P-adic Numbers

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

March 15, 2022

Abstract

This paper will begin by introducing some of the prerequisite knowledge and definitions needed to define p$-$adic numbers and their applications. This will be done by building them alongside the reals and providing the needed history. The main focus though is to give the motivation for their discovery, the intuition behind them, and proving Ostrowksi's theorem to enforce their importance. Exploring the definition of completion and the ring of p-adic integers. Finally exploring some unnatural properties of them.

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,

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

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. We know from previously that we can simply take a base 10 integer and express it in base p, where p is a prime number, and have its p-adic equivalent, but the p-adic numbers are supposed to be an extension of the rational numbers so let us consider a rational number x. We know that it is of the form $\frac{a}{b}$. To follow from the work of the previous section let $a = 245$ with $b = 4$ and lets work in the 2-adic system. We know from perviously that 245 is 11110101_2 and we see that

$$\begin{aligned} \frac{245}{4} &= 1 \cdot 2^{-2} + 0 \cdot 2^{-1} + 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 \\ &= 111101.01_2 \end{aligned}$$

where the decimal behaves as normally in base 10. Technically there wasn't much if any calculations needed here since just like in base 10 when we are dividing by a power of p

we simply "move" the decimal point to the left based on what power of p we are dividing by. In this case $4 = 2^2$. So in a sense this was trivial, but let us ease into some not as nice fractions. let us consider $\frac{1}{2}$ in the $5-$adic system. We get,

$$\frac{1}{2} = 5 \cdot \frac{-1}{2} + 3$$

this tells us that 3 will be the last digit and we know it to be unique since 5 is prime. Continuing this division with remainder we get,

$$\begin{aligned} \frac{-1}{2} &= 5 \cdot \frac{-1}{2} + 2 \\ \frac{-1}{2} &= 5 \cdot \frac{-1}{2} + 2 \\ &\vdots \end{aligned}$$

and we see this process just repeats meaning $\frac{1}{2}$ in the $5-$adic system will simply be $\ldots 223_5 = \bar{2}3_5$. This is the general idea of how to obtain the $p-$adic expansion of a rational number (note that the for an integer the $p - adic$ expansion is simply its expression in base p). There is a lot being tucked under the rug here, but in order to have time to talk about more advanced topics we will be omitting some little details. We see then that any rational number can expressed in the form,

$$x = \frac{a}{b} = \sum_{n \geqslant n_0} a_n p^n$$

where $n_0 \geqslant 0$ if and only if $p \nmid b$ and $n_0 > 0$ if and only if $p \nmid b$ AND $p \nmid a$ where we assume $\frac{a}{b}$ is in its lowest terms.

Now let us return a bit to Hensel's Analogy, we see that for every rational number when converted to its $p-$adic expansion we will have finitely many negative powers of p. This is called a "finite-tailed Laurent series in p".[1] Which is referencing the expansion is finite to the left (or finite to the right once we write it out in the specified base). Now we know that $\mathbb{C}((X - \alpha))$ is a field, will the set of all finite tailed Laurent series in powers of p be a field? The answer is yes! This field is actually refered to as $\mathbb{Q}_p$ which is said as the field of $p-$adic numbers. Now that we got some basic concepts down we can actually dive into one of the problems that $p-$adic numbers are closely related to.

3.1 Solving Congruences Modulo p^n

Problems of these kind are common in a field like Number Theory, so to begin this let us consider an equation that has solutions in $\mathbb{Q}$,

$$X^2 = 16.$$

Which has solutions $x = \pm 4$. Now we want to consider it modulo p^n and $\forall n \in \mathbb{N}$, in order to solve congruences like,

$$X^2 \equiv 16 \bmod p^n$$

and for the integers we know that $X = \pm 4$ gives solutions of the congruence for every n. Want we want to do is consider it from a $p-$adic point of view. Let us consider specifically the $3-$adic system. Recall this means we will be writing with class representatives between 0 and $3^n - 1$ for solutions modulo 3^n. So first let us look at $X = 4$ we have,

$$\begin{aligned} X &\equiv 4 \equiv 1 \bmod 3^1 \\ X &\equiv 4 = 1 + 1 \cdot 3^1 \bmod 3^2 = 9 \\ X &\equiv 4 = 1 + 1 \cdot 3^1 \bmod 3^3 = 27 \\ &\vdots \end{aligned}$$

which we see will continue on for the rest of the powers of 3, giving the $3-$adic expansion of the solution as,

$$4 = 1 \cdot 3^0 + 1 \cdot 3^1 = 11_3$$

let us consider the more interesting solution though, $X = -4$ we see that,

$$\begin{aligned} X &\equiv -4 \equiv 2 = 2_3 \bmod 3 \\ X &\equiv -4 \equiv 5 = 2 + 1 \cdot 3^1 = 12_3 \bmod 9 \\ X &\equiv -4 \equiv 23 = 2 + 1 \cdot 3^1 + 2 \cdot 3^2 = 212_3 \bmod 27 \\ X &\equiv -4 \equiv 77 = 2 + 1 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 = 2212_3 \bmod 81 \\ &\vdots \end{aligned}$$

continuing this as before gives the $3-$adic expansion of the solution which we see to be infinite!

$$X = -4 = 2 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots = \ldots 2212_3 = \bar{2}12_3$$

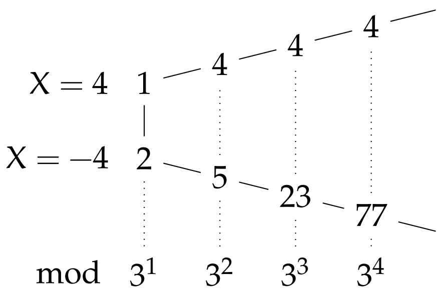
We see that the solutions for the congruencies are "coherent" meaning if we take the solution for 3^4 which was $X = 77$ and reduce it modulo 3^3 we get $X = 23$, which is the corresponding solution for 3^3, which leads to a definition.

Definition 3.1. *(**Coherent**) Let p be a prime integer. A sequence of integers α_n such that $0 \leqslant \alpha_n \leqslant p^n - 1$ is **coherent** if for every $n \geqslant 1$ it satisfies,*

$$\alpha_{n+1} \equiv \alpha_n \bmod p^n$$

*in the case where p must be specified, the sequence will be called p**-adically coherent**.* [1]

When we have a **coherent** sequence of integers we can visualize the solutions as a branch, let us consider specifically the solutions we worked out above $X = \pm 4$.



Anyone familiar with congruencies would know this was already obvious for these solutions since they are actually solutions in $\mathbb{Z}$, what is new is the connection between expressing the roots as coherent sequences containing their $p-$adic expansions.

To make it more interesting let us consider an equation that doesn't have solutions in $\mathbb{Q}$, a notable one to consider is,

$$X^2 = 2.$$

Let us look at this under the $7-$adic lens,

$$X^2 \equiv 2 \bmod 7$$

we obtain two solutions:

$$X \equiv 3 \bmod 7 \qquad\qquad X \equiv 4 \equiv -3 \bmod 7.$$

Now let us continue like before and find solutions for $n = 2$ or in other words

$$X^2 \equiv 2 \bmod 49$$

recall though to be **coherent**, these solutions reduced modulo 7 must also be solutions for $n = 1$. This gives us the requirements,

$$X = 3 + 7k \qquad\qquad X = 4 + 7k$$

so let us begin solving for the first solution, plugging it in gives us,

$$\begin{aligned} (3+7k)^2 &\equiv 2 \bmod 49 \\ 9 + 42k &\equiv 2 \bmod 49 \\ 7(1+6k) = 7 + 42k &\equiv 0 \bmod 49 \\ 1 + 6k &\equiv 0 \bmod 7 \\ k &\equiv 1 \bmod 7. \end{aligned}$$

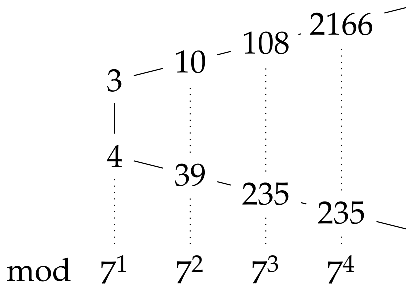
By definition this gives us then that, $k = 7m + 1$ where $m \in \mathbb{Z}$. Plugging this back into X gives us that $X = 10 + 49m$, meaning this solution for $n = 2$ is,

$$X \equiv 10 \bmod 49.$$

Similarly we obtain the second solution in the same fashion which works out to be,

$$X \equiv 39 \equiv -10 \bmod 49.$$

From here one repeat these steps for $n = 3, 4, 5\ldots$ to then create the branches that we saw before. It should be noted though that this is not a way to predict numbers will appear in the branch, but what this repetition does tell us though is that we can find two coherent sequences of solutions. [1]



Which gives us the sequence of integers,

$$\begin{aligned} \alpha_1 &= (3, 10, 108, 2166, \ldots) \\ \alpha_2 &= (4, 39, 235, 235, \ldots) \end{aligned}$$

as our solutions, and now repeating what we did previous we can obtain the 7−adic expansion of the solution,

$$\begin{aligned} 3 &= 3 = 3_7 \\ 10 &= 3 + 1 \cdot 7^1 = 13_7 \\ 108 &= 3 + 1 \cdot 7^1 + 2 \cdot 7^2 = 213_7 \\ 2166 &= 3 + 1 \cdot 7^1 + 2 \cdot 7^2 + 6 \cdot 7^3 = 6213_7 \end{aligned}$$

meaning the 7−adic solutions are simply,

$$\begin{aligned} \alpha_1 &= \ldots 6213_7 \\ \alpha_2 &= \ldots 0454_7. \end{aligned}$$

So we could continue this methodology infinitely to keep obtaining the rest of the solution, since we can't predict what the rest of the solution will look like with what we have currently. Think of this similar to how we can work out the decimal expansion of the square root of 2 in $\mathbb{R}$ and get as close as we'd like, but we can't predict what the expansion will look like. [3] Finally these two 7−adic numbers are the roots of the equation $X^2 = 2$ in the field of 7−adic numbers, $\mathbb{Q}_7$. These sequences of congruences modulo higher and higher powers of p and solving the corresponding equation in $\mathbb{Q}_p$ are of the important reasons for using p−adic methods in Number Theory. [1] This leads beautifully into the next important topic pertaining to p−adic numbers and that is completion, which is why we chose the example of $X^2 = 2$.

4 Completing $\mathbb{Q}$

Let us bring in some of the definitions defined in the introduction. One might have picked up why they were defined, since they in a way served as a spoiler for what is to come especially after showing some properties of the $p-$adics. First we will bring in a few other definitions.

Definition 4.1. *(**Cauchy Sequence** [4]) A sequence (x_n) is a **Cauchy** if $\forall \varepsilon > 0$ there exists some $N \in \mathbb{N}$ such that for all $n, m > N$ it satisfies,*

$$|x_n - x_m| < \varepsilon.$$

When a sequence is Cauchy, all it is really saying about the sequence is that the terms in the sequence become arbitrarily close to one another and in a sense "settle" on something. Which is why the convergence of a sequence implies it is Cauchy. [4]

Definition 4.2. *(**Complete**) A metric space is called **complete** if every Cauchy sequence composed of elements in the metric space converges within the metric space. Such a metric space is also referred to as a **Cauchy Space**.* [5]

Remark. The field $\mathbb{Q}$ is NOT complete. Recall we simply have to show an example of one Cauchy sequence composed of rational numbers that converges to something not in $\mathbb{Q}$. One example would be,

$$x_n = \left(1 + \frac{1}{n}\right)^n$$

which one can prove is convergent to e, therefore Cauchy, but $e \notin \mathbb{Q}$. This leads one to construct the reals, $\mathbb{R}$, in order to complete $\mathbb{Q}$ under the standard Euclidean absolute value.

Now we may wonder what other metrics (distance functions) we can impose on $\mathbb{Q}$ and what number systems may come from there. In fact the field of $p-$adic numbers can be analytically constructed through this. This leads to the formal construction of $\mathbb{Q}_p$, by defining the $p-$adic absolute value, but first we must define $p-$adic valuation.

Definition 4.3. *(**P-adic valuation** [1]) $P-$adic valuation is defined as the map,*

$$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

where if $x \in \mathbb{Z}$, then $v_p(x)$ is the unique positive integer satisfying,

$$x = p^{v_p(x)} x'$$

where $p \nmid x'$.

If $x \in \mathbb{Q} - \mathbb{Z}$ then x is of the form $x = \dfrac{a}{b}$ where $a, b \in \mathbb{Z}$, so $v_p(x)$ is defined to be,

$$v_p(x) = v_p(a) - v_p(b).$$

Lastly we define $v_p(0) = \infty$ (the reason will be more obvious soon).

Example. First lets cover an integer example, so let $x = 90$ and $p = 3$. The 3—adic evaluation of 90 will be 2 since,

$$90 = 3^2 \cdot 10.$$

Now consider the case $x = \frac{13}{24}$ and $p = 2$. So we have $\nu_2(13) = 0$ since we can't factor out any non-zero powers of 2, and $\nu_2(24) = 3$ since we can factor out 8. This means,

$$\nu_2\left(\frac{13}{24}\right) = \nu_2(13) - \nu_2(24) = 0 - 3 = -3.$$

With this we can now define the p—adic absolute value.

Definition 4.4. *(**P-adic absolute value** [1]) The* p*—adic absolute value is a function,*

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geqslant 0}$$

defined as,

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

where p *is a prime integer.*

Proposition 4.5. *The* p*—adic absolute value is a non-Archimedean absolute value on* $\mathbb{Q}$*.*

Proof. Let $x, y \in \mathbb{Q}$,

(1) If $|x|_p = 0$ then by definition 4.4, $x = 0$

(2) If $x = 0$ or $y = 0$ then it is obvious that $|xy|_p = |x|_p\,|y|_p$. Now in the case that $x \neq 0$ and $y \neq 0$ we have

$$|xy|_p = p^{-\nu_p(xy)} \qquad |x|_p\,|y|_p = p^{-\nu_p(x) - \nu_p(y)} \tag{1}$$

so we have to show that $\nu_p(xy) = \nu_p(x) + \nu_p(y)$.

Lemma 4.6.

$$\nu_p(xy) = \nu_p(x) + \nu_p(y)$$

Proof. Recall the definition of the p—adic valuation **Definition 4.3** and apply to it x, y individually we get,

$$x = p^{\nu_p(x)}x' \qquad y = p^{\nu_p(y)}y'$$

therefore,

$$xy = p^{\nu_p(x)}x'p^{\nu_p(y)}y' = p^{\nu_p(x)+\nu_p(y)}x'y'$$

by **Definition 4.3** $p \nmid x'$ and $p \nmid y'$, thus $p \nmid x'y'$. So we have that

$$\nu_p(xy) = \nu_p(x) + \nu_p(y)$$

since it satisfies,

$$xy = p^{\nu_p(xy)}(xy)'$$

□

Now applying **Lemma 4.6** $-\nu_p(xy) = -\nu_p(x) - \nu_p(y)$. All together then we have,

$$|xy|_p = p^{-\nu_p(xy)} = p^{-\nu_p(x)-\nu_p(y)} = |x|_p\,|y|_p$$

satisfying the multiplicativity requirement.

(3) Now to verify the triangle inequality and strong triangle inequality, if $x + y = 0$ then it is obvious that $|x + y|_p = 0$ and therefore $|x + y|_p \leqslant |x|_p + |y|_p \leqslant \max\left\{|x|_p, |y|_p\right\}$.

So let us consider the case that $x + y \neq 0$ and without loss of generality that $|x|_p > |y|_p$, and therefore $|x|_p \neq 0 \neq x$. It follows then that $\nu_p(x) \leqslant \nu_p(y)$ and by **Definition 4.4** we have,

$$|x + y|_p = p^{-\nu_p(x+y)} \qquad\qquad |x|_p = p^{-\nu_p(x)}$$

To complete this we need,

Lemma 4.7.

$$\nu_p(x + y) \geqslant \max\{\nu_p(x), \nu_p(y)\}$$

Proof. See [2] □

So applying **Lemma 4.7** we have,

$$\nu_p(x + y) \geqslant \max\{\nu_p(x), \nu_p(y)\} = \nu_p(x)$$

therefore,

$$p^{-\nu_p(x+y)} \leqslant p^{-\nu_p(x)}$$

which means then that,

$$|x + y|_p \leqslant |x|_p = \max\left\{|x|_p, |y|_p\right\}.$$

All together then we have that the p—adic absolute value is non-Archimedean on $\mathbb{Q}$. □

Let us take a pause here and answer some questions. We were able to motivate the field of p—adic numbers with Hensel's Analogy, and see why one would want such a number system. Right now though, depending on the person, one might feel this p—adic absolute value seems forced, or randomly made up. Why care about different absolute values, why not just stick to the traditional absolute value? One may also wonder if there are other absolute values we can define on $\mathbb{Q}$. This leads to a very important theorem that puts the p—adic value on the same level as the standard absolute value, and to be considered just as natural.

Theorem 4.8. *(**Ostrowski's Theorem** [1]) Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to one of the absolute values $|\cdot|_p$ where p is either a prime integer or $p = \infty$ (the absolute value of the real numbers)*

That is to say an absolute value on the rational must fall under one of these three,

$$|\cdot|_0 = \begin{cases} 0 & x = 0 \\ 1 & x =\neq 0 \end{cases}$$

$$|\cdot|_\infty = \begin{cases} x & x \geqslant 0 \\ -x & x < 0 \end{cases}$$

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

Proof. Let us consider two cases for a non-trivial absolute value, where it is Archimedean and where it is non-Archimedean.

(1) $|\cdot|$ is Archimedean. Let us consider the least positive integer x_0 such that $|x_0| > 1$, we know such an integer has to exist because if not this absolute value would be non-Archimedean. This means then that we can find an $\alpha \in \mathbb{R}$ that will satisfy the following,

$$|x_0| = x_0^\alpha.$$

Now we claim that this α will realize the equivalence between $|\cdot|$ and $|\cdot|_\infty$. So all that we have to prove now is that for every $y \in \mathbb{Q}$ we have $|y| = |y|_\infty^\alpha$, but knowing the properties of absolute values we simply have to show it for all positive integers $n \in \mathbb{Z}_+$ that $|n| = |n|_\infty^\alpha$ since the rationals will follow from that. We know the equality will hold for $x = x_0$, but to prove it in general, we can take an arbitrary integer x and write it in base x_0 so to have in the form,

$$x = a_0 + a1x_0 + a_2x_0^2 + \cdots + a_kx_0^k.$$

where we have $0 \leqslant a_i \leqslant x_0 - 1$ and $a_k \neq 0$. We see though that k is determined by $x_0 \leqslant x < x_0^{k+1}$, which says that,

$$k = \left\lfloor \frac{\log x}{\log x_0} \right\rfloor$$

Now let us take the absolute values and we get,

$$|x| = \left| a_0 + a_1x_0 + a_2x_0^2 + \ldots a_kx_0^k \right| \qquad \text{applying triangle inequality}$$
$$\leqslant |a_0| + |a_1|\, x_0^\alpha + |a_2|\, x_0^{2\alpha} + \cdots + |a_k|\, x_0^{k\alpha}$$

Now recall that x_0 is the smallest integer such that $|x_0| > 1$, we know then that $|a_i| \leqslant 1$ and we get,

$$|x| \leqslant 1 + x_0^\alpha + x_0^{2\alpha} + \cdots + x_0^{k\alpha}$$

$$
\begin{aligned}
&= x_0^{k\alpha}\left(1 + x_0^{-\alpha} + x_0^{-2\alpha} + \cdots + x_0^{-k\alpha}\right) \\
&= x_0^{k\alpha}\sum_{i=0}^{k} x_0^{-i\alpha} \\
&\leqslant x_0^{k\alpha}\sum_{i=0}^{\infty} x_0^{-i\alpha} \\
&= x_0^{k\alpha}\frac{x_0^{\alpha}}{x_0^{\alpha}-1}
\end{aligned}
$$

Now it's obvious that $\frac{x_0^{\alpha}}{x_0^{\alpha}-1}$ is positive, and so let $C = \frac{x_0^{\alpha}}{x_0^{\alpha}-1}$, so now we have,

$$|x| \leqslant Cx_0^{k\alpha} \leqslant Cx^{\alpha}.$$

This applies to every x since our choice was arbitrary, now let us apply it to an integer of the form x^N and we see we get,

$$\left|x^N\right| \leqslant Cx^{N\alpha}$$

Recall that C did not depend on the choice of x, so we can consider taking the Nth root to obtain,

$$|x| \leqslant \sqrt[N]{C} \cdot x^{\alpha}.$$

Now as $N \to \infty$ we have that $\sqrt[N]{C} \to 1$, meaning $|x| \leqslant |x|^{\alpha}$ which is part of what we want! So now we just need to show the reverse inequality, so let's consider x written in base x_0 again,

$$x = a_0 + a_1x_0 + a_2x_0^2 + \cdots + a_kx_0^k.$$

Using the fact that $x_0^{k+1} > x \geqslant x_0^k$ we get,

$$x_0^{(k+1)\alpha} = \left|x_0^{k+1}\right| = \left|x + x_0^{k+1} - x\right| \leqslant |x| + \left|x_0^{k+1} - x\right|$$

so that,

$$|x| \geqslant x_0^{(k+1)\alpha} - \left|x_0^{k+1} - x\right| \geqslant x_0^{(k+1)\alpha} - (x_0^{k+1} - x)^{\alpha}.$$

Recall though that $x \geqslant x_0^k$ so we get,

$$|x| \geqslant x_0^{(k+1)\alpha} - (x_0^{k+1} - x_0^k)^{\alpha} = x_0^{(k+1)\alpha}\left(1 - \left(1 - \frac{1}{x_0}\right)^{\alpha}\right)$$

Now similar to before let $C_1 = 1 - \left(1 - \frac{1}{x_0}\right)^{\alpha}$ which we see is not dependent on our choice of x and wil be positive. This gives us,

$$|x| \geqslant C_1x_0^{(k+1)\alpha} > C_1x^{\alpha}$$

Like before we apply the same reasoning to get the reverse inequality, and therefore have that $|x| = |x|_{\infty}^{\alpha}$. Thereby proving any Archimedean absolute value one can construct that is not the trivial one will be equivalent to $|\cdot|_{\infty}$ as desired.

(2) Now suppose we have an absolute value, $|\cdot|$ that is not Archimedean, then every integer x must have the result that $|x| \leqslant 1$. Now because $|\cdot|$ is non-trivial we have that there must be a smallest integer, x_0 such that $|x_0| < 1$. First consider the case that $x_0 = bk$ where $b, k < x_0$, then by how x_0 was defined we have that $|b| = |k| = 1$ and that $|bk| = |x_0| < 1$ which cannot be. Therefore we have that x_0 must actually be prime! So, let us use traditional notation and let $p = x_0$. Now we want to show that this absolute value is actually equivalent to the $p-$adic absolute value.

Now our goal is to show that for any integer $k \in \mathbb{Z}$ that is not divisible by p then $|k| = 1$. To do this, we know if we divide k by p then through division with remainder we have,

$$k = ap + b$$

where $0 < b < p$. Recall we defined p through x_0 and so p is minimal. Then by the minimality of p we have that $|b| = 1$, and that $|qp| < 1$, because $|a| \leqslant 1$ ($|\cdot|$ was assumed to be non-Archimedean and $|p| < 1$ through construction). Now because $|\cdot|$ is non-Archimedean we have that $|k| = 1$. Therefore given any $k \in \mathbb{Z}$, we write it as $k = p^{\nu}k'$ where $p \nmid k'$. Then we have that,

$$|k| = |p|^{\nu} \left|k'\right| = |p|^{\nu} = c^{-\nu}$$

where we have $c = |p|^{-1} > 1$. Meaning $|\cdot|$ is equivalent to the $p-$adic absolute value. Completing the proof of Ostrowski's Theorem.

□

Hopefully this shows that the $p-$dic absolute value can be considered as natural as the standard absolute value. Here is a good place to expand on the shift of notation by using $|\cdot|_{\infty}$ as the "usual" absolute value. If we think of ∞ as an infinite "prime", we can consider all absolute values on $\mathbb{Q}$ coming from a finite or an infinite prime [2].

There are many contexts in arithmetic that it is considered useful to work with "all primes". Meaning it is useful to use the information obtained from all the absolute values that arise from $\mathbb{Q}$. One can think of $|\cdot|_{\infty}$ ($\mathbb{R}$'s absolute value) as recording information relating to the sign, while other absolute values record information relating to a variety of primes [3].

Theorem 4.9. *Let $\mathbb{K}$ be a field with an absolute value $|\cdot|$. Then there exists a complete field $\mathbb{K}'$ with an absolute value $|\cdot|'$ that extends $\mathbb{K}$. The completion $\mathbb{K}'$ is unique up to isomorphism. Moreover, on $\mathbb{K}$, $|\cdot|'$ restricts to $||$, and $\mathbb{K}$ is dense in $\mathbb{K}'$.*

Proof. See [2]. □

This finally leads us to the field of $p-$adic numbers.

Definition 4.10. (***Field of** p**-adic numbers** $\mathbb{Q}_p$* [1]*) The field of $p-$adic numbers, denoted $\mathbb{Q}_p$, is defined as the completion of $\mathbb{Q}$ under the $p-$adic metric. We know this completion to exist and be unique by **Theorem 4.9**.*

Which is what we have been building towards! From here we can also define the ring of $p-$adic integers, denoted by $\mathbb{Z}_p$, but some things should be mentioned first. This construction was through an analytic lens, but the field of $p-$adic numbers can also be constructed by first algebraically constructing the ring of $p-$adic integers and then considering its fraction fraction field, which will end up being $\mathbb{Q}_p$. Similar to how we can construct $\mathbb{Q}$ from $\mathbb{Z}$.

It should also be clear that due to **Theorem 4.8** and **Theorem 4.9**, the field $\mathbb{R}$ and $\mathbb{Q}_p$ are the only completions of $\mathbb{Q}$!

4.1 Completing $\mathbb{Z}$

The title of this subsection may seem a bit strange to someone exposed to a bit of real analysis. Since any Cauchy sequence constructed by integers converges to an integer. This is because Cauchy sequences of integers are, boring. To anyone unfamiliar as to why, recall a sequence is Cauchy when the terms in the sequence become arbitrarily close to one another, but integers are at least "1 away" from one another. This means the only way to construct a Cauchy sequence of integers is to let the sequence be a constant sequence, meaning each term in the sequence is the same, making them uninteresting. Recall though we have a new metric, the $p-$adic metric, meaning we have a new notion of distance. Under the $p-$adic metric, integers can become arbitrarily close to one another!

Definition 4.11. *(Ring of $p-$adic integers $\mathbb{Z}_p$. [1]) The ring of $p-$adic integers, denoted by $\mathbb{Z}_p$, is defined as,*

$$\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p \mid |x|_p < 1 \right\}$$

Like before, $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$, this is because under our new metric we can find Cauchy sequences of integers that converge outside of $\mathbb{Z}$.

5 Exploring $\mathbb{Q}_p$

Now that we've achieved our main goal of defining the field of $p-$adic numbers and the motivation behind them, let's explore them and see how they compare to what we are familiar with.

Theorem 5.1. *Let (x_n) be a sequence in $\mathbb{Q}_p$, (x_n) is Cauchy if and only if $\forall \varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $\forall n \geqslant N$ we have,*

$$|x_{n+1} - x_n| < \varepsilon.$$

Proof. $(\Rightarrow)$ Assuming (x_n) is Cauchy. Let $\varepsilon > 0$, then there exists $N \in \mathbb{N}$ such that for all $n, m \geqslant N$ we have,

$$|x_n - x_m|_p < \varepsilon.$$

Let $n \geqslant N$, then it is obvious that $n + 1 \geqslant N$ and we have,

$$|x_{n+1} - x_n|_p < \varepsilon$$

proving the forward direction.

($\Leftarrow$) Now we assume that for every $\varepsilon > 0$ there exists some $N \in \mathbb{N}$ such that for all $n \geqslant N$ we have,

$$|x_{n+1} - x_n|_p < \varepsilon.$$

Now let $n, m \geqslant N$, in the case that $n = m$ we have,

$$|x_n - x_m|_p = |0|_p = 0 < \varepsilon$$

so let us consider when $n \neq m$. Without loss of generality let $n > m$, we then have $n = m + a$ for some $a \in \mathbb{Z}$. Therefore we can write $|x_n - x_m|_p$ as,

$$|(x_{m+a} - x_{a+m-1}) + (x_{m+a-1} - x_{a+m-2}) + \cdots + (x_{m+1} - x_m)|_p$$

recall though that the $p-$adic absolute value is non-Archimedean so,

$$|x_n - x_m|_p \leqslant \max\left\{|x_{m+i} - x_{m-i-1}|_p : i = 1, \ldots, k\right\}.$$

We have then for some i_0, $1 \leqslant i_0 \leqslant k$,

$$\left|x_{m+i_0} - x_{m+i_0-1}\right|_p = \max\left\{|x_{m+i} - a_{m+i-1}|_p : i = 1, \ldots, k\right\}$$

Meaning we have $|x_n - x_m|_p \leqslant \left|x_{m+i_0} - x_{m+i_0-1}\right|_p$. Note though that $m \geqslant N$, then through our assumption we have,

$$\left|x_{m+i_0} - x_{m+i_0-1}\right|_p < \varepsilon.$$

Then through transitivity we have that

$$|x_n - x_m|_p < \varepsilon$$

making (x_n) Cauchy as desired. □

Let us consider something a bit more interesting though. Maybe you've seen a sum that goes like,

$$\sum_{i=1}^{\infty} = \frac{-1}{12}$$

which is actually only true if using a different definition of summation, specifically Ramanujan Summation. Since under standard definitions the sum of all natural numbers is actually divergent. Similarly to this,

$$\sum_{n=0}^{\infty} 2^n$$

or not? Of course it is divergent under the standard definition of summation and working with the integers, but what if I told you that under the $2-$adic system this sum actually converged to something, specifically -1! We will prove this, by proving something more general.

Lemma 5.2. *Under the* $p-$*adic number system,* $\sum_{n=0}^{\infty} p^n$ *converges and its sum is* $\dfrac{1}{1-p}$.[3]

Proof. Let (x_n) be the sequence of partial sums for $\sum_{n=0}^{\infty} p^n$. Then for all $n \in \mathbb{N}_0$ we have,

$$x_n = \sum_{i=0}^{n-1} p^i.$$

It can be seen that,

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

Therefore,

$$x_n = \sum_{i=0}^{n-1} p^i = \frac{1-p^n}{1-p}.$$

Notice now that,

$$\lim_{n\to\infty} \frac{1}{1-p} = \frac{1}{1-p}$$

but since we are in the $p-$adic system it can be easily verified that $\lim_{n\to\infty} p^n = 0$. Now all together we have,

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} \frac{1}{1-p} - \lim_{n\to\infty} \frac{1}{1-p} \cdot \lim_{n\to\infty} p^n = \frac{1}{1-p}$$

as desired □

Meaning under the $p-adic$ number system we can take the infinite sum of powers of p and it will not only converge, but converge to something negative! This is very different from what we are used to. This also reveals why under the p-adic metric the integers are not complete since we created a sequence of partial sums where each term is an integer and is converging to something outside of $\mathbb{Z}$ (at least for $p > 2$) [2].

Another thing to note is that this is analogous the formula of a geometric series in $\mathbb{R}$. Recall though that only held true where $|x| < 1$. Through similar reasoning this can also be extended to hold for all $x \in \mathbb{Q}_p$ that satisfy $|x|_p < 1$. [3]

6 Conclusion

We were able to construct the field of $p-$adic numbers in a more natural way to show them similarly to the reals, while at the same time contrasting their differences. Hopefully through the exposure of Ostrowski's Theorem one can see the importance of these numbers and explore them further! Their uniqueness is also matched greatly by their utility. One important mathematical object needed in Andrew Wiles' proof of Fermat's Last Theorem was p-adic numbers. They are also being explored in elliptical curve cryptography by considering an elliptical curve over the field of $p-$adic numbers. There use has also been found by physicists who are exploring p−adic quantum mechanics. Unfortunately we weren't able to touch on some very interesting geometric or topological properties of p−adic numbers, but hopefully one is motivated enough to go explore those through the references provided. We also weren't able to go over some visualization of a "p−adic number line", but the presentation that accompanies this paper goes into that. Thank you for reading.

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)

[6] David A. Madore (2000) *A First Introduction to* p*-adic numbers*, http://www.madore.org/ david/math/padics.pdf