P-adic Numbers

Kevin Guillen
Department of Mathematics
University of California at Santa Cruz
Santa Cruz, CA 95064 USA

February 27, 2022

Abstract

This paper will begin by introducing some of the prerequisite knowledge needed to begin defining p-adic numbers and their applications. Then give a brief history of p-adic numbers to then explain how one goes from the rationals to p-adic numbers. Then to highlight the differences from the real numbers. Then take an algebraic look through $\mathbb{Q}_p$ and what it means to be a completion of the rationals, and definitions and examples of p-adic analysis

1 Introduction

The real numbers are a number system we should all be familiar with, since it is what appears most natural in our day to day lives. For one to construct the reals from the rationals though, it turns out to be difficult due to one needing more machinery than when going from the natural numbers $\mathbb{N}$, to the integers $\mathbb{Z}$ and finally to the rationals $\mathbb{Q}$. In these two "jumps" one simply needed to introduce one more algebraic operation to get the next. For example one got the integers from the natural numbers through the introduction of subtraction, and the rationals from the integers through the introduction of division. The new machinery one needed to jump from the discrete $\mathbb{Q}$ to the continuous $\mathbb{R}$ was the introduction of a limit [4] . The standard definition of a limit in the real numbers depends on the standard notion of distance, the Euclidean absolute value, which is a *metric* or a *distance function*[5]. That's the key though, the Euclidean absolute value is *a* metric, so while this paper is not on measure theory, this will be important for what comes next. We know that $\mathbb{Q}$ was a field and through the Euclidean absolute value we were able to obtain the reals, which now leads us to define the general notion of absolute value for an arbitrary field $\mathbb{F}$.

Definition 1.1 (Absolute Value)**.** An **absolute value** on a field $\mathbb{F}$ is a function $|\cdot|$ from $\mathbb{F}$ to $\mathbb{R}_{\geqslant 0}$ that satisfies the following properties for all $a, b \in \mathbb{F}$:

(1) Positive-definiteness: $|a| = 0 \iff a = 0$

(2) Multiplicativity: $|ab| = |a|\,|b|$

(3) Triangle Inequality: $|a + b| \leqslant |a| + |y|$

and if an absolute value satisfies,

(4) Strong Triangle Inequality: $|a + b| \leqslant \max\{|a|, |b|\}$

it is called *non-Archimedean*.

We also define a metric as follows,

Definition 1.2 (Metric)**.** A **metric** on $\mathbb{F}$ is defined by a distance function $d : \mathbb{F} \times \mathbb{F} \to \mathbb{R}_{\leqslant 0}$. We see then that an absolute value induces a metric by,

$$d(a, b) = |a - b|$$

for all $a, b \in \mathbb{F}$ A set where a metric is defined is called a *metric space*, and a set with a metric is induced by a non-Archimedean absolute value is called a *ultrametric space*

We see then that $(\mathbb{R}, d)$ where d is the usual Euclidean absolute value, we have a metric space that we all naturally know.

What was the point of all this, why did we review these definitions and constructions? Well, there is a different number system one can obtain from the rationals that is just as, if not more, fascinating than the reals, and that is the *p-adic* number system.

Definition 1.3 (p-adic integer)**.** Let $p \in \mathbb{Z}$ be a prime number. Then a **p-integer** x is the base p expansion of some integer $a \in \mathbb{Z}$, that is,

$$a = a_1 p^0 + a_2 p^1 + \cdots + a_n p^n \qquad a_1, a_2, \ldots a_n \in \mathbb{Z}/p\mathbb{Z}$$
$$x = a_1 a_2 \ldots a_n$$

where we will define p-adic integers to be "closer" to one another based on how many powers of p we can fit into their difference. This number system, even though unnatural, will prove to be a useful toolset and yield a number of fascinating and unintuitive results. We will touch on many familiar topics relating to the reals, and how those topics look like in this number system. We stop here since it will be good to see why how anyone would think of a number system and see the motivation behind its discovery.

2 Hensel's Analogy

This definition/construction of $p-$adic numbers may seem a bit aimless and random, but once we see what was going through the mind of Hensel, we will see that this number system is indeed well motivated and natural.

Kurt Hensel (29 December 1861 - 1 June 1941) was a German mathematician born in Konigsberg, who studied under Leopold Kronecker and Karl Weierstrass. At the time Hensel was interested in the analogy between,

$$\mathbb{Z} \text{ with its fraction field } \mathbb{Q} \longleftrightarrow \mathbb{C}[X] \text{ with its fraction field } \mathbb{C}(X).$$

Hensel learned of this analogy from his doctoral advisor Kronecker, who believed there could be a single theory covering both of them. Kronecker never was able to create this theory, but Hensel was very interested in this analogy between the two [1].

We can see how this interest through the following explanations. Taking a function $f(X)$ from $\mathbb{C}(X)$ we know it is a rational function or in other words the quotient of two functions,

$$f(X) = \frac{P(X)}{Q(X)},\ P(X), Q(X) \in \mathbb{C}[X].$$

Taking a rational number x from $\mathbb{Q}$ we know that it is rational, as the name suggests, more specifically a quotient of two integers,

$$x = \frac{p}{q},\ p, q \in \mathbb{Z}.$$

The next parallel is that we know both the rings $\mathbb{Z}$ and $\mathbb{C}[X]$ are unique factorization domains, meaning every non-zero non-unit element in them can be written uniquely as a product of prime elements in the ring (up order and units). More explicitly for $x \in \mathbb{Z}$ non-zero and not ± 1 we can express it uniquely for $n \in \mathbb{N}$ as,

$$x = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n},\ p_1 \dots p_n \text{ are prime integers},\ e_1 \dots e_n \in \mathbb{N}$$

And for $P(X) \in \mathbb{C}[X]$ where $P(X)$ is non-zero and not a unit, we can express it uniquely, for some $n \in \mathbb{N}$, as,

$$P(X) = a(X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_n),\ a, \alpha_1 \dots \alpha_n \in \mathbb{C}.$$

From here one might be able to see what the point of Hensel's analogy was. It's that primes,p, in $\mathbb{Z}$ are analogous to linear polynomials, $(X-\alpha)$, in $\mathbb{C}[X]$

Extending this into solutions for equations. If we take a polynomial with integer coefficients, we call its roots *algebraic numbers*. Now something similar is said when we take a polynomial with coefficients in $\mathbb{C}[X]$, its roots will be called *algebraic functions*.

Example: Consider the polynomial $Y^2 - 2$, we know $\sqrt{2}$ is a root of it, and therefore $\sqrt{2}$ is an algebraic number.

Now for the polynomial with coefficients in $\mathbb{C}[X]$, $Y^2 - (X^3 - 3X - 1)$ the function $\sqrt{X^3 - 3X - 1}$ is a root of it, and therefore and algebraic function.

Going back to Hensel's analogy now, Hensel was working on a specific problem about algebraic numbers, so he considered the analogous problem in terms of algebraic functions. This problem that Hensel was working on turned out to be relatively easy to solve under algebraic functions by expanding functions into its power series [1]. Explicitly this means, given $P(X) \in \mathbb{C}[X]$ and $\alpha \in \mathbb{C}$ we have the following,

$$\begin{aligned} P(X) &= a_0 + a_1(X-\alpha)^1 + a_2(X-\alpha)^2 + \cdots + a_n(X-\alpha)^n \\ &= \sum_{i=o}^{n} a_i(X-\alpha)^i. \end{aligned}$$

Which gives us information of how $P(X)$ behaves around α. Now if only we had this sort of expansion for integers. In a way we do though! Consider the number 245, we can expand it out as follows,

$$245 = 5 \cdot 10^0 + 4 \cdot 10^1 + 2 \cdot 10^2$$

which is nothing new, we do it all the time we just stop thinking about it. The issue for Hensel though was that 10 is not a prime in $\mathbb{Z}$ while $(X-\alpha)$ is a prime in $\mathbb{C}[X]$. Knowing the definition of $p-$adic numbers we know what comes next. Hensel considered taking a base 10 integer and expressing it a number in base p. So we see our 245 becomes,

$$\begin{aligned} 245 &= 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 + 0 \cdot 2^6 + 1 \cdot 2^7 \\ &= 11110101_2 \end{aligned}$$

which we see is analogous to the power series for functions since 2 is a prime element in $\mathbb{Z}$

3 Properties of p-adic numbers

Now that we see how Hensel arrived at p-adic numbers let us expand on some of the definitions given during the introduction and dive deeper into the world of $p-$adic numbers

4 $\mathbb{Q}_p$, completion of $\mathbb{Q}$

Go over some algebra examples, to ultimately construct the p-adic field $\mathbb{Q}_p$. Explore $\mathbb{Q}_p$, talk about the ring of p-adic integers, density, and Hensel's Lemma.

5 Elementary analysis with $\mathbb{Q}_p$

Normal analysis topics like Sequences and Series, Integrals, and Power Series. (Need to read more)

References

[1] Fernando Gouvea (2003) *p-adic Numbers: An Introduction*, Springer Science & Business Media, 2003.

[2] Alain M. Robert (2000) *A Course in p-adic Analysis*, Springer; 2000th edition

[3] Svetlana Katok (2007) *P-adic Analysis Compared With Real (Student Mathematical Library)*, American Mathematical Society

[4] Terence Tao (2016) *Analysis I: Third Edition*, Hindustan Book Agency, 1st ed. 2016 edition

[5] James Munkres (2000) *Topology*, Pearson College Div; 2nd edition (January 7, 2000)