\Gamma(z)\zeta(z).$$

Then

$$I(z) = \frac{\sin(\pi z)}{\pi}\Gamma(z)\zeta(z).$$

By Equation 2.5,

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

and thus,

$$\zeta(z) = \Gamma(1-z)I(z).$$

□

Note that $\Gamma(1-z)$ and $I(z)$ are fully defined and analytic for $\mathrm{Re}(z) < 1$, so with this equation, we can define $\zeta(z)$ for $\mathrm{Re}(z) < 1$. This is how analytic continuation works: we rewrite a function in terms of other functions with larger domains, and use the new equation to extend our first function.

2.2 Zeta and the Bernoulli Numbers

At this point, we can introduce Bernoulli numbers. Bernoulli numbers were first discovered by Seki Takakazu in Japan, but due to Eurocentrism, they are conventionally named after Western mathematician Jacob Bernoulli (O'Connor and Robertson, 1997: p. 32).

There are several ways to define Bernoulli numbers. They show up as coefficients in equations which sum up the first n numbers, raised individually to some power m. Another way to define them is with Bernoulli polynomials, which are coefficients themselves. In short,

$$\frac{ze^{xz}}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n, \tag{2.9}$$

where $B_n(x)$ is defined as the nth Bernoulli polynomial. For this sum to converge, $|z| < 2\pi$.

Behold, the first five Bernoulli polynomials:

$$\begin{aligned}
B_0(x) &= 1\\
B_1(x) &= x - \frac{1}{2}\\
B_2(x) &= x^2 - x + \frac{1}{6}\\
B_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{2}x\\
B_4(x) &= x^4 - 2x^3 + x^2 - \frac{1}{30}\\
B_5(x) &= x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x
\end{aligned}$$

The Bernoulli numbers are $B_n(0)$, but we just write B_n.
The first five Bernoulli numbers are:

$$\begin{aligned}
B_0 &= 1\\
B_1 &= -\frac{1}{2}\\
B_2 &= \frac{1}{6}\\
B_3 &= 0\\
B_4 &= -\frac{1}{30}\\
B_5 &= 0
\end{aligned}$$

It turns out that for every n odd and greater than 1, $B_n = 0$.
It can also be shown that

$$B_n(0) = B_n(1) \text{ for } n \geq 2.$$

See Apostol (1998: p.265) for proofs.

Mathematicians have no real explanation for why Bernoulli numbers pop up in so many contexts, so there is little overall intuition for their appearance in the Riemann zeta function. Earlier integral representations of the Riemann zeta function do, however, bear a passing resemblance to the function in Equation 2.9, and thus, perhaps it is not quite as surprising that we find Bernoulli polynomials in the next lemma.

Lemma 2.2.1. *For every positive integer n,*

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}. \tag{2.10}$$

Proof. Lemma 2.1.1 says

$$\zeta(z) = \Gamma(1-z)I(z),$$

and via analytic continuation, this equation will hold for all values of z.

Let n be a nonnegative integer. Then by Lemma 2.1.1

$$\zeta(-n) = \Gamma(1-(-n))I(-n) = \Gamma(n+1)I(-n).$$

For $n \in \mathbb{Z}$, we can directly compute the right hand side of the equation to get the Bernoulli polynomials.

First consider $I(-n)$. In the proof of Lemma 2.1.1 we found the integral along C_1 to be

$$\int_{\varepsilon}^{\rho} -r^{z-1}e^{-\pi i z}g(-r)\,dr.$$

Additionally, the integral along C_3 was

$$\int_{\varepsilon}^{\rho} r^{z-1}e^{\pi i z}g(-r)\,dr.$$

If $z=-n$ is an odd integer, then $e^{\pi i(-n)} = -1 = e^{-\pi i(-n)}$. If $z=-n$ is even, then $e^{\pi i(-n)} = 1 = e^{-\pi i(-n)}$.

Either way, $\int_{C_1} = -\int_{C_3}$ when n is an integer. For example, if $n=2$, then the integral along C_1 is

$$\int_{\varepsilon}^{\rho} -rg(-r)\,dr$$

while the integral along C_3 is

$$\int_{\varepsilon}^{\rho} rg(-r)\,dr.$$

Ultimately, adding $\int_{C_1} + \int_{C_3}$ results in 0 at integer values of n; C_1 and C_3 will cancel each other out. Accordingly, we only need to solve I$(-n)$ over C_2, which is a simple, closed, positively-oriented curve. By Cauchy's Residue Theorem,

$$I(-n) = \frac{1}{2\pi i}\cdot 2\pi i \cdot \operatorname*{Res}_{s=0}\left(\frac{s^{-n-1}e^{s}}{1-e^{s}}\right).$$

To find the residue, we manipulate the integrand of $I(-n)$ into Equation 2.9:

$$\begin{aligned}\frac{s^{-n-1}e^s}{1-e^s} &= -s^{-n-2}\frac{se^s}{e^s-1} \\ &= -s^{-n-2}\sum_{m=0}^{\infty}\frac{B_m(1)}{m!}s^m \\ &= -\sum_{m=0}^{\infty}\frac{B_m(1)}{m!}s^{m-n-2}.\end{aligned}$$

Momentarily setting aside the negative sign, the residue of an integral is the coefficient on s^{-1} in the Laurent expansion of the integrand. The Laurent series, in this case, is the sum given. Since $m-n-2=-1$ when $m=n+1$, the residue will be

$$\frac{B_{n+1}(1)}{(n+1)!}.$$

Thus, $\mathrm{I}(-n) = -\frac{B_{n+1}(1)}{(n+1)!}$. For n, a positive integer, $\Gamma(n+1)=n!$. Therefore,

$$\begin{aligned}\zeta(-n) &= -n!\frac{B_{n+1}(1)}{(n+1)!} \\ &= -\frac{B_{n+1}(1)}{n+1}.\end{aligned}$$

As mentioned earlier, $B_n(1)=B_n(0)$ for $n \geq 2$, and hence,

$$B_{n+1}(1) = B_{n+1}(0) \text{ for } n > 0.$$

Therefore,

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}.$$

□

We are almost at our final version of the Riemann zeta function. Only a few quick manipulations remain.

Lemma 2.2.2. *For positive integer k,*

$$\zeta(1-2k) = -\frac{B_{2k}}{2k}. \tag{2.11}$$

Proof. By Lemma 2.2.1

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}.$$

Let $-n = 1 - 2k$, so $n = 2k - 1$. Note that $n > 0$ if k is a positive integer. Hence,

$$\zeta(1-2k) = -\frac{B_{2k}}{2k}.$$

□

At this point, we need the following identity:

Lemma 2.2.3. *For Re*$(z) > 1$,

$$\zeta(1-z) = 2\cos\left(\frac{\pi z}{2}\right)\Gamma(z)(2\pi)^{-z}\zeta(z). \tag{2.12}$$

Proofs can be found in Apostol (1998: p.259) or Koblitz (1984: p.22).

Lemma 2.2.3 holds for any positive integer k, but by slightly limiting the input, the output can be further generalized.

Theorem 2.2.1. *For integer* $k > 1$,

$$\zeta(1-k) = -\frac{B_k}{k}. \tag{2.13}$$

Proof. If k is even, then we can represent it as $k = 2m$ for $m \in \mathbb{Z}$. Therefore, by Lemma 2.2.1 , $\zeta(1-k) = -\frac{B_k}{k}$.

If k is odd but greater than 1, then

$$\cos\left(\frac{\pi k}{2}\right) = 0.$$

Additionally, $B_k = 0$ when k is an odd integer greater than 0. Hence, by Lemma 2.2.3, $\zeta(1-k) = 0 = -\frac{B_k}{k}$. □

A great deal of complex analysis went into proving such a simple equation. In deriving Theorem 2.2.1 we saw links between the Gamma function, multiple zeta functions, and Bernoulli polynomials. Although we have yet to find an overarching explanation to the appearance of Bernoulli numbers, on a mathematical level, they arose naturally from various integral representations. The p-adic analogue to the Riemann zeta function builds on Theorem 2.2.1 as, (un)surprisingly, the Bernoulli numbers also pop up in the p-adics.

Chapter 3

A p-adic Primer

This chapter provides an introduction to the p-adic field, assuming prior knowledge of basic number theory and analysis.

3.1 The Basics

The p-adic numbers are a field built around some specific prime p. Accordingly, when working in the p-adics, we should think in terms of p.

To build the norm, first start with a smaller measuring tool.

Definition 3.1.1 (p-adic Valuation)**.** *Let n be a nonzero integer, and let $v_p(n)$ be the unique nonnegative integer satisfying*

$$n = p^{v_p(n)} n', \qquad p \nmid n', \qquad n' \in \mathbb{Z}.$$

Then $v_p(n)$ is the p-adic valuation of n.

In other words, the p-adic valuation is the largest power of p which divides n. For example,

$$v_5(10) = 1, \text{ since } 10 = 5^1(2)$$
$$v_7(10) = 0, \text{ since } 10 = 7^0(10).$$

If we are working in $\mathbb{Q}^\times$, the valuation is defined to be

$$x = \frac{a}{b}, \; v_p(x) = v_p(a) - v_p(b).$$

Here are some examples:

$$v_3\left(\frac{2}{9}\right) = 0 - 2 = -2,$$
$$v_3\left(\frac{6}{27}\right) = 1 - 3 = -2.$$

It appears our valuation is well-defined. By convention, $v_p(0) = \infty$.

Lemma 3.1.1. *For all x and $y \in \mathbb{Q}$,*

(*a*) $v_p(xy) = v_p(x) + v_p(y)$

(*b*) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$

Proof. Let $x = p^m j$ and let $y = p^n k$ where $j, k \in \mathbb{Q}$ and p does not divide the numerator or denominator of j or k. For part (a), if $j \neq 0$ and $k \neq 0$, we have

$$xy = (p^m j)(p^n k) = p^{m+n} jk.$$

Therefore, $v_p(xy) = v_p(x) + v_p(y)$.
If $j = 0$, then $x = 0$, $m = \infty$, and $\infty + n$ is still ∞. The same goes for $k = 0$.

For part (b),

$$x + y = p^m j + p^n k = p^n(p^{m-n} j + k).$$

If $j = 0$, then $x = 0$ and $v_p(0) = \infty$. Then

$$v_p(y) = m \geq \min\{m, \infty\}.$$

The same goes for if $k = 0$.

Let $j \neq 0$ and $k \neq 0$. Without loss of generality, say $m \geq n$. If $m \neq n$, then $(p^{m-n} j + k) \equiv k \pmod{p}$.

Because $k \neq 0$, we know that $p \nmid (p^{m-n} j + k)$. Hence, $v_p(x + y) = n$.

If $m = n$, then the p-term vanishes and we could potentially get another p out of $j + k$, meaning our exponent on p might be even greater.

In any case,
$$v_p(x + y) \geq n = \min\{v_p(x), v_p(y)\}.$$

□

Now that we have a way to measure the amount of p in some number, we can start thinking about size and distance.

Definition 3.1.2 (Norm)**.** *Norm $|\cdot|$ on arbitrary field $\mathbb{K}$ with some elements x, y is a function that maps $\mathbb{K}$ to the nonnegative reals with the following properties*:

1. $|xy| = |x||y|$
2. $|x + y| \leq |x| + |y|$
3. $|x| = 0$ *if and only if* $x = 0$.

Some norms have another feature, sometimes called the "stronger triangle inequality" because it implies the norm triangle inequality, and sometimes called the non-Archimedean property.

Definition 3.1.3 (Non-Archimedean Property)**.** *A norm is non-Archimedean if, for any x, y elements in the field,*

$$|x + y| \leq \max\{|x|, |y|\}.$$

The p-adic valuation is easily manipulated into a non-Archimedean norm. If v_p stays an exponent, property (a) from Lemma 3.1.1 becomes the first property of the norm definition. We still want to measure in terms of prime p, so we keep p as the base. The first attempt looks like

$$|x|_p = p^{v_p(x)}.$$

Comparing part (b) of Lemma 3.1.1 to the triangle inequality (part 2 of the norm definition), on the other hand, does not bring the same success. If the exponent gains a negative sign though, part (b) flips to the correct inequality.

There is no way to raise p to a power and achieve exactly 0, so we just set

$$|0|_p = 0$$

to fulfill our last property.

Definition 3.1.4 (p-adic Norm)**.** *Let $x \in \mathbb{Q}$. Then*

$$|x|_p = \begin{cases} p^{-v_p(x)}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

is the p-adic norm.

We usually measure size in relation to 0 so it might not be obvious at first why the p-adic norm is so weird. But when we measure distance from 0, we are subtracting and adding, which works for any number. In the p-adics, we are factoring, and that means any number which does not have a multiple of p in the numerator or denominator is in a nebulous this-seems-wrong kind of space.

A closely related concept is a metric, or a measure of distance.

Definition 3.1.5 (Metric)**.** *A metric or distance function on arbitrary field $\mathbb{K}$ maps $\mathbb{K}$ to the nonnegative real numbers. For elements x and y and z in $\mathbb{K}$, the metric d has the following properties*:

1. $d(a, b) > 0$ *and* $d(a, a) = 0$
2. $d(a, b) = d(b, a)$
3. $d(a, b) \leq d(a, c) + d(c, b)$.

Lemma 3.1.2. *The p-adic norm $d(a, b) = |a - b|_p$ for p-adic numbers a and b is also a metric.*

Proof. The proof of property 1 is straightforward. For distinct a, b,

$$|a - b|_p = p^{-v_p(a-b)}.$$

The only way to get 0 out of the norm is if $a - b = 0$, meaning $a = b$, so the only instance of zero is $d(a, a) = 0$.

For part 2, observe

$$|a - b|_p = |(-1)(b - a)|_p.$$

By norm properties, the right hand side becomes

$$|-1|_p \cdot |b - a|_p = |b - a|_p.$$

Thus, $|a - b|_p = |b - a|_p$.

The metric triangle inequality, helpfully, stems from the norm triangle inequality:

$$\begin{aligned} |a - b|_p &= |a - c + (-b + c)|_p \\ &\leq |a - c|_p + |c - b|_p. \end{aligned}$$

Hence, $|a - b|_p$ is a metric function. ∎

3.2 Finding Expansions

By convention, we write numbers in base 10. The p-adic expansion of a number is, essentially, writing in base p.

Definition 3.2.1 (p-adic Expansion)**.** *The p-adic expansion of a is*

$$\sum_i a_i p^i = a_{n_0} p^{n_0} + a_{n_1} p^{n_1} + a_{n_2} p^{n_2} + \dots$$

where $a_{n_i} \in \mathbb{Z}$ and $0 \le a_{n_i} \le p - 1$.

In general, we use a_0 to denote the “constant" term, i.e. the coefficient on p^0. If $a \in \mathbb{Z}$, then $a \equiv a_o \pmod{p}$.

The complicated subscripts are necessary in case a has negative powers of p in its expansion. Some expansions could go on to the right forever, but every expansion is “finite-tailed" on one end. These expansions cannot go on forever to the left; there is always a starting point. We begin by finding expansions for positive integers, and progress by level of difficulty: negative integers, fractions, and finally, irrational numbers.

For integer a, things are simple. The expansion of a positive integer a follows the rule

$$a \equiv a_0 + \cdots + a_k p^k \pmod{p^{k+1}}.$$

For instance, the 7-adic expansion of 10 is

$$10 = 3 + 1 \cdot 7.$$

Think of negative integers as additive inverses. Then the p-adic expansion for $-a$ is the number which results in the 0 expansion.

Because $1 + (-1) = 0$, the 5-adic expansion of -1 is

$$-1 = 4 + (4 \cdot 5) + (4 \cdot 5^2) + \dots.$$

This way,

$$\begin{aligned} 1 + (-1) &= 1 + (0 \cdot 5) + (0 \cdot 5^2) + \dots \\ &\quad + 4 + (4 \cdot 5) + (4 \cdot 5^2) + \dots \\ &= (1 \cdot 5) + (4 \cdot 5) + (4 \cdot 5^2) + \dots \\ &= 0 + (5 \cdot 5) + (4 \cdot 5^2) + \dots \\ &= 0 + (0 \cdot 5) + (0 \cdot 5^2) + \dots. \end{aligned}$$

The p-adic expansion of a fraction is found through long division. In the 7-adics, $\frac{2}{9}$ is computed by first writing 2 and 9 in base 7:

$$\begin{aligned} 2 &= 2 \\ 9 &= 2 + (1 \cdot 7) \end{aligned}$$

and dividing.

$$\begin{array}{r|llllll}
 & 1 + & (3 \cdot 7)+ & (5 \cdot 7^2)+ & (0 \cdot 7^3)+ & (3 \cdot 7^4)+ & \cdots \\ \cline{2-7}
2 + (1 \cdot 7) & 2 + & (0 \cdot 7)+ & (0 \cdot 7^2)+ & (0 \cdot 7^3)+ & (0 \cdot 7^4)+ & \cdots \\
 & 2 + & (1 \cdot 7) & & & & \\ \cline{2-7}
 & & (-1 \cdot 7)+ & (7 \cdot 7)+ & (-1 \cdot 7^2)+ & (7 \cdot 7^2)+ & \cdots \\ \cline{2-7}
 & & (6 \cdot 7)+ & (6 \cdot 7^2)+ & (6 \cdot 7^3)+ & (6 \cdot 7^4)+ & \cdots \\
 & & (6 \cdot 7)+ & (3 \cdot 7^2) & & & \\ \cline{2-7}
 & & & (3 \cdot 7^2)+ & (6 \cdot 7^3)+ & (6 \cdot 7^4)+ & \cdots \\
 & & & (3 \cdot 7^2)+ & (6 \cdot 7^3) & & \\ \cline{4-7}
 & & & & & (6 \cdot 7^4)+ & \cdots \\
 & & & & & & \ddots
\end{array}$$

We could go on forever, but the first part of the expansion is

$$\frac{2}{9} = 1 + (3 \cdot 7) + (5 \cdot 7^2) + (0 \cdot 7^3) + (3 \cdot 7^4) + \dots .$$

When we subtract in the p-adics, we borrow from the right side, not the left. Even though every coefficient to the right in the first line is a 0, we tell ourselves that eventually, somewhere down the line, we will hit a nonzero which we can borrow from. The higher and higher powers of 7 are practically nothing anyway, so eventually, it is as though we are subtracting an infinitesimally small amount. We just do it and hope no one catches us.

Arithmetic like above reveals similarities between the p-adics and mod p^n. To divide 2 by $2 + 1 \cdot 7$, we start by finding some number to multiply 2 and get back 2. Obviously, $2 \cdot 1 = 2$, so, without much excitement, we label the first number in the answer 1. Skip ahead several lines, though, and we have $3 \cdot 7^2 + \dots$. How can we multiply something by 2 to get 3? Go into mod

7. Then

$$\begin{aligned} 2x &\equiv 3 \pmod{7} \\ 2(5) &\equiv 3 \pmod{7} \\ 2(5) &= 3 + 1 \cdot 7. \end{aligned}$$

Of course, we actually multiply by $5 \cdot 7^2$ to match powers of 7, so the $1 \cdot 7$ is really a $1 \cdot 7^3$ which we carry over to the other 7^3 term. Much of p-adic arithmetic is like this: go into mod p, go out of mod p, then carry the p-term.

If, say, we wanted to find the expansion of n^a to the p^n-place for integers n and a, we could calculate the entire thing mod p^{n+1} and rewrite everything in base p. Reducing mod p^{n+1} is like throwing away all terms with powers of p higher than n. This is exactly what we want in an abbreviated p-adic expansion. In Chapters 4 and 5.2, further examples will demonstrate this even deeper connection to mod.

The construction of irrational numbers in the p-adics is exactly like the construction of irrationals in the reals. We define them to be the limits of p-adic Cauchy sequences, which means the p-adics are complete. Much like standard irrational numbers, p-adic irrationals are those numbers with infinite and non-repeating p-adic expansions.

With every type of real number accounted for, the formal field of p-adics can now be defined.

Definition 3.2.2 (p-adic Field)**.** *The field of p-adic numbers, denoted $\mathbb{Q}_p$, is the set of p-adic numbers under addition and multiplication.*

3.3 Sorting the Numbers

The p-adic numbers are split into three general categories. Let $x \in \mathbb{Q}_p$, and $a \in \mathbb{N}$, and $p \nmid x'$. There are several types of numbers in a p-adic space:

1. $|x|_p > 1$ meaning $x = p^{-a}(x')$.
2. $|x|_p = 1$ meaning $x = p^0(x')$
3. $|x|_p < 1$, meaning $x = p^a(x')$ (or $x = 0$)

The first type of number is a (simplified) fraction with a denominator containing p. Additionally, any infinite Cauchy sequence made with numbers in this category leads to an irrational number also in this category. The number has a factor of p to a negative power, so the absolute value gives a positive power of p. For instance, $\frac{1}{11} = 11^{-1}$, and thus

$$\left|\frac{1}{11}\right|_{11} = 11.$$

These fractions are huge in the p-adic space because everyone else is stuck at or below a size 1.

There exists better p-adic notation than simply saying a "group of numbers." For $n \in \mathbb{N} \cup \{0\}$, mathematicians often study p-adic sets denoted $p^n\mathbb{Z}_p$:

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq p^{-a}\}.$$

These sets are called balls, and they will be discussed further in the next section. The case $n = 0$ is of particular interest as it encapsulates type 2 and type 3 of the numbers listed above.

Definition 3.3.1 (p-adic Integers). *The p-adic integers form the ring*

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

The norm of any p-adic integer becomes a fraction between 0 and 1 (or 1 itself). For example, $|49|_7 = \frac{1}{7^2}$ and $|\frac{39}{2}|_{13} = \frac{1}{13}$.

On the other hand, every number without any factors of p has a valuation of 0, so their absolute values are all equal to 1. These are the only numbers with multiplicative inverses in the p-adic integers.

Definition 3.3.2 (p-adic Units). *The p-adic units are*

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

Essentially, the p-adic units are every number without p in the numerator or denominator (when simplified).

Take a moment to consider p-adic expansions within the p-adic norm. Let $a \in \mathbb{Z}_p$ and say $|a|_p = p^{-2}$. That means that the lowest power of p in a is p^2:

$$|a|_p = |a_2p^2 + \ldots|_p.$$

In other words, any coefficients like a_0 or a_1 must be 0:

$$a = 0 + (0 \cdot p) + (a_2 \cdot p^2) + \ldots.$$

Alternatively, if $a = a_{-1}p^{-1} + a_0 + \ldots$, then

$$|a_{-1}p^{-1} + a_0 + \ldots|_p = |p^{-1}(a_{-1} + a_0p + \ldots)|_p = p.$$

That is to say, any number with a negative power of p in its expansion cannot be a p-adic integer.

Remark. *If $|a|_p = p^n$, then the p-adic expansion of a begins at the p^{-n} place.*

We move on to a bit of $\mathbb{Z}_p$ analysis. Set X is *dense* in set Y if every point of Y is a limit point of X, or if there exists a sequence of terms in X converging to a point in Y for every point in Y.

Proposition 3.3.1. *The nonnegative integers are dense in $\mathbb{Z}_p$.*

Proof. The p-adic expansion of every term in $\mathbb{Z}_p$ is a series of nonnegative integers. The sequence of partial sums,

$$\begin{aligned} &a_0 \\ &a_0 + (a_1 \cdot p) \\ &a_0 + (a_1 \cdot p) + (a_2 \cdot p^2) \\ &\ldots \end{aligned}$$

is a sequence made of nonnegative integers, all converging to a p-adic integer. □

Lastly, we briefly touch on convergence. As a result of the non-Archimedean inequality and $\mathbb{Q}_p$'s completeness, series convergence in $\mathbb{Q}_p$ is a straightforward affair.

Proposition 3.3.2. *An infinite series converges in $\mathbb{Q}_p$ if and only if its terms go to 0.*

For a proof, see Gouvêa (1997: p.89).

3.4 A Sketch of the Landscape

In topology, space is broken up into neighborhoods or open balls.

Definition 3.4.1 (Open Ball)**.** *Let $a \in \mathbb{Q}_p$, and $r > 0$. The open ball of radius r and center a is the set*

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

In the p-adics, every open set is also closed, and every closed set is also open, in $\mathbb{Q}_p$. As a result, we do not worry too much about whether a p-adic set needs to be open or closed. Eventually, we will integrate over certain p-adic balls, so Section 4.4 relies heavily on the facts we are about to establish.

Lemma 3.4.1. *Given any two balls in $\mathbb{Q}_p$, either they are completely distinct sets, or one ball is fully contained within the other.*

A proof of the above can be found in Gouvêa (1997: p.36).

Now consider the elements of the ball

$$B(a, p^{-N}) = \left\{ x \in \mathbb{Z}_p : |x - a|_p \leq \frac{1}{p^N} \right\}.$$

Let

$$x = x_0 + x_1 p + \cdots + x_N p^N + \ldots$$

and let

$$a = a_0 + a_1 p + \cdots + a_N p^N + \ldots.$$

Then

$$|x - a|_p = |(x_0 - a_0) + p(x_1 - a_1) + \cdots + p^N(x_N - a_N) + \ldots|_p \leq \frac{1}{p^N}$$

if and only if every term before p^N is zero. In other words, $x_i = a_i$ for $i < n$.

Write

$$x = a_0 + a_1 p + \cdots + a_{N-1} p^{N-1} + x_N p^N + \ldots.$$

Reduce mod p^N to get

$$x \equiv a_0 + a_1 p + \cdots + a_{N-1} p^{N-1} \equiv a.$$

Accordingly, $x \equiv a \pmod{p^N}$.

Another way to write $B(a, p^{-N})$, then, is by equivalence class:

$$B(a, p^{-N}) = \{x \in \mathbb{Z}_p : x \equiv a \pmod{p^N}\}.$$

Sometimes, we write $B(a, p^{-N})$ as $a + (p^N)$, a ball centered at a with radius $\frac{1}{p^N}$. The notation will be discussed more in Section 4.4.

Lemma 3.4.2. *Every ball of the form $a + (p^N)$ can be decomposed into a finite, disjoint union of balls $\hat{a} + (p^M)$ where M is a fixed integer greater than N, and $\hat{a} \equiv a \pmod{p^N}$.*

Formally,

$$a + (p^N) = \bigsqcup_{0 \leq \hat{a} \leq p^M - 1} \hat{a} + (p^M).$$

Proof. Fix an $M \in \mathbb{Z}$ such that $M > N$.

First, we prove that the $\hat{a}$ balls are disjoint. If we take the centers of our balls to be only the representatives of $\mathbb{Z}/p^M\mathbb{Z}$, meaning $\{0, 1, \ldots, p^M - 1\}$, the balls will be disjoint. This is because every element in any $\hat{a} + (p^M)$ will be equivalent to $\hat{a}$ mod p^M, and no number b can be equivalent to two distinct representatives mod p^M. Accordingly, let each $\hat{a} \in \{0, 1, \ldots, p^M - 1\}$ with no repetition. Then for distinct $\hat{a}$'s, the balls $B(\hat{a}, p^{-M})$ are disjoint.

Next, we establish that the balls will be fully contained inside $a + (p^N)$. As previously discussed, $a + (p^N) = \{x \in \mathbb{Z}_p : x \equiv a \pmod{p^N}\}$. Therefore, if $a \equiv \hat{a} \pmod{p^N}$, then $\hat{a} \in a + (p^N)$. We disregard all $\hat{a}$'s which are not already in $a + (p^N)$; we keep only those for which $\hat{a} \equiv a \pmod{p^N}$. Because $B(\hat{a}, p^{-M})$ is a smaller ball, and its center is inside $B(a, p^{-N})$, they must intersect. By Lemma 3.4.1, two balls are either disjoint, or one is contained inside the other. Thus, $\hat{a} + (p^M) \subset a + (p^N)$.

Suppose there is some point c which is not in any included $\hat{a} + (p^M)$. Then $c \equiv \hat{c} \pmod{p^M}$ where $\hat{c}$ is not in $a + (p^N)$. This means that $\hat{c} \not\equiv a \pmod{p^N}$. If $c \equiv \hat{c} \pmod{p^M}$, then because $M > N$, we must have $c \equiv \hat{c} \pmod{p^N}$ too. By the transitive property, $c \not\equiv a \pmod{p^N}$. Therefore, if c is not an element of any $\hat{a} + (p^M)$ then c is not an element of $a + (p^N)$. We conclude that we have not left out any points, and $\hat{a} + (p^M)$ balls must cover all of $a + (p^N)$.

This gives us a disjoint covering of $B(a, p^{-N})$. The covering is finite, both because $\mathbb{Z}_p$ is compact, and because there are only as many possible $\hat{a}$ candidates as there are representatives mod p^M. Hence, for all $\hat{a} \equiv a \pmod{p^M}$,

$$a + (p^N) = \bigsqcup_{0 \le \hat{a} \le p^M - 1} \hat{a} + (p^M).$$

□

3.5 Continuity

A significant issue with functions is ensuring continuity. The final goal is to interpolate functions, so it is a good idea to understand p-adic continuity.

We will use absolute value signs as the metric rather than a more general distance metric because this thesis stays mostly in the real and p-adic spaces, both of which use similar notation.

A function is pointwise continuous if changing the input a small amount also only changes the output a small amount. Formally,

Definition 3.5.1 (Continuity)**.** *For x and y in X, the map $f : X \to K$ is continuous at point y if, for every $\varepsilon > 0$, there exists a $\delta > 0$ such that*

$$|x - y| < \delta \text{ implies } |f(x) - f(y)| < \varepsilon.$$

A much stronger version of continuity is uniform continuity.

Definition 3.5.2 (Uniform Continuity)**.** *For x and y in X, the map $f : X \to K$ is uniformly continuous if, for every $\varepsilon > 0$, there exists a $\delta > 0$ such that*

$$|x - y| < \delta \text{ implies } |f(x) - f(y)| < \varepsilon.$$

While a continuous function needs a δ for each point, a uniformly continuous function guarantees that the same δ will work for any two points, given a fixed ε. Every uniformly continuous function is continuous, but not every continuous function is uniformly so.

Consider $f(x) = \frac{1}{x}$. Let $\varepsilon > 1$. If $x = \frac{1}{s}$ and $y = \frac{1}{s+1}$, then

$$\left|\frac{1}{s} - \frac{1}{s+1}\right| = \frac{1}{s^2 + s}.$$

On the other hand,

$$|f(x) - f(y)| = |s - (s + 1)| = 1.$$

Thus, for any delta, we can always find an s such that $\frac{1}{s^2+s} > \delta$ while still remaining less than ε.

Hence, $f(x)$ is not uniformly continuous, although it is continuous on $(0, \infty)$.

Uniform continuity is incredibly powerful. Some well-known results of uniform continuity are listed below.

Theorem 3.5.1. *Let $f : X \to Y$ be a continuous mapping. If X is compact, then f is uniformly continuous on X.*

Theorem 3.5.2. *If $f : B \to K$ is a uniformly continuous mapping, and B is dense in A, then f has a unique continuous extension to A.*

Consult Rudin (1976) for proofs of the above..

The strict inequalities used for continuity are conventional, but changing to $\leq$ or $\geq$ would work just as well. If we want something smaller than a given ε, we can just pick a smaller δ.

In the p-adics, higher powers of p are quite small, so adding an arbitrary multiple of p^v is equivalent to adding ε and δ in classical analysis proofs. By

Theorem 3.5.1, if f is continuous on a dense subset of $\mathbb{Z}_p$ (or $\mathbb{Z}_p$ itself), then it is uniformly continuous since $\mathbb{Z}_p$ is compact. This thesis will only look at values in $\mathbb{Z}_p$, so that is enough for us. The p-adic (uniform) continuity criterion can be written in several different ways.

Definition 3.5.3 (p-adic Continuity I)**.** *Let S be dense in $\mathbb{Z}_p$. Map $f : S \longrightarrow K$ is uniformly continuous if, for $x, y \in S$ and $m \in \mathbb{Z}$, there exists an $n \in \mathbb{Z}$ such that*

$$x \equiv y \pmod{p^n} \textit{ implies } f(x) \equiv f(y) \pmod{p^m}.$$

By definition of mod, the above means that for integers j and k, $x = y + jp^n$ and $f(x) = f(y) + kp^m$. The p-adic absolute value simplifies things a bit.

Definition 3.5.4 (p-adic Continuity II)**.** *Let S be dense in $\mathbb{Z}_p$. Map $f : S \longrightarrow K$ is uniformly continuous if, for $x, y \in S$ and $m \in \mathbb{Z}$, there exists an $n \in \mathbb{Z}$ such that*

$$|x - y|_p \leq \frac{1}{p^n} \textit{ implies } |f(x) - f(y)|_p \leq \frac{1}{p^m}.$$

3.6 Conceptualizing p-adic Topology: A Study in Indigo

All functions in this thesis are interpolated for $\mathbb{Z}_p$ rather than $\mathbb{Q}_p$, so we spend most of our time there. A good portion of interpolation requires understanding the topology of the p-adic integers. How, then, do we conceptualize $\mathbb{Z}_p$, with its new ways of grouping numbers together?

Suppose you are taking part in a study where you are given a large bowl of dark blue paint (indigo blue, if you are curious), and an infinite supply of white paint (China white) off to the side. You are also given a teaspoon.

The instructions say to add teaspoons of white paint to the blue until you have created your perfect shade. Then, write down the number of teaspoons you added. Being, as you are, a big fan of dark blue, you only add three teaspoons of white to your bowl. The person to the right of you adds twelve teaspoons and is dismayed by the amount of stirring required. The person to the left of you disdainfully declares that they will add five million teaspoons, daring anyone to challenge them. You decide they are probably the type of person who likes to play devil's advocate in history classes.

Once everyone has completed their paint mixtures, the people in charge collect your data and thank you. They say they are going to sort you into groups based on the number of teaspoons and your Spotify Wrapped, and build personality archetypes around it (psych majors are always saying things like this).[1] Then, they send you home with 20 bucks and a voucher for frozen yogurt.

Topology in the p-adics works a lot like the paint study. Imagine $\mathbb{Z}_p$ as a chart of all the study data. At the center is 0, pure white.

At the edges are those who added no paint at all, with a p-adic value of 1. This is an entire collection of different people (or numbers) who, despite not being the same person (or number), are p-adically the same size.

Add one teaspoon of white paint and you have made slightly lighter shade of blue, a little bit closer to that 0. This is everything with a p-adic value of $|p|_p$ or $\frac{1}{p}$. Perhaps there is an integer a such that someone is actually ap rather than p. Perhaps there is another integer b such that someone else is bp. Regardless, everyone is in the same category.

Two teaspoons means you are in the $|p^2|_p$, or the $\frac{1}{p^2}$ group, and so on.

We can use the study to investigate balls like $B(a, p^{-N})$ from Section 3.4 too.

For example, you and the person to the right of you are exactly p^{-3} away from each other:

$$\begin{aligned} \text{You } &= ap^3 \\ \text{Them } &= bp^{12} \\ |\text{You } - \text{ Them}|_p &= |ap^3 - bp^{12}|_p = |p^3(a - bp^9)|_p = \frac{1}{p^3}. \end{aligned}$$

Meanwhile, you and the person to your left are also p^{-3} away from each other:[2]

$$\begin{aligned} \text{You } &= ap^3 \\ \text{Them } &= cp^{5{,}000{,}000} \\ |\text{You } - \text{ Them}|_p &= |ap^3 - cp^{5{,}000{,}000}|_p = |p^3(a - cp^{4{,}999{,}997})|_p = \frac{1}{p^3}. \end{aligned}$$

This is the ball $B(a, p^{-3})$ at work. Because everyone contains p^k where $k \geq 3$, the first three terms in their p-adic expansions will all be 0. Hence,

$$\text{You } \equiv \text{ Person to the Right } \equiv \text{ Person to the Left} \pmod{p^3}.$$

[1]A psych major has assured me that personality archetypes are pseudoscience. So if you are a psych major, this is a joke.

[2]Statistically-speaking. Emotionally, you are worlds apart.

All of you exist inside $B(a, p^{-3})$. It is as though the researchers made a group of everyone who added three or more teaspoons of white paint.

Every ball functions like this, as though every group made by the psych study is of the form "everyone who added x teaspoons or more." For any ball of radius p^{-N}, every number of size p^{-M} where $M > N$ is included.

Moreover, by definition of the p-adic norm, there is no way to take the norm of something and get a number which is not a power of p. Thus, every p-adic number is some power of p away from everything else.

If we were to extend this metaphor to the rest of $\mathbb{Q}_p$, we could say that if lightening the paint means multiplying by p, darkening the paint is like dividing by p.

You may still be in suspense over this story. Rest easy, reader. Your personality archetype is Admiral Blue. Also, you did get frozen yogurt. It was mango, and it was delicious.

Chapter 4

DIY p-adic Zeta

Finally, we can commence with the Riemann zeta p-adic interpolation. This chapter begins with interpolating a smaller component of the function. Next, we investigate something called a "p-Euler term," and then build a p-adic measure. In Section 4.4, we build a p-adic integral. Section 4.5 finally sees the interpolation of the zeta function.

Overall, we try to slowly build up to the more complicated function seen below.

As seen in Section 2.2, for integer $k > 1$,

$$\zeta(1-k) = -\frac{B_k}{k}. \tag{4.1}$$

The standard Riemann zeta function is an infinite sum but the p-adic Riemann zeta function is based around Equation 4.1.

The end goal is a version of the Riemann zeta function which takes integer values and outputs p-adic values.

Definition 4.0.1 (Kubota-Leopoldt Zeta Function)**.** *The Kubota-Leopoldt p-adic zeta function is the continuous map $\zeta_p : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ defined as*

$$\zeta_p(1-k) = (1-p^{k-1})\left(\frac{-B_k}{k}\right). \tag{4.2}$$

What is of even more importance, though, is establishing that the above equation is equivalent to

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

for $\alpha \in \mathbb{Z}_p^\times$ and k a positive integer. Later, we will prove that all outputs will be independent of the choice of α. The result is two separate representations of the Kubota-Leopoldt zeta function. The fancy integral representation of the function is known as a "Mellin-Mazur integral transform." Do not worry too much about the notation and Greek letters for the moment; we will build up to them.

Through substitution of Equation 4.1 into Equation 4.2, we can further establish the helpful relation for integer $k > 1$:

$$\zeta_p(1-k) = (1-p^{k-1})\zeta(1-k).$$

Once we have established the above relations, we can extend the Kubota-Leopoldt zeta function to allow inputs of any p-adic integer, rather than just $(1-k) \in \mathbb{Z}$. Any p-adic integer will be congruent to some number mod $p-1$, between 0 and $p-2$. We will fix a representative s_0 and stipulate that any input must be congruent to this $s_0 \pmod{p-1}$. The generalized p-adic zeta function is more like a family of functions: if we want a different s_0, we end up with a slightly different equation.

Notationally, we let S be the set of all p-adic integers congruent to $s_0 \pmod{p-1}$. Then the generalized p-adic zeta function, written ζ_{p,s_0}, maps from S to $\mathbb{Z}_p$.

For $s \in \mathbb{Z}_p$ and $\alpha \in \mathbb{Z}_p^\times$,

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

4.1 A Smaller Step

In the previous section, we said we wanted to prove that our eventual p-adic zeta function is equal to

$$\frac{1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}. \tag{4.3}$$

Moreover, we will want to generalize the zeta function to

$$\zeta_{p,s_0}(s) = \frac{1}{\alpha^{-(s_0+s(p-1))}-1}\int_{\mathbb{Z}_p^\times} x^{s_0+s(p-1)-1}\mu_{1,\alpha}. \tag{4.4}$$

Those integrands, x^{k-1} and $x^{s_0+s(p-1)-1}$, are a much smaller function. In simpler terms, they are x^s where $s \in \mathbb{Z}_p$.

Before interpolating the whole Riemann zeta function, it's easier to begin with this simpler component:

$$f(s) : \mathbb{Z}_p \to \mathbb{Z}_p$$

defined by

$$f(s) = n^s$$

where n is a fixed nonnegative integer. Although the x in Equation 4.4 seems to be a p-adic integer, and $f(n)$ uses a normal integer for n, the process of taking p-adic integrals will reconcile the difference.

Many parts of modular arithmetic act oddly when numbers are divisible by our mod, and the p-adics are closely related to mod. It might, then, be prudent to interrogate $p|n$ here, and see if $f(s)$ is still continuous.

Suppose $p|n$. Then by definition of divisibility, $n = pm$ for some integer m. We could rewrite $f(s)$ as

$$f(s) = (pm)^s.$$

To check continuity, we would like to see what happens when we change our input a little bit. Start with s_0 and let $s = s_0 + ap^v$, where a and v are positive integers.

Then

$$\begin{aligned} |n^{s_0} - n^s|_p &= |(pm)^{s_0} - (pm)^{s_0+ap^v}|_p \\ &= |p^{s_0}m^{s_0}|_p|1 - p^{ap^v}m^{ap^v}|_p \\ &\leq \frac{1}{p^{s_0}}. \end{aligned}$$

The second term in the second to last line, mod p, reduces to 1, so we know it is not divisible by p. Hence, the p-adic absolute value of the whole thing is $1/p^{s_0}$, regardless of the actual values of a or m or v. Moving closer to s does not change the output in any way, so we can never get close enough to prove continuity when $p|n$. Accordingly, we restrict ourselves to $p \nmid n$.

Numbers in the p-adics often have infinite-tailed expansions, and we want to be able to use these infinite expansions as exponents.

When a calculator computes 9^e, it is not really plugging in the irrational number e. It cannot possibly compute the infinite number of digits contained in e. Instead, it calculates an approximation. It might calculate $9^{2.7}$, and then $9^{2.71}$, then $9^{2.7182}$, and so on. The exponents start out the same but new numbers are added to the end of the decimal each time. Eventually, the calculator will stop adding digits, take the limit of its outputs, and call it a day.

We too will calculate approximations; we just have to make sure our outputs are close to each other each step of the way so they converge p-adically.

Let $s \in \mathbb{Z}_p$,

$$s = s_0 + s_1 p + s_2 p^2 + s_3 p^3 + \dots.$$

Consider the partial sums of s:

$$\begin{aligned} &s_0 \\ &s_0 + s_1 p \\ &s_0 + s_1 p + s_2 p^2 \\ \dots \end{aligned}$$

We can construct n^s for some positive integer n by taking the limit of n to the partial sums of s:

$$\begin{aligned} &n^{s_0} \\ &n^{s_0+s_1 p} \\ &n^{s_0+s_1 p+s_2 p^2} \\ &\dots \end{aligned}$$

To ensure that the p-adic limit exists, each partial n^s must be close to the one before and after it. This can be difficult to guarantee.

For example, consider $10^{2+(7^2)+\cdots}$ p-adically. Let $n = 10 = 3 + 1 \cdot 7$ and $s_0 = 2$. Let $s = 2 + 7^2$, and let $p = 7$. Then

$$\begin{aligned} |10^2 - 10^{2+7^2}|_7 &= |10^2|_7 \cdot |1 - 10^{7^2}|_7 \\ &= 1 \cdot |1 - (3 + 1 \cdot 7)^{7^2}|_7. \end{aligned}$$

By Fermat's Little Theorem, $a^p \equiv a \pmod{p}$. A direct consequence is that $3^{7^2} \equiv 3 \pmod{7}$, and therefore

$$\begin{aligned} (3 + 7)^{7^2} &\equiv 3^{7^2} \pmod{7} \\ &\equiv 3 \pmod{7}. \end{aligned}$$

By definition of mod, $(3+1\cdot 7)^{7^2} = 3+7m$ where m is some integer. Substitute in the new representation for $(3 + (1 \cdot 7))^{7^2}$ to get

$$|1 - 3 - 7m|_7 = |-2 - 7m|_7 = 1.$$

Even though s_0 and s were 7-adically close, $f(s_0)$ and $f(s)$ were not. To get around this, we use another application of Fermat's Little Theorem:

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

Proposition 4.1.1. *Let $f(s) : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ be the function $f(s) = n^s$ where $p \nmid n$. If $s \equiv s_0 \pmod{p-1}$ and $s \equiv s_0 \pmod{p^k}$, then $f(s_0)$ and $f(s)$ are p-adically close to each other, meaning the distance between them is less than a power of p.*

Proof. Let $s = s_0 + m(p-1)p^k,\ m \in \mathbb{Z}$.

Then $|s_0 - s|_p = |-p^k(p-1)m|_p \le \frac{1}{p^k}$. We need to show that $|n^{s_0} - n^s|_p$ is also small. Without loss of generality, let $s > s_0$:

$$|n^{s_0} - n^s|_p = |n^{s_0}|_p \cdot |1 - n^{m(p-1)(p^k)}|_p = 1 \cdot |1 - (n^{p-1})^{mp^k}|_p.$$

By Fermat's Little Theorem, $n^{p-1} \equiv 1 \pmod{p}$, which means $n^{p-1} = 1 + bp$ for integer b. Through substitution,

$1 \cdot |1 - (n^{p-1})^{mp^k}|_p = |1 - (1 + bp)^{mp^k}|_p$ which, by the binomial formula, becomes

$$= |1 - (1 + mp^k(bp) + \frac{(mp^k)!b^2p^2}{2(mp^k-2)!} + \cdots + (bp)^{mp^k})|_p$$
$$= |-bmp^{k+1} + \frac{1}{2}(b^2mp^{k+1}(mp^k-1)) + \cdots + (bp)^{mp^k}|_p.$$

Every term in that last line has at least p^{k+1} in it, and thus

$$|n^{s_0} - n^s|_p \le |p^{k+1}|_p = \frac{1}{p^{k+1}}.$$

□

The idea of proving two outputs are close when two inputs are close is equivalent to proving continuity. Before explicitly making the connection between 4.1.1 and function continuity, however, we need new terminology.

Definition 4.1.1 (Set S). *Let S be the set of all p-adic integers which are congruent to s_0 mod $p-1$ and mod p^k for some nonnegative integer k.*

Corollary 4.1.0.1. *The function $f(s) = n^s$ is a continuous mapping from S to $\mathbb{Z}_p$.*

Proof. This follows directly from Proposition 4.1.1. □

One last lemma remains before we test out the new function.

Lemma 4.1.1. *For natural numbers a and m and n, if $p \nmid a$,*

$$(1 + a \cdot p^m)^{p^n} = 1 + a \cdot p^{m+n} + \dots$$

where every term after $a \cdot p^{m+n}$ is a larger power of p.

The proof is merely the binomial formula.

To test out the lemmas, we can modify the earlier example. Let $n = 10$, $s_0 = 2$, and $s = 2 + 6 \cdot 7^2$. Then

$$\begin{aligned} |10^2 - 10^{2+6\cdot 7^2}|_7 &= |10^2|_7 \cdot |1 - ((3 + 1 \cdot 7)^6)^{7^2}|_7 \\ &= 1 \cdot |1 - (1 + 7k)^{7^2}|_7 \text{ by Fermat's Little Theorem for integer } k \\ &= |1 - (1 + k \cdot 7^3 + \dots)|_7 \text{ by Lemma 4.1.2} \\ &\le \frac{1}{7^3}. \end{aligned}$$

Happily, we have ended up somewhere nice.

Although it may seem as though we have limited the candidates for s, by the below lemma, any p-adic input will work.

Lemma 4.1.2. *Fix some $s_0 = \{0, 1, \dots, p-2\}$. Then S is dense in $\mathbb{Z}_p$.*

Proof. One definition of density states that A is dense in B if, for any $b \in B \backslash A$ and for any $\varepsilon > 0$, there is an element $a \in A$ such that $|a - b| \le \varepsilon$. In the p-adics, we want to find an element of S less than some power of p away from $b \in \mathbb{Z}_p$.

Let

$$b = b_0 + b_1 p + b_2 p + \cdots + b_n p^n + \dots,$$

and let $\varepsilon = \frac{1}{p^{n+1}}$ where $n \in \mathbb{N}$.

Mod $p - 1$, let

$$b_0 + b_1 p + \cdots + b_n p^n \equiv y,$$

where $0 \le y \le p - 2$. All we need to do is add another term to get to $s_0 \pmod{p-1}$. If $s_0 - y \equiv z \pmod{p-1}$, then add zp^{n+1}. Multiplying by p^{n+1} will not change the value mod $p-1$, because $p^{n+1} \equiv 1 \pmod{p-1}$. Therefore, $zp^{n+1} \equiv z \pmod{p-1}$.

Thus,

$$\beta = b_0 + b_1 p + \cdots + b_n p^n + zp^{n+1} \in S,$$

and

$$|b - \beta|_p = |(b_{n+1} - z)p^{n+1} + \dots|_p \le \frac{1}{p^{n+1}}.$$

By definition, S is dense in $\mathbb{Z}_p$. □

By density on a compact set, we have a unique extension $f(s) : S \to \mathbb{Z}_p$ to $f(s) : \mathbb{Z}_p \to \mathbb{Z}_p$. In practice, we use the approximations detailed above as our partial s_0 sums.

Example: Let $n = 10$, and let

$$s = \frac{2}{9} = 1 + (3 \cdot 7) + (5 \cdot 7^2) + (0 \cdot 7^3) + \dots.$$

The proof of the density of S outlines our strategy for computing n^s to the 7^3 place. Start with $a = 1$ and find n^a :

$$10^1 = 3 + (1 \cdot 7).$$

The next partial sum is $1 + (3 \cdot 7)$, which is congruent to 4 mod 6. Since $1 - 4 \equiv 3 \mod 6$, to make the sum congruent to 1 mod 6 (and 7), add $3 \cdot 7^2$. Let $b = 1 + (3 \cdot 7) + (3 \cdot 7^2)$, and rewrite in terms of 6, leaving the initial 1 alone:

$$b = 1 + (7)(24) = 1 + (6 \cdot 4 \cdot 7).$$

Plug into $f(s)$:

$$\begin{aligned} 10^{1+6\cdot4\cdot7} &= (3 + (1 \cdot 7))[((3 + 1 \cdot 7)^6)^4]^7 \\ &= (3 + (1 \cdot 7))((1 + (1 \cdot 7) + (3 \cdot 7^2) + (3 \cdot 7^3) + \dots)^4)^7 \\ &= (3 + (1 \cdot 7))(1 + (4 \cdot 7) + (4 \cdot 7^2) + (5 \cdot 7^3) + \dots)^7 \\ &= (3 + (1 \cdot 7))(1 + (0 \cdot 7) + (4 \cdot 7^2) + (3 \cdot 7^3) + \dots) \\ &= 3 + (1 \cdot 7) + (5 \cdot 7^2) + (0 \cdot 7^3) + \dots. \end{aligned}$$

The remaining calculations are quite similar. We shall leave the explicit computation to the reader, but if you intend to do it, the multinomial formula and/or copious amounts of free time are advised. The next partial sum leads us to

$$c = 1 + (6 \cdot 4 \cdot 7) + (6 \cdot 5 \cdot 7^2),$$

meaning our calculations will build on 10^b:

$$\begin{aligned} 10^c &= (10^b)[((3 + (1 \cdot 7))^6)^5]^{7^2} \\ &= 3 + (1 \cdot 7) + (5 \cdot 7^2) + (5 \cdot 7^3) + \dots. \end{aligned}$$

Any further calculations will merely change the 7^4 and higher powers, so we stop here. Accordingly,

$$10^{1+(3\cdot7)+(5\cdot7^2)+(0\cdot7^3)+\dots} = 3 + (1 \cdot 7) + (5 \cdot 7^2) + (5 \cdot 7^3) + \dots..$$

To transition to the Riemann zeta function, we need to go from n^s to n^{-s}. Thankfully, the proof of Proposition 4.1.1 still holds with a negative sign in front of the exponents (this is left to the reader as an exercise. Turnabout is fair play). Thus, we retain our domain.

4.2 Interlude

The function n^s in the previous section did not work when p divided n, so we know that the $\frac{1}{n^s}$ term in the Riemann zeta sum will not be interpolatable when $p|n$. As may be evident from the amount of pages left to go, interpolating the Riemann zeta function is a rather complicated process. Still, we can pretend for the moment that all we need to do is isolate the parts of the sum we can work with:

$$\begin{aligned}
\zeta(s) &= \sum_{n=1} \frac{1}{n^s} \\
&= \sum_{n=1,p\nmid n} \frac{1}{n^s} + \sum_{n=1,p|n} \frac{1}{n^s} \\
&= \sum_{n=1,p\nmid n} \frac{1}{n^s} + \sum_{n=1} \frac{1}{p^s n^s} \\
&= \sum_{n=1,p\nmid n} \frac{1}{n^s} + \frac{1}{p^s}\zeta(s).
\end{aligned}$$

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

Solving for ζ^* in the previous equation achieves

$$\zeta^*(s) = (1 - p^{-s})\zeta(s).$$

An alternative form for the Riemann zeta function is called an "Euler product," or an infinite product

$$\zeta(s) = \prod_{\text{prime } p} \left(\frac{1}{1 - p^{-s}}\right).$$

Multiplying the Riemann zeta function by $(1 - p^{-s})$ amounts to removing a factor from this infinite product, so the process described above is often called "removing the p-Euler factor." Regardless of where the rest of the interpolation takes us, we will need to take out the p-Euler factor. This is not the end goal, but it is a good start.

4.3 Measures

The best interpolation we have for $\frac{-B_k}{k}$ involves an integral, which means we are going to need a p-adic measure.

The standard calculus integral looks like

$$\int_a^b f(x)\,dx.$$

Every integral needs three things:

1. an interval (like $[a,b]$),
2. an integrand (like $f(x)$), and
3. a measure (like dx).

Number 1 is straightforward. Recall Section 3.4's discussion of balls of the form

$$a+(p^n) \text{ or } B(a,p^{-n}) = \left\{x \in \mathbb{Q}_p : |x-a|_p \leq \frac{1}{p^n}\right\}.$$

The full notation is $a + p^n\mathbb{Z}_p$, but it becomes abbreviated to $a + (p^n)$. These are our intervals.

Integration in the p-adics takes place over sets which are both compact and open. Every compact-open set in $\mathbb{Z}_p$ can be written as the disjoint union of $B(a,p^{-n})$ for different values of a. This is great news because we are going to need to be able to break regions up into disjoint areas (or balls) for our integral measure.

As the name suggests, a measure is how we measure or quantify sets.

Definition 4.3.1 (Measure)**.** *A measure μ on topological space A is an additive map from A to the nonnegative reals.*

For example, the standard measure for $\mathbb{R}^k$ is called the Lebesgue measure. For $\mathbb{R}^1$, this looks like the distance between two points: $|b-a|$. For $\mathbb{R}^2$, Lebesgue measure is area and for higher dimensions, it is volume.

Since we are talking about area, it makes sense to build up a larger region with its smaller components. This is the "additive" component mentioned in the definition. We need our measure to respect addition because otherwise, nothing makes sense and we might as well take up philosophy. Specifically, the measure should be additive for finite disjoint sets. If the sets overlap, "adding" them becomes convoluted; see Figure 4.1 for an example.

Formally, for measure μ and disjoint sets A_i,

$$\mu\left(\bigsqcup_{i=1}^{k} A_i\right) = \sum_{i=1}^{k} \mu(A_i).$$

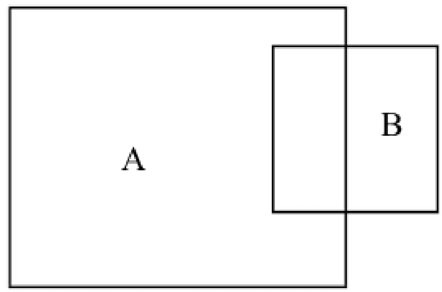

Figure 4.1 $A \cup B = A + B - (A \cap B)$?

In the p-adics, measures must also be bounded. For an explanation, consult Bowers (2004: p.19).

The measure which we will use is the regularized kth Bernoulli measure, denoted $\mu_{k,\alpha}$. The reason is twofold. First, Bernoulli numbers are already vital to the Riemann zeta function, and they are closely related to Bernoulli measures. More pressingly, though, Bernoulli polynomials turn out to be the only polynomials which work as p-adic measures, so we are not exactly drowning in alternatives.

We actually start with the Bernoulli distribution (unrelated to probability), which is *almost* a measure, except it is not always bounded. The Bernoulli distribution is defined by

$$\mu_k(a + (p^n)) = p^{n(k-1)} B_k\left(\frac{\{a\}}{p^n}\right)$$

where $B_k(x)$ is the kth Bernoulli polynomial, and $\{a\}$ is the representative from $\{0, \ldots, p^n - 1\}$ which is congruent to a mod p^n. Most of the time, to make things easier, we forego the brackets and just write a.

Recall, from Section 2.2, the Bernoulli polynomials:

$$B_0(x) = 1,$$
$$B_1(x) = x - \frac{1}{2},$$
$$B_2(x) = x^2 - x - \frac{1}{6},$$

and so on.

Some Bernoulli measures:

$$\mu_0(a + (p^n)) = p^{n(-1)} B_0\left(\frac{a}{p^n}\right) = \frac{1}{p^n}, \text{ and}$$
$$\mu_1(a + (p^n)) = p^{n(0)} B_1\left(\frac{a}{p^n}\right) = \frac{a}{p^n} - \frac{1}{2}.$$

The first, μ_0, is known as the p-adic Haar distribution, and μ_1 is the Mazur distribution.

Section 2.2 also established that $B_k(0) = B_k$, the k^{th} Bernoulli number.

Thus, for example,

$$\mu_k(\mathbb{Z}_p) = \mu_k(0 + (p^0)) = B_k(0) = B_k,$$

and

$$\mu_k(p\mathbb{Z}_p) = \mu_k(0 + (p^1)) = p^{k-1} B_k.$$

This is mostly a good way to quantify our region, but as stated earlier, to be a p-adic measure, any distribution μ must be bounded by some real constant. As it stands now, μ_k has a tendency to go off to infinity.

All is not lost; it is possible to turn the Bernoulli distribution into a measure by "regularizing" it.

Definition 4.3.2 (Bernoulli Measure)**.** *For all $\alpha \in \mathbb{Z}_p^\times$, the k^{th} Bernoulli measure over compact-open set X is*

$$\mu_{k,\alpha}(X) = \mu_k(X) - \alpha^{-k}\mu_k(\alpha X).$$

In Section 4.5, we will see that the choice of α does not matter: the answer will still be the same.

Alas, the regularized Haar distribution is a bit anticlimactic:

$$\begin{aligned}\mu_{0,\alpha}(a + (p^n)) &= \mu_0(a + (p^n)) - \alpha^0 \mu_0(\alpha a + (p^n)) \\ &= \frac{1}{p^n} - \frac{1}{p^n} \\ &= 0.\end{aligned}$$

Fine. Whatever. The Mazur measure, on the other hand, is functional. Letting $(\alpha a)_0$ be the representative from $(\alpha a + (p^n))$ such that $0 \le (\alpha a)_0 \le$

$p^n - 1$, we find

$$\begin{aligned}\mu_{1,\alpha} &= \mu_1(a + (p^n)) - \alpha^{-1}\mu_1(\alpha a + (p^n)) \\ &= \frac{a}{p^n} - \frac{1}{2} - \frac{1/\alpha(\alpha a)_0}{p^n} + \frac{\alpha^{-1}}{2} \\ &= \frac{1/\alpha - 1}{2} + \frac{1}{\alpha}\left(\frac{\alpha a}{p^n} - \frac{(\alpha a)_0}{p^n}\right) \\ &= \frac{1/\alpha - 1}{2} + \frac{1}{\alpha}\left\lfloor \frac{\alpha a}{p^n} \right\rfloor.\end{aligned}$$

For example,

$$\mu_{k,\alpha}(\mathbb{Z}_p) = B_k(0) - \alpha^{-k}B_k(0) = (1 - \alpha^{-k})B_k.$$

Additionally,

$$\begin{aligned}\mu_{k,\alpha}(p\mathbb{Z}_p) &= \mu_k(p\mathbb{Z}_p) - \alpha^{-1}\mu_k(\alpha p\mathbb{Z}_p) \\ &= p^{k-1}B_k - \alpha^{-k}p^{k-1}B_k \\ &= p^{k-1}B_k \cdot (1 - \alpha^{-k}).\end{aligned}$$

Picture $\mathbb{Z}_p$ as the ball $B(0,1) = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$, meaning $\mathbb{Z}_p^\times$ is the boundary. The inside of the ball, or every $x \in \mathbb{Q}_p$ such that $|x|_p < 1$, is $p\mathbb{Z}_p$. Thus, $\mathbb{Z}_p = \mathbb{Z}_p^\times \cup p\mathbb{Z}_p$ without any overlap.

A defining quality of a measure is that it is an additive map, so

$$\begin{aligned}\mu_{k,\alpha}(\mathbb{Z}_p^\times) &= \mu_{k,\alpha}(\mathbb{Z}_p) - \mu_{k,\alpha}(p\mathbb{Z}_p) \\ &= [(1 - \alpha^{-k}) - p^{k-1}(1 - \alpha^{-k})]B_k \\ &= (1 - p^{k-1})(\alpha^{-k} - 1)(-B_k).\end{aligned}$$

The goal of changing from a distribution to a measure is to get a bound. We can be more specific than simply saying a measure like $\mu_{1,\alpha}$ is bounded though.

Lemma 4.3.1. *For compact-open set $X \subset \mathbb{Z}_p$,*

$$|\mu_{1,\alpha}(X)|_p \leq 1.$$

Proof. For some interval $I = a + (p^n)$ and some $\alpha \in \mathbb{Z}_p^X$,

$$\mu_{1,\alpha}(a + (p^n)) = \frac{1/\alpha - 1}{2} + \frac{1}{\alpha}\left\lfloor \frac{\alpha a}{p^n} \right\rfloor.$$

By the non-Archimedean property,

$$|\mu_{1,\alpha}(I)|_p \leq \max\left\{\frac{1/\alpha - 1}{2}, \frac{1}{\alpha}\left\lfloor\frac{\alpha a}{p^n}\right\rfloor\right\}.$$

Since $\alpha \in \mathbb{Z}_p^\times$, $|1/\alpha|_p = 1$. Furthermore, since all numbers outside $\mathbb{Z}_p$ have p in the denominator, all integers must be elements of $\mathbb{Z}_p$. Consequently, $\left\lfloor\frac{\alpha a}{p^n}\right\rfloor \in \mathbb{Z}_p$. Therefore,

$$\left|\frac{1}{\alpha}\left\lfloor\frac{\alpha a}{p^n}\right\rfloor\right|_p \leq 1.$$

If $p = 2$, then α must be odd. Thus $(1/\alpha) - 1 = (1-\alpha)/\alpha$ must have an even numerator. Multiplying through by $1/2$ then clears the 2 in the denominator:

$$\left|\frac{(1/\alpha) - 1}{2}\right|_p \leq 1.$$

If $p > 2$, then $\frac{1}{2\alpha} \in \mathbb{Z}_p^\times$ and $\frac{1}{2} \in \mathbb{Z}_p^\times$. By the non-Archimedean property,

$$\left|\frac{1}{2\alpha} - \frac{1}{2}\right|_p \leq \max\left\{\frac{1}{2\alpha}, \frac{1}{2}\right\} = 1.$$

Combining everything, we see $|\mu_{1,\alpha}(I)| \leq 1$.

Any compact-open set X can be expressed as the disjoint union of balls like I, and measures are additive maps, so by the non-Archimedean property,

$$|\mu_{1,\alpha}(X)|_p \leq \max\{\mu_{1,\alpha}(I_i)\} \leq 1.$$

□

We specifically bounded $\mu_{1,\alpha}$ because, regardless of which Bernoulli measure we ultimately want to use, all other Bernoulli measures can be related back to $\mu_{1,\alpha}$.

Lemma 4.3.2. *Let d_k be the lowest common divisor of the coefficients of $B_k(x)$. Then*

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

The d_k is unimportant, but difficult to get rid of. We can safely forget about it, except in calculations. Lemma 4.3.2 otherwise says

$$\mu_{k,\alpha}(X) \sim k a^{k-1}\mu_{1,\alpha}(X).$$

The above statement is like a change of variable in standard calculus. Imagine you are changing an integral variable from x to x^k. You also need to change the measure, from dx to $d(x^k)$:

$$\frac{d(x^k)}{dx} = kx^{k-1}.$$

The $d(x^k)$ denotes x^k evaluated on a vanishingly small interval $[a, b]$, defined as $b^k - a^k$. The p-adic measure $\mu_{k,\alpha}$ is like this $d(x^k)$, and we can write $\mu_{k,\alpha}([a, b])$. Similarly, the dx is x evaluated on $[a, b]$: $b - a$. In our case, dx is $\mu_{1,\alpha}([a, b])$. Recall that dx means taking the measure of an incredibly tiny interval, one where b gets closer and closer to a. Putting everything together, $\frac{d}{dx}(x^k)$ acts like the fraction

$$\lim_{b \to a} \frac{\mu_{k,\alpha}([a, b])}{\mu_{1,\alpha}([a, b])} = kx^{k-1}.$$

Next multiply through by the denominator:

$$\lim_{b \to a} \mu_{k,\alpha}([a, b]) = kx^{k-1}\mu_{1,\alpha}([a, b]).$$

Replace the interval $[a, b]$ with our actual area X to get

$$\mu_{k,\alpha}(X) = kx^{k-1}\mu_{1,\alpha}(X).$$

In other words, the ka^{k-1} is really the chain on switching measures. For a more formal proof, see Koblitz (1984: p.37).

4.4 Building the Integral

Having defined the p-adic measure, we can now assemble the general p-adic integral.

The traditional Riemann integral is defined by taking a limit of Riemann sums, where for partition P,

$$R(P, f) = \sum_{i=1}^{n} f(c_i)\Delta x_i$$

for some c_i in each interval.
The p-adic analogue follows the same layout.

Definition 4.4.1 (p-adic Riemann Sums). *For some $x_{a,N} \in a + (p^N)$ and p-adic measure μ on compact-open set X, the Riemann sum over X is*

$$S_N = \sum_{a+(p^N)\subset X} f(x_{a,N})\mu(a + (p^N)).$$

Theorem 4.4.1. *If $f : X \to Y$ is continuous with $X \subset \mathbb{Z}_p$, then the limit*

$$\lim_{N\to\infty} \{S_N\}$$

converges to a limit in Y independent of the choice of $x_{a,N}$. We call this unique limit

$$\int_X f\mu.$$

Proof. Consider the sequence of Riemann sums $\{S_N\}$. We can show that this sequence is Cauchy. Since $\mathbb{Q}_p$ is complete, that means $\{S_N\}$ converges.

We cannot always directly take the measure of X because X might not be connected. Consequently, we break X up into compact-open sets U.

The measure on X must be bounded so that the integral can converge. In general, by definition, a p-adic measure is bounded, so there exists some $B_i \in \mathbb{R}$ such that $\mu(U) \leq B_i$ for a compact-open $U \subset X$. Let B_1 be the bounding constant for the first compact-open set, B_2 for the second compact-open set, and so on. Because X is compact, it can be covered by a finite number of these U sets. Thus, there will be a maximum constant. Let $B = \max\{B_1, B_2, \dots\}$. Then $\mu(U) \leq B$ for every $U \subset X$.

Let $U = B(a, p^{-N})$, or disjoint balls of the form $a + (p^N)$.

Next, fix $\varepsilon > 0$. By compactness, the continuous function $f(x)$ is uniformly continuous. By definition, there is some $N_0 \in \mathbb{N}$ such that $N > N_0$ implies

$$|f(a) - f(\hat{a})|_p < \frac{\varepsilon}{B} \text{ when } a \equiv \hat{a} \pmod{p^N}.$$

Let $M > N > N_0$. To prove that the series of S_N is Cauchy, we want to prove that $|S_N - S_M|_p < \varepsilon$.

Let U be of the form $a + (p^N)$. Choose N large enough so that every $a + (p^N)$ ball is either contained in X or disjoint from it. In other words, pick a covering which is small enough to cover X entirely without going over.

Recall from Section 3.4 that we can define the balls so that $a \in \{0, \dots, p^N - 1\}$. Further, for each term in S_N, let the representative from $a + (p^N)$ be $x_{a,N} = a$. Now is a good time to relate S_N to S_M via $a + (p^N)$.

By Lemma 3.4.2, we can write

$$a + (p^N) = \bigsqcup_{0 \le \hat{a} \le p^M - 1} \hat{a} + (p^M).$$

Substitute the prior equation into S_N:

$$S_n = \sum_{\hat{a}+(p^M) \subset X} f(a)\mu(\hat{a} + (p^M)).$$

By construction, the representatives for S_M will be $x_{a,M} = \hat{a}$. Accordingly,

$$\begin{aligned} |S_N - S_M|_p &= \left| \sum_{\hat{a}+(p^M)\subset X} [f(a) - f(\hat{a})]\mu(\hat{a} + (p^M)) \right|_p \\ &\le \sum_{\hat{a}+(p^M)\subset X} |f(a) - f(\hat{a})|_p \cdot |\mu(\hat{a} + (p^M))|_p \\ &\text{and by the non-Archimedean property,} \\ &\le \max\{|f(a) - f(\hat{a})|_p \cdot |\mu(\hat{a} + (p^M))|_p\} \\ &< \max\left\{\frac{\varepsilon}{B} \cdot B\right\} \\ &= \varepsilon. \end{aligned}$$

Thus, $\{S_N\}$ is Cauchy. By completeness, $\{S_N\}$ converges.

It remains to show that $\{S_N\}$ converges independent of the choice of $x_{a,N}$. However, as discussed in Section 3.4, any representative from $a + (p^N)$ will be congruent to $a \pmod{p^N}$. By the same argument, any representative from $\hat{a} + (p^M)$ will be congruent to $\hat{a} \pmod{p^M}$. All we needed for the sum to converge was $|f(a) - f(\hat{a})|_p < \frac{\varepsilon}{B}$. This inequality stems from $a \equiv \hat{a} \pmod{p^N}$.

Let $x_{\hat{a},M}$ such that $c \in B(\hat{a}, p^{-M})$. Then $c \equiv \hat{a} \pmod{p^M}$. By definition of mod, $c = \hat{a} + kp^M$ for some integer k. Since $M > N$, that last equation can be rewritten as $c = \hat{a} + k(p^N)(p^{M-N})$. When reduced, we see that

$$c \equiv \hat{a} \pmod{p^N}.$$

Since $\hat{a} \equiv a \pmod{N}$, the transitive property says

$$c \equiv a \pmod{p^N}.$$

Thus, we also have $|f(a) - f(c)|_p < \frac{\varepsilon}{B}$, and everything else will progress the same.

If we change the representative for $x_{a,N}$, the same argument applies. In all cases, $x_{a,N} \equiv x_{\hat{a},M} \pmod{p^N}$.

Therefore, the sequence converges independent of the choice of representative. □

Like any self-respecting integral, the p-adic version has bounding properties.

Proposition 4.4.1. *If $f : X \to \mathbb{Q}_p$ is a continuous function, $|f(x)|_p \leq A$ for all $x \in X$, and $\mu(U) \leq B$ for all compact-open $U \subset X$, then*

$$\left| \int_X f\mu \right|_p \leq AB.$$

Proof. We defined $\int_X f\mu$ to be the limit of sums

$$\sum f(x)\mu(x),$$

and by the non-Archimedean property,

$$\left| \sum f(x)\mu(x) \right|_p \leq \max\{|f(x)|_p \cdot |\mu|_p\} \leq AB.$$

□

Corollary 4.4.1.1. *If $f, g : X \to \mathbb{Q}_p$ are two continuous functions and $|f(x) - g(x)|_p \leq \varepsilon$ for all $x \in X$, and $\mu(U) \leq B$ for all compact-open sets $U \subset X$, then*

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

Proof. This follows directly from Proposition 4.4.1. □

4.5 The Mellin-Mazur Integral

At long last, we can return to the main task: interpolating $-B_k/k$. As shown in the previous section, $\mu_k(\mathbb{Z}_p) = B_k$. When we integrate 1 over an area, we get the measure of that area. In other words,

$$\int_{\mathbb{Z}_p} \mu_k = B_k.$$

Therefore,

$$-\frac{B_k}{k} = -\frac{1}{k}\int_{\mathbb{Z}_p} \mu_k.$$

Unfortunately, μ_k is a distribution, not a measure, so it is not integrable. It is, however, possible to relate μ_k to $\mu_{k,\alpha}$ given that one is built off the other, so we can continue to work with regularized measures with the knowledge that things will connect back to Bernoulli numbers.

Theorem 4.5.1. *For compact-open subset $X \subset \mathbb{Z}_p$,*

$$\int_X 1\mu_{k,\alpha}(x) = k\int_X x^{k-1}\mu_{1,\alpha}(x).$$

Proof. By definition,

$$\int_X \mu_{k,\alpha} = \lim_{N\to\infty} \sum_{a+(p^N)\subset X} \mu_{k,\alpha}(a+(p^N)).$$

Lemma 4.3.2 says that

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

for some $A \in \mathbb{Z}$. Thus,

$$\begin{aligned} d_k \sum_{a+(p^N)\subset X} \mu_{k,\alpha}(a+(p^N)) &= \sum_{a+(p^N)\subset X} (d_k k a^{k-1}\mu_{1,\alpha} + Ap^N) \\ &= d_k k \sum_{a+(p^N)\subset X} a^{k-1}\mu_{1,\alpha} + p^N \sum_{a+(p^N)\subset X} A. \end{aligned}$$

Because $A \in \mathbb{Z}_p$, it does not have any factors of p in its denominator. Therefore, p^N cannot be cancelled out by A. As N goes to infinity, $p^N \to 0$. Thus, the

$$\lim_{N\to\infty} p^N \sum_{a+(p^N)\subset X} A = 0.$$

Then

$$d_k \lim_{N\to\infty} \sum_{a+(p^N)\subset X} \mu_{k,\alpha}(a+(p^N)) = d_k k \lim_{N\to\infty} \sum_{a+(p^N)\subset X} a^{k-1}\mu_{1,\alpha}.$$

Since d_k is nonzero, we divide it out. Let $x \in B(a, p^N)$. Then, letting $x_{a,N} = x$ in the Riemann sum, we see

$$\lim_{N\to\infty} \sum_{a+(p^N)\subset X} \mu_{k,\alpha}(a+(p^N)) = k \cdot \lim_{N\to\infty} \sum_{a+(p^N)\subset X} x^{k-1}\mu_{1,\alpha}.$$

Equivalently,

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

□

As we know from Section 4.1, x^s is interpolatable so long as $p \nmid x$. Consequently, let the integral interval be $\mathbb{Z}_p^\times$.

Then we can show that $\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}$ is continuous for certain k values. By Lemma 4.3.1

$$|\mu_{1,\alpha}(U)| \leq 1.$$

Let $f(x) = x^{k'-1}$ where $k' \equiv k \mod p^N(p-1)$. As per our earlier work, by uniform continuity of f,

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

Then Corollary 4.4.1.1 says that

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

So if we fix $s_0 \in \{0, 1, \ldots, p-2\}$ and define S to be the set of all positive integers congruent to s_0 mod $p-1$, we can interpolate $\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}$ as a continuous function where k runs through S. Explicitly, we have

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

Hold onto the s_0 interpretation of the integral, because it will be useful for generalizing the Kubota-Leopoldt function later.

Definition 4.5.1 (Kubota-Leopoldt Zeta Function)**.** *The Kubota-Leopoldt p-adic zeta function is the continuous map* $\zeta_p : \mathbb{Z} \to \mathbb{Z}_p$ *defined as*

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

Theorem 4.5.2. *The Kubota-Leopoldt zeta function is equivalent to a Mellin-Mazur integral*:

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

for $\alpha \in \mathbb{Z}_p^\times$ and k a positive integer. The equality holds for any choice of α so long as $\alpha \neq 1$.

Proof. By Theorem 4.5.1, we know

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

Section 4.3 established that

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

Some manipulation finally gets us what we want:

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

Combined with Theorem 4.5.1,

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

The Kubota-Leopoldt zeta function is defined to be the left side,

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

Remember when we pulled out a factor of $1-p^{-s}$? Here we see the same thing, but for $s = 1-k$. This is why we define the function at $1-k$ rather than at k itself.

Consider the right side of the equation, what is called a Mellin-Mazur integral transform. If $\alpha = 1$, then $1/(\alpha^{-k}-1) = 1/0$. Accordingly, we restrict to $\alpha \neq 1$. The last thing to note is that, outside of the pole, α does not really matter because $\zeta_p(1-k)$ does not depend on α. The two functions are equal, as already proven, so any choice of α should get the same answer for the same k.

All our knowledge concludes in the final equivalent relations seen in the theorem. □

We interpolated a special form of the Riemann zeta function, but we can be confident that we have actually made a function analogous to Riemann zeta. This is because, even though they may not look incredibly similar in all forms, the two are closely related.

Proposition 4.5.1. *At positive integer k,*

$$\zeta_p(1-k) = (1-p^{k-1})\zeta(1-k).$$

Proof. Classical Riemann zeta analysis establishes that

$$\zeta(1-k) = \frac{-B_k}{k}$$

for integers $k > 1$, and thus by substitution,

$$\zeta_p(1-k) = (1-p^{k-1})\zeta(1-k).$$

□

We defined the p-adic zeta function to look like the normal zeta function in its Bernoulli form, but that definition brought with it two extra forms of the p-adic zeta: one in terms of the ordinary Riemann zeta function, and another in the form of a Mellin-Mazur integral.

The Mellin-Mazur form becomes undefined when $\alpha = 1$ or when $k = 0$, because then

$$\frac{1}{\alpha^{-k}-1} = \frac{1}{0}.$$

As already noted, the requirement on α means that if we want to use the integral version, we must specifiy $\alpha \neq 1$. The restriction on k means that ζ_p has a simple pole at 1, or $\zeta_p(1-0)$.

There is, in fact, a more general p-adic zeta function in its integral form which allows for p-adic inputs rather than just integer inputs.

Definition 4.5.2 (Generalized p-adic Zeta Function)**.** *For a fixed s_0 such that $0 \leq s_0 \leq p-1$, and $s \in \mathbb{Z}_p$,*

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

Recall from Section 4.1 that x^s is only defined for $s \equiv s_0 \pmod{p-1}$, so ζ_{p,s_0} is really a family of functions: one for each s_0. Whenever $k \equiv s_0 \pmod{p-1}$, say, $k = s_0 + k_1(p-1)$,

$$\zeta_{p,s_0}(k_1) = \zeta_p(1-k).$$

Exactly like its integer counterpart, ζ_{p,s_0} has a simple pole when k or $s_0 + s(p-1) = 0$. Thus, if $s_0 = 0$, we restrict $s \neq 0$.

We can finish up by plugging some values into the interpolated functions.

After all the hard work and backbreaking analysis, finding some values of the p-adic Riemann zeta function is quite simple. Take the equation

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

Let $p = 7$ and $k = 10$. Then

$$B_{10} = \frac{5}{66}$$

giving us

$$\begin{aligned}\zeta_7(1-10) &= (1-7^{10-1})\left(-\frac{5}{66 \cdot 10}\right)\\ &= (-40353606)\left(-\frac{1}{132}\right)\\ \zeta_7(-9) &= \frac{6725601}{22}.\end{aligned}$$

The 7-adic expansion of 6725601 is $1 + (1 \cdot 7) + (1 \cdot 7^2) + \cdots + (1 \cdot 7^8)$. The coefficients are 1 all the way through. Also,

$$22 = 1 + 3 \cdot 7.$$

When we divide, we see that

$$\zeta_7(-9) = 1 + (5 \cdot 7) + (6 \cdot 7^2) + (1 \cdot 7^3) + \ldots.$$

Chapter 5

Finale

We turn our attention to what comes after the Kubota-Leopoldt zeta function. How is it useful? What was the point of all this?

It turns out that the Kubota-Leopoldt zeta function is a special case of the Kubota-Leopoldt L-function. This p-adic L-function is a topic of much study in modern number theory, particularly throughout Iwasawa theory and the Langlands program.

Before the advent of the p-adics, L-functions were created as a way to generalize the Riemann zeta function. Like the Riemann zeta function, they have Euler products, functional equations, sums, and analytic continuations.

5.1 Dirichlet Characters

To explore L-functions, we will need a type of function from number theory called a Dirichlet character.

Definition 5.1.1 (Dirichlet character)**.** *A Dirichlet character, χ mod n, is a multiplicative operation*

$$\chi : (\mathbb{Z}/n\mathbb{Z})^{\times} \to \mathbb{C}\backslash\{0\}.$$

If k reduces to m mod n, then $\chi(k) = \chi(m)$.

The symbol $(\mathbb{Z}/n\mathbb{Z})$ means the integers mod n, so the “$\times$" in the corner means we are looking at every number with an inverse mod n. Number theory tells us that invertible numbers mod n are those which are relatively prime to n.

A multiplicative function is one which respects multiplication mod n. In other words,

$$\chi(ab) = \chi(a)\chi(b).$$

This property allows us to identify how χ maps the identity element:

$$\begin{aligned} \chi(1 \cdot a) &= \chi(1)\chi(a) \\ \chi(a) &= \chi(1)\chi(a) \end{aligned}$$

and we conclude that $\chi(1) = 1$ always.

One last important property of χ is about its output, concerning Euler's phi function $\phi(n)$.

Proposition 5.1.1. *Dirichlet character χ maps $(\mathbb{Z}/n\mathbb{Z})^{\times}$ to the $\phi(n)^{th}$ roots of* 1.

Proof. By Euler's Theorem, $a^{\phi(n)} \equiv 1 \mod n$ when $n \nmid a$. Every $a \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ is indivisible by n. Hence,

$$\begin{aligned} \chi(a^{\phi(n)}) &= \chi(1) \\ \chi(a \cdot a \cdot \cdots \cdot a) &= 1 \\ \chi(a) \cdot \chi(a) \cdot \cdots \cdot \chi(a) &= 1 \\ \chi(a)^{\phi(n)} &= 1 \\ \chi(a) &= \sqrt[\phi(n)]{1}. \end{aligned}$$

That last line says that χ maps arbitrary element a to a $\phi(n)^{th}$ root of 1. $\square$

One way to define a Dirichlet character is to let $\chi(a) = 1$ for every a such that $\gcd(a, n) = 1$. This way, $\chi(a)$ always maps to a root of 1. We call this the *trivial character*.

Another typical Dirichlet character is the Legendre symbol. Let $a \in \mathbb{Z}/p\mathbb{Z}$. We define the Legendre symbol via

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \equiv 1 \mod 4, \\ -1 & \text{if } a \equiv 3 \mod 4. \end{cases}$$

Since we are not diving too deeply into Dirichlet characters, we can imagine them sending every input to either 1 or −1, like the Legendre symbol does.

5.2 p-adic L-functions

Dirichlet characters play a central role in L-functions. Essentially, χ takes the place of 1 since it already maps inputs to the roots of 1.

Definition 5.2.1 (Dirichlet L-function)**.** *The Dirichlet L-function for Dirichlet character χ mod n and for $Re(s) > 1$ is*

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

Its Euler product form is

$$L(s, \chi) = \prod_{\text{prime } p}^{\infty} \frac{1}{1 - \chi(p)p^{-s}}.$$

Like the Riemann zeta function, L-functions have continuations to the rest of the complex plane, and they have poles at $s = 1$.

While we are generalizing things, we may as well introduce the generalized Bernoulli numbers, written $B_{k,\chi}$. They require concepts far more sophisticated than what we can discuss here. For more information, and for a proof of the following equation, consult Ireland and Rosen (1990: p.264).

For positive integer k,

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

Look familiar?

There is a p-adic interpolation of L-functions, of which the p-adic Riemann zeta is a special case. In the p-adics, we use a specific Dirichlet character called the *Teichmüller character*, denoted ω.

Definition 5.2.2 (Kubota-Leopoldt p-adic L-function)**.** *For positive integer k and p-adic integer s, there exists a meromorphic function $L_p(s, \chi)$ such that*

$$L_p(1 - k, \chi) = L(1 - k, \chi\omega^{-k}).$$

Additionally, if p is odd,

$$L_p(1 - k, \chi) = -\frac{B_{k,\chi}}{k}.$$

The explicit integral version of L_p is rather complicated, but it too bears resemblance to the Kubota-Leopoldt zeta function. More information can be found in Jacinto and Williams (2017).

Certain inputs of various L-functions, including p-adic ones, reveal information about arithmetic sequences, elliptic curves, and more.

To learn about L-functions in general, try Davenport (1982), which discusses arithmetic progressions of prime numbers, Siegel's theorem, and Dedekind zeta functions.

Elliptic curves and their relations to L-functions culminate in the Birch and Swinnerton-Dyer conjecture, one of the Millenium problems from the Clay Institute of Mathematics. These problems are famously unsolved, and whoever proves or disproves one will win a million dollars. A write-up on the Birch and Swinnerton-Dyer conjecture can be found in Wiles (2006).

For a slightly different path, try cyclotomic fields. The Dirichlet character mapped elements to various roots of 1. The study of these roots of unity, as they are called, proves to be a rich one. A popular avenue of research in modern number theory is cyclotomic fields, which are the rational numbers adjoined with certain roots of unity. More information can be found in Washington (1997).

Cyclotomic fields and p-adic L-functions are united by Iwasawa theory, an area of number theory which requires many prerequisites. Iwasawa theory is based around the publications of Kenkichi Iwasawa in the 1950s. Much of the background knowledge required can be found in Cassels and Fröhlich (1986) including class number theory, cohomologies, and Galois groups. The foundational, and more advanced, work of Iwasawa Theory is Iwasawa (1973).

One step more abstract is the Langlands program, an overarching summary of modern number theory which combines many different regions of study via L-functions. The Langlands program is considered ill-understood by many modern mathematicians, but it is a popular topic of research. Look at Bump et al. (2003) for further information.

The L-functions of Langlands or Birch and Swinnerton-Dyer are abstract and notation-heavy, requiring years of research to understand. Yet they are not so far removed from the p-adic Riemann zeta function. The beauty of analytic number theory is how it builds on itself in a million different ways. There are countless directions to go in, many of which are still unknown, unexplored, unimagined.

Bibliography

Apostol, Tom M. 1998. *Introduction to Analytic Number Theory*. Springer-Verlag.

Bowers, A. 2004. p-adic measures and bernoulli numbers.

Bump, Daniel, E de Shalit, SS Kudla, E Kowalski, D Gaitsgory, and JW Cogdell. 2003. *An Introduction to the Langlands Program*, vol. 140. Springer Science & Business Media.

Cassels, John William Scott, and Albrecht Fröhlich. 1986. *Algebraic Number Theory*. London Mathematical Society London.

Davenport, Harold. 1982. *Multiplicative Number Theory*, vol. 74. Springer Science & Business Media.

Gouvêa, Fernando Q. 1997. *p-adic Numbers: An Introduction*. Springer.

Ireland, Kenneth, and Michael Rosen. 1990. *A Classical Introduction to Modern Number Theory. 1990*, vol. 16. Springer.

Iwasawa, Kenkichi. 1973. On zl-extensions of algebraic number fields. *Annals of Mathematics* 246–326.

Jacinto, Joaquín Rodrigues, and Chris Williams. 2017. An introduction to p-adic l-functions. *Lecture Notes* .

Koblitz, Neal. 1984. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. New York: Springer-Verlag.

O'Connor, J., and E. Robertson. 1997. Takakazu shinsuke seki biography.

Rudin, Walter. 1976. *Principles of Mathematical Analysis*, vol. 3. McGraw-Hill New York.

Washington, Lawrence C. 1997. *Introduction to Cyclotomic Fields*, vol. 83. Springer Science & Business Media.

Wiles, Andrew. 2006. The birch swinnerton-dyer conjecture. In *The Millennium Prize Problems*, eds. James A Carlson, Arthur Jaffe, and Andrew Wiles, 29–41. Clay Mathematics Institute, American Mathematical Society.