An Overview of p-adic Numbers, Analysis, and ζ-function

Aathreya Kadambi

April 2023

Contents

1 Introduction: p-adic Numbers

Before we start, I will mention that this presentation will be based on Professor Neal Koblitz's books on the subject. Here is a brief history of p-adic analysis given by him in his book:

Kummer and Hensel	1850-1900	Introduced p-adic numbers and developed basic properties
Minkowski	1884	Proved that an equation $a_1x_1^2 + \ldots + a_nx_n^2 = 0$ is solvable in the rational numbers if and only if it is solvable in the reals and in the p-adic numbers for all primes p
Tate	1950	Fourier analysis on p-adic groups; pointed toward interrelations between p-adic numbers and L-functions and representation theory
Dwork	1960	Used p-adic analysis to prove the rationality of the ζ-function of an algebraic variety defined over a finite field, part of teh Weil conjectures
Kummer	1851	Congruences for Bernoulli numbers
Kubota-Leapoldt	1964	Interpretation of Kummer congruences for Berknoulli numbers using p-adic zeta-function
Iwasawa, Serre, Mazur, Manin, Katz, others	1960s-1980s	p-adic theories for many arithmetically interesting functions

We start by introducing the p-adic numbers. To do this, we need a few definitions.

Definition (Metric). Let X be a nonempty set. A distance or **metric** on X is a function $d : X \times X \to \mathbb{R}_{\geq 0}$ such that

1. $d(x, y) = 0$ if and only if $x = y$.
2. $d(x, y) = d(y, x)$.
3. $d(x, y) \leq d(x, z) + d(z, y)$ for all $z \in X$.

Definition (Metric Space). A set X and a metric d together are called a **metric space**.

Generally, we work with X being a field, and our metrics will come from norms on the field, defined as follows:

Definition (Norm). A **norm** on a field F is a map, denoted $|\ |$, from F to $\mathbb{R}_{\geq 0}$ such that

1. $|x| = 0$ if and only if $x = 0$.
2. $|x \cdot y| = |x| \cdot |y|$.

3. $|x + y| \leq |x| + |y|$.

Definition (v_p, ord$_p$). Let p be any prime number. For any nonzero integer a, let $v_p(a)$ be the largest power of p which divides a.

Definition (p-adic Norm). Define the map $| \, |_p$ on $\mathbb{Q}$ as:

$$|x|_p = \begin{cases} \frac{1}{p^{v_p(x)}} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

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

Proof by checking the three properties.

We now classify norms:

Definition (Non-Archimedian Norms/Metrics). A norm is called **non-Archimedian** if $|x + y| \leq \max(|x|, |y|)$ always holds. A metric is called **non-Archimedian** if $d(x, y) \leq \max(d(x, z), d(z, y))$.

We call norms and metrics that are not non-Archimedian as Archimedean. We can easily verify that $| \, |_p$ is a non-Archimedian norm on $\mathbb{Q}$.

Definition (Cauchy Sequence). In a metric space X, a **Cauchy sequence** $(a_k)_{k \in \mathbb{N}}$ of elements in X is a sequence such that for all $\epsilon > 0$, there exists N such that $d(a_m, a_n) < \epsilon$ whenever $m, n > N$.

Definition (Equivalence of Norms/Metrics). Two metrics d_1 and d_2 are **equivalent** if a sequence is Cauchy with respect to d_1 if and only if it is Cauchy with respect to d_2. Two norms are **equivalent** if their corresponding metrics are equivalent.

Theorem (Ostrowski's Theorem). Every nontrivial norm $| \, |$ on $\mathbb{Q}$ is equivalent to $| \, |_p$ for some prime p or for $p = \infty$.

Remark. Here $| \, |_\infty$ denotes the regular absolute value. A trivial norm is a norm $| \, |$ such that $|0| = 0$ and $|x| = 1$ for $x \neq 0$.

Here is one more important theorem:

Theorem. In a metric space with a non-Archimedian metric, a sequence is Cauchy if ando nly if the difference between adjacent terms approaches zero, and as a corollary if the metric space is also complete, an infinite sum converges if and only if its general term approaches zero.

Now, let us take a look at how we will build up complex numbers from this new metric.

- Obtain $\mathbb{Q}_p$, the p-adic completion of $\mathbb{Q}$, which we get by considering Cauchy sequences of rational numbers.
- Perform an infinite sequence of field extensions to join solutions to higher degree polynomial equations, resulting in an algebraically closed field $\overline{\mathbb{Q}}_p$.
- Unfortunately this is not complete, so we complete again to get Ω.

After performing the first step, the following theorem gives us a good feel for $\mathbb{Q}_p$:

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

1. $0 \leq a_i < p^i$ for $i = 1, 2, 3, \ldots$.
2. $a_i \equiv a_{i+1} \pmod{p^i}$ for $i = 1, 2, 3, \ldots$.

We can extend this idea to all $a \in \mathbb{Q}_p$ by first multiplying a by p^m to get a p-adic number $a' = ap^m$ satisfying $|a'|_p \leq 1$. We then get the following representation for elements of $\mathbb{Q}_p$:

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \ldots + \frac{b_{m-1}}{p} + b_m + b_{m+1}p + b_{m+2}p^2 + \ldots$$

Definition (p-adic Integers). We define $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \le 1\}$ to be the **p-adic integers**.

2 Analysis of Ω

Rather than show how Ω is constructed, for the purposes of this analysis course, it is more interesting to proceed with some analysis of Ω. We start with power series. Analogously to Hadamard's formula, we define the radius of convergence of a power series as follows:

Definition (Radius of Convergence). Consider the expression

$$f(X) = \sum_{n=0}^{\infty} a_n X^n$$

where $a_n \in \Omega$ for each n. When $|a_n x^n|_p \to 0$, we can give $f(x)$ the value $\sum_{n=0}^{\infty} a_n x^n$. The **radius of convergence** defined as

$$\frac{1}{R} = \limsup |a_n|_p^{1/n}.$$

It can then be shown that the series converges if $|x|_p < R$ and diverges when $|x|_p > R$.

Theorem. If $|x|_p < R$, f converges at x. If $|x|_p > R$, f diverges at x.

Proof.

Consider $|x|_p = (1-\epsilon)R$ for $\epsilon > 0$. Then $|a_n x^n|_p = (|a_n|_p^{1/n})^n (R(1-\epsilon))^n$, and since there are only finitely many n such that $|a_n|_p^{1/n} > \dfrac{1}{R - \frac{1}{2}\epsilon R}$,

$$\lim_{n\to\infty} |a_n x^n|_p \le \lim_{n\to\infty} \left(\frac{(1-\epsilon)R}{(1-\frac{1}{2}\epsilon)R} \right)^n = 0$$

Similarly, we can show that when $|x|_p > R$, this limit is not zero. ■

Definition (Closed Disc). The **closed disc** of radius $r \in \mathbb{R}$ about $a \in \Omega$ is

$$\overline{D}_a(r) := \{x \in \Omega : |x-a|_p \le r\}$$

Definition (Open Disc). The **open disc** of radius $r \in R$ about $a \in \Omega$ is

$$D_a(r) := \{x \in \Omega : |x-a|_p < r\}$$

We also denote $\overline{D}(r) := \overline{D}_0(r)$ and $D(r) := D_0(r)$.

Remark. $\overline{D}_a(r)$ and $D_a(r)$ are both simultaneously closed and open, so the above definitions are a bit questionable topologically. We ware working in a "totally disconnected topological space".

Here are some quick Lemmas that I will not show here:

Lemma. Every $f(X)$ with p-adic integer coefficients converges in $D(1)$.

Lemma. Every $f(X)$ which converges in a disc $D = D(r)$ or $\overline{D}(r)$ is continuous on D.

Remark. As an interesting warning, it is important to note that series of rational numbers may not converge to the same rational number with respect to $|\ |_p$ and $|\ |_\infty$.

Definition (Differentiable). A function $f : \Omega \to \Omega$ is **differentiable** at $a \in \Omega$ if $\dfrac{f(x) - f(a)}{x - a}$ approaches a limit in Ω as $|x-a|_p \to 0$.

Definition (Locally Analytic). If a function can be represented by a convergent power series in a neighborhood of any point in its region of definition, we say that it is **locally analytic**.

Theorem. If $f(X) = \sum_{n=0}^{\infty} a_n X^n$ is a power series, then it is differentiable at every point in its disc of convergence, and it can be differentiated term by term. In particular, its derivative at a point a in the disc of convergence is

$$\sum_{n=1}^{\infty} n a_n a^{n-1}$$

Remark. There is a theory of integration on Ω, but I won't discuss that today.

3 p-adic Distributions and The p-adic ζ Function

Before we consider the p-adic ζ Function, we have the following theorem:

Theorem.

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

where B_{2k} is the Bernoulli number.

This theorem motivates the study of the $-\frac{B_{2k}}{2k}$ term. We again start with some definitions.

Definition (Interval). A set of the form $a + p^N\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x-a|_p \leq (\frac{1}{p^N})\}$ (denoted $a + (p^N)$) for $a \in \mathbb{Q}_p$ and $N \in \mathbb{Z}$ is called an **interval**.

Definition (Locally Constant). Let X And Y be two topological spaces. A map $f : X \to Y$ is called **locally constant** if every point $x \in X$ has a neighborhood U such that $f(U)$ is a single element of Y.

Definition 1 (p-adic Distribution). A **p-adic distribution** μ is a $\mathbb{Q}_p$ linear map from the $\mathbb{Q}_p$ vector space of locally constant functions on X to $\mathbb{Q}_p$. We denote $\mu(f)$ as $\int f\mu$.

Definition 2 (p-adic Distribution). A **p-adic distribution** μ on X is an additive map from the set of compact open sets in X to $\mathbb{Q}_p$. In other words, if $U \subseteq X$ is the disjoint union of compact open sets $U_1, U_2, \ldots, U_n$, then

$$\mu(U) = \mu(U_1) + \ldots + \mu(U_n).$$

Proposition. Every map μ from the set of intervals contained in X to $\mathbb{Q}_p$ for which $\mu(a + (p^N)) = \sum_{b=0}^{p-1} \mu(a + bp^N + (p^{N+1}))$ whenever $a + (p^N) \subseteq X$ extends uniquely to a p-adic distribution on X.

We will now take a look at the Bernoulli Distributions.

Definitions (Bernoulli Polynomials $B_k(x)$). Consider

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

Collecting the terms for t^k, for each k we obtain a polynomial in x. $B_k(x)$ the **Bernoulli polynomial** is defined to be $k!$ times this polynomial.

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

Using the previous proposition,

Proposition. $\mu_{B,k}$ extends to a distribution on $\mathbb{Z}_p$ called the "k^{th}" Bernoulli distribution.

Example. The first few Bernoulli distributions are

$$\mu_{B,0}(a+(p^N)) = p^{-N}$$

which is called the **Haar distribution**,

$$\mu_{B,1}(a+(p^N)) = B_1(\frac{a}{p^N}) = \frac{a}{p^N} - \frac{1}{2}$$

which is called the **Mazur distribution**, and

$$\mu_{B,2}(a+(p^N)) = p^N(\frac{a^2}{p^{2N}} - \frac{a}{p^N} + \frac{1}{6})$$

Now a full consideration of this subject would take far too long, so I will simply summarize various pieces.

Definition (Measure). A p-adic distribution μ on X is a **measure** if its value on compact open $U \subseteq X$ are bounded by some constant $B \in \mathbb{R}$.

To make the Bernoulli distributions measures, we perform a process called regularization and define:

Definition (Regularized Bernoulli Distribution). Denoted by $\mu_{k,\alpha}$ or $\mu_{B,k,\alpha}$,

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

Definition (p-adic ζ Function). If k is a positive integer,

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

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

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

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