Introduction to p-adic numbers

Diana-Maria Harambas

Fall 2023

This paper was written to support my presentation within the Undergraduate Seminar I course offered at Constructor University, and held by Dr. Keivan Mallahi-Karai.

ABSTRACT. In this paper, the field $\mathbb{Q}_p$ of $p-$adic numbers is constructed as a completion of the rational numbers. The necessary background will be introduced, including definitions of metric and ultrametric spaces, a brief discussion on constructing the real numbers, and properties of Cauchy sequences with respect to non-archimedean absolute values. Before introducing $\mathbb{Q}_p$ (and then $\mathbb{Z}_p$), the $p-$adic valuation and metric are presented, with an example of calculating distances with the newly-shown $3-$adic metric. Some interesting properties on the representations of the $p-$adic integers and numbers are stated and are followed by a fractal-like visualisation of $\mathbb{Z}_3$ (which can be generalized to $\mathbb{Z}_p$), alongside results in the topology and geometry in $\mathbb{Q}_p$.

Contents

1 Motivation and background

Although we are used to working in different fields, we are most aware of the construction of real numbers as a completion of the rationals. The $p-$adic numbers, where p is a prime number, however, are used as an alternate completion of $\mathbb{Q}$ and come from a different definition of distance between two numbers. Moreover, according to Ostrowski's theorem (Theorem 2.6 in this paper), the only norms on $\mathbb{Q}$ up to equivalence are the usual one and $p-$adic one.

Using $p-$adic numbers might be, at first, an unusual way to think about certain problems, but sometimes it actually is an easier method than working in $\mathbb{R}$. In number theory, for example, we deal a lot with divisibility, prime numbers and powers of primes (a great example is Hasse's local-global principle) - the $p-$adic numbers have a useful distance function which evaluates "how divisible" by p a rational number is.

Since this distance function is the one which brings the changes between our completions of $\mathbb{Q}$, we should start with remembering the definition of a metric space.

1.1 Absolute value and metric spaces

We know that $\mathbb{R}$ is a complete metric space, and the interesting aspect for $p-$adic numbers is that they are not only a complete metric space, but also an *ultrametric* space. To define this *ultrametric* notion, we need to trace back the definitions and start with the properties of the absolute value on some arbitrary field $\mathbb{F}$. For this section, the paper will follow the structure of [1] and [2].

Definition 1.1 (Absolute value). *For a field $\mathbb{F}$, an absolute value is a function $|\cdot| : \mathbb{F} \longrightarrow \mathbb{R}_{\geq 0}$ such that, for any $x, y \in \mathbb{F}$ the following hold:*

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

Definition 1.2 (Non-archimedean absolute value). *For a field $\mathbb{F}$, an absolute value is non-archimedean if, apart from the properties of an absolute value, it also satisfies a stronger version of the triangle inequality, for any $x, y \in \mathbb{F}$:*

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

Now that we classified our absolute values into archimedean and non-archimedean, we can talk about the difference between a metric space and an ultrametric space.

Definition 1.3 (Metric. Metric space). *A metric on $\mathbb{F}$ is defined by the distance function $d : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{R}_{\geq 0}$ induced by the absolute value on $\mathbb{F}$ and defined by*

$$d(x, y) = |x - y|, \forall x, y \in \mathbb{F}.$$

A set with a metric is a metric space.

Definition 1.4 (Ultrametric. Ultrametric space). *A metric on a space is called an ultrametric if it is induced by a non-archimedean absolute value.*

A set together with an ultrametric is called an ultrametric space.

Proposition 1.5. *In an ultrametric space containing arbitrarily chosen x, y with $|x| \neq |y|$,*

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

Proof. $|x| \neq |y|$ implies that one of $|x| > |y|$ or $|x| < |y|$ is true. Without loss of generality, let us consider $|x| > |y|$. In our ultrametric space, the absolute value is non-archimedean, hence it will respect the stronger version of the triangle inequality:

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

which in this case is

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

But since $x = (x + y) + (-y)$, and $|-y| = |y|$, we apply the stronger condition again to obtain that

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

We know the statement above is true and now need to evaluate $\max\{|x + y|, |y|\}$. If the maximum is $|y|$, then $|x| \leq |y|$, which contradicts the assumption that $|x| > |y|$. Therefore, we need $|x + y| > |y|$. Then,

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

From $|x| \geq |x + y|$ and $|x| \leq |x + y|$, we deduce $|x| = |x + y|$, so

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

QED

This is not the only interesting property of ultrametric spaces, but we will discuss some others in a future section, when we describe certain properties of the geometry of $p-$adic numbers.

At the beginning of section 1, we described $\mathbb{R}$ as a complete metric space, and the definition of completeness might be required, but for that we need to recall the definition of Cauchy sequences. In section 1.2, we'll discuss these and also outline a method of constructing $\mathbb{R}$ from $\mathbb{Q}$.

1.2 Cauchy sequences and $\mathbb{R}$ as a completion of $\mathbb{Q}$

Definition 1.6 (Cauchy sequence)**.** *A sequence (x_n) is Cauchy if for every $\epsilon > 0$, there exists a natural number N such that*

$$|x_n - x_m| < \epsilon, \forall m, n \geq N.$$

Proposition 1.7. *Every Cauchy sequence is a bounded sequence.*

We say that a Cauchy sequence (x_n) is a *null sequence* if $\lim_{k\to\infty} |x_k| = 0$, and we know that the following results hold:

1. If $(x_n), (y_n)$ are null sequences, then $(x_n + y_n)$ is a null sequence.
2. If (x_n) is a null sequence and (a_n) is a bounded sequence, then $(x_n \cdot a_n)$ is null.
3. If (a_n) contains infinitely many zeros, then it is a null sequence.

Definition 1.8 (Equivalent Cauchy sequences)**.** *For Cauchy sequences $(x_n), (y_n)$, define their difference as the sequence $z_n = x_n - y_n$. We say that $(x_n), (y_n)$ are equivalent if they differ by a null sequence, i.e. if (z_n) is a null sequence.*

We write this as $(x_n) \sim (y_n)$. Since $\sim$ is an equivalence relation, we can create a partition of equivalence classes. This, alongside the algebra theorem below (which explains why a completion for a general field $\mathbb{K}$ and an absolute value must exist), is enough to build the real numbers - which is complete under the standard metric.

Definition 1.9 (Complete metric space)**.** *A metric space X is complete under the given metric if every Cauchy sequence (x_n) is convergent, with the limit in X.*

Theorem 1.10. *If $\mathbb{K}$ is a field with absolute value $|\cdot|$, we can extend it to a complete field $\mathbb{K}'$ with absolute value $|\cdot|'$. Moreover, $\mathbb{K}$ is dense in its completion $\mathbb{K}'$, which is unique up to isomorphism.*

We extend $\mathbb{Q}$ to $\mathbb{R}$ using the following definition of the real numbers.

Definition 1.11 (The set of real numbers)**.** *We define $\mathbb{R}$ as the partition of all Cauchy sequences into equivalence classes of the relation $\sim$.*

With this, the condition of a complete metric space is satisfied by $\mathbb{R}$.

This construction outline is also used for the $p-$adic numbers, where the metric used won't be the usual one, but a new one, defined in the next section. However, there is one last relevant lemma on Cauchy sequences to be discussed before advancing to the next section.

Lemma 1.12. *A sequence (x_n) of rational numbers is Cauchy with respect to a non-archimedean absolute value if and only if for every $\epsilon > 0$, there exists natural number N such that*

$$|x_{n+1} - x_n| < \epsilon, \forall n \geq N.$$

Proof. If the sequence is Cauchy, the implication follows trivially. Conversely, by taking $m = r + n > n$ we obtain:

$$|x_m - x_n| = |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \cdots + x_{n+1} - x_n| \leq$$

$$\leq \max\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \ldots, |x_{n+1} - x_n|\} < \epsilon,$$

hence the sequence is Cauchy. QED

2 The $p-$adic metric and $p-$adic numbers

Since our goal is to prove that the $p-$adic numbers, written as $\mathbb{Q}_p$, form a complete ultrametric space, we need to define what our distance function is. For that, we start with $p-$adic valuation. [1]

2.1 The $p-$adic valuation

Definition 2.1 ($p-$adic valuation)**.** *Define a function $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ such that:*

- *For a non-zero integer number a, we can define $v_p(a)$ as the unique positive integer such as*
$$a = p^{v_p(a)} b, \text{ where } p \nmid b.$$
- *For all non-zero rational numbers $x = \frac{m}{n}$, with m, n non-zero integers,*
$$v_p(x) = v_p(m) - v_p(n).$$
- $v_p(0) = \infty$.

This is called the $p-$adic valuation on $\mathbb{Q}$.

Lemma 2.2. *For all $x, y \in \mathbb{Q}$, the following properties hold:*

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x + y) \geq min\{v_p(x), v_p(y)\}$

Proof for 1: If either one of x, y is 0, then the equality is clear. Else, we can write them as $x = \frac{m}{n}, y = \frac{q}{r}$, with m, n, q, r non-zero integers with

$$m = p^{v_p(m)} \cdot m', \text{ with } p \nmid m',$$

$$n = p^{v_p(n)} \cdot n', \text{ with } p \nmid n',$$

$$q = p^{v_p(q)} \cdot q', \text{ with } p \nmid q',$$

$$r = p^{v_p(r)} \cdot r', \text{ with } p \nmid r'.$$

Then $v_p(xy) = v_p(\frac{mq}{nr}) = v_p(mq) - v_p(nr) = (v_p(m) + v_p(q)) - (v_p(n) + v_p(r))$, because $mq = p^{v_p(m)+v_p(q)}m'q'$ and $nr = p^{v_p(n)+v_p(r)}n'r'$. This means that

$$v_p(xy) = ((v_p(m) + v_p(q)) - ((v_p(n) + v_p(r)) = ((v_p(m) - v_p(n)) + ((v_p(q) - v_p(r))$$

$$v_p(xy) = v_p(x) + v_p(y).$$

QED

Proof for 2: If $x + y = 0$, then the inequality is trivially true. Else, let's assume, without loss of generality, that $\min\{v_p(x), v_p(y)\} = v_p(x)$., which is finite considering that $x + y \neq 0$. We'll write $x = \frac{m}{n}$, with m, n non-zero integers.

If $y = 0$, then $v_p(x + y) = v_p(x)$ clearly. Then, let's consider the case in which $y \neq 0$. Hence $y = \frac{q}{r}$, with $q, r \in \mathbb{Z} \setminus \{0\}$.

We know that $v_p(x) \leq v_p(y)$, therefore

$$v_p(m) - v_p(n) \leq v_p(q) - v_p(r) \iff$$

$$\iff v_p(m) + v_p(r) \leq v_p(q) + v_p(n) \iff$$

$$\iff v_p(mr) \leq v_p(qn).$$

Let $k, l \in \mathbb{Z}$ not divisible by p such that

$$mr = p^{v_p(mr)}a,$$

$$qn = p^{v_p(qn)}b.$$

Because $v_p(mr) \leq v_p(qn)$, $p^{v_p(mr)}|p^{v_p(qn)}$, and therefore $mr + qn$ will be divisible by $p^{v_p(mr)}$. This means that

$$v_p(mr) \leq v_p(mr + qn) \iff$$

$$\iff v_p(m) + v_p(r) \leq v_p(mr + qn) \iff$$

$$\iff v_p(m) - v_p(n) \leq v_p(mr + qn) - v_p(r) - v_p(n) \iff$$

$$\iff v_p(x) \leq v_p(x + y) \iff$$

$$\iff \min\{v_p(x), v_p(y)\} \leq v_p(x + y).$$

With this in mind, we can move forward and define the $p-$adic metric. QED

2.2 The $p-$adic metric

Definition 2.3 ($p-$adic absolute value)**.** *The $p-$adic absolute value is a function $|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$ such that*

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

This induces the metric (the distance function), which we will call d_p.

Example 2.4. *We will calculate the distance between some integers using the $3-$adic metric:*

- $d_p(1,2) = |2-1|_p = |1|_p = 1$
- $d_p(1,7) = |7-1|_p = |6|_p = \frac{1}{3}$
- $d_p(9,18) = |18-9|_p = |9|_p = \frac{1}{9}$
- $d_p(9,27) = |27-9|_p = |18|_p = \frac{1}{9}$
- $d_p(9,27) = \max\{|9|_p, |27|_p\} = \max\{\frac{1}{9}, \frac{1}{27}\} = \frac{1}{9}$

Proposition 2.5. *The $p-$adic absolute value is a non-archimedean absolute value on $\mathbb{Q}$.*

Proof. First, we need to prove that it satisfies the properties of an absolute value (from **Definition 1.1**). Condition 1 and 2 are true, as immediate results of **Definition 2.3**, and **Lemma 2.2**, respectively.

It remains to prove that the triangle inequality holds and, for showing that $|\cdot|_p$ is non-archimedean, we will prove that the stronger version of the triangle inequality, from **Definition 1.2**, is also satisfied.

In case $x + y = 0$, then $|x+y|_p = 0$ and both inequalities hold true. In case $x + y \neq 0$, let's assume that $\max\{|x|_p, |y|_p\} = |x|_p$, without loss of generality. Hence $|x|_p > 0$ and $v_p(x) \leq v_p(y)$. From **Lemma 2.2**, we have $v_p(x+y) \geq \min\{v_p(x), v_p(y)\} = v_p(x)$.

This implies $p^{-v_p(x+y)} \leq p^{-v_p(x)}$, i.e. $|x+y|_p \leq |x|_p = \max\{|x|_p, |y|_p\}$.

Since we proved the inequality from **Definition 1.2**, the triangle inequality is also true, and $|\cdot|_p$ is a non-archimedean absolute value. QED

Now that we familiarised ourselves with the $p-$adic absolute value, we can continue with the construction of the $p-$adic numbers field.

2.3 The $p-$adic numbers

We'll start with an important theorem that classifies the absolute values on $\mathbb{Q}$, which yields to the possible completions of $\mathbb{Q}$. [3]

Theorem 2.6 (Ostrowski)**.** *Every nontrivial absolute value defined on $\mathbb{Q}$ is either the standard absolute value or one of the $p-$adic absolute values.*

Knowing this, it is natural to want to work in complete metric spaces, so one should question whether the field of rational numbers is complete under the $p-$adic metric or not.

Proposition 2.7. *$\mathbb{Q}$ is not complete under the $p-$adic metric.*

Proof. In order to show this, we need to take a Cauchy sequence of rational numbers that won't have its limit in $\mathbb{Q}$. Let's take the $p-$adic metric for some odd prime p. Then, let us choose an integer a such that:

- a is not a square in $\mathbb{Q}$
- $p \nmid a$
- a is a quadratic residue mod p

We know such number a exists (take a perfect square b^2 non-divisible by p in $\mathbb{Z}$, then $a = p + b^2$ will satisfy the properties above). We now build a Cauchy sequence of rational numbers with respect to our non-archimedean absolute value $|\cdot|_p$. We will do this step by step:

- choose x_0 to be some solution of $x_0^2 \equiv a \pmod{p}$
- choose x_1 that satisfies $x_1 \equiv x_0 \pmod{p}$ and $x_1^2 \equiv a \pmod{p^2}$ (such solution can be found by the "lifting" technique learnt in Number Theory when solving congruences modulo p^n)
- continue the process inductively and choose x_n such that $x_n \equiv x_{n-1} \pmod{p^n}$ and $x_n^2 \equiv a \pmod{p^{n+1}}$

We claim that this is a Cauchy sequence under the non-archimedean $p-$adic metric. This is true because, by applying **Lemma 1.12**, we can show that

$$\lim_{n\to\infty} |x_{n+1} - x_n|_p = \lim_{n\to\infty} |m \cdot p^{n+1}|_p \leq \lim_{n\to\infty} \frac{1}{p^{n+1}} = 0,$$

i.e. the sequence (x_n) is Cauchy. Moreover,

$$\lim_{n\to\infty} |x_n^2 - a|_p = \lim_{n\to\infty} |m' \cdot p^{n+1}|_p \leq \lim_{n\to\infty} \frac{1}{p^{n+1}} = 0,$$

which is equivalent to saying that the limit of our sequence is the square root of a. However, a is not a square in the field of rational numbers, and that leads us to the end of our proof: we found a rational Cauchy sequence with no limit in $\mathbb{Q}$, therefore $\mathbb{Q}$ is not complete with respect to $|\cdot|_p, \forall p$ odd primes.

The proof for $p = 2$ is similar and thus can be omitted here - instead of looking at square roots, one should explore cube roots. QED

Now that we have proven that the field of rational numbers is not complete under our $p-$adic absolute value, we acknowledge the need for a completion field:

Definition 2.8 (The field of $p-$adic numbers)**.** *$\mathbb{Q}_p$, called the field of $p-$adic numbers, is the completion of $\mathbb{Q}$ with respect to the $p-$adic metric.*

We respect **Definition 1.8** for the equivalence classes of Cauchy sequences and in a similar fashion, $\mathbb{Q}_p$ will be the partition of equivalence classes of all Cauchy sequences under $|\cdot|_p$. Or, it can be defined equivalently as the quotient of the ring of Cauchy sequences under $|\cdot|_p$, call it C_p, by its maximal ideal of null sequences $N = \{(x_n) \mid \lim_{n\to\infty} |x_n|_p = 0\}$, i.e.

$$\mathbb{Q}_p = C_p/N$$

Proposition 2.9. *$\mathbb{Q}_p$ is an ultrametric space.*

The proof follows from the definition of the $p-$adic metric, induced by a non-archimedean absolute value.

We'll also introduce the $p-$adic integers, as they will help us "visualise" better how the $p-$adic metric works.

Definition 2.10 (The $p-$adic integers)**.** *$\mathbb{Z}_p$, called the ring of $p-$adic integers is defined as follows:*

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

As remarks, $\mathbb{Z}_p$ is actually the completion of $\mathbb{Z}$ under the $p-$adic metric, and its units are the elements x for which $|x|_p = 1$.

The question that arises now is how do we represent numbers in $\mathbb{Z}_p$ and $\mathbb{Q}_p$. We'll show that we can represent the numbers as a "power series in p". In the proof, we'll use the following proposition:

Proposition 2.11. *For any element $a \in \mathbb{Z}_p$, there exists a unique Cauchy sequence of integers x_n converging to a such that:*

- $x_{n+1} \equiv x_n \ (mod\ p^n)$
- $0 \leq x_n \leq p^n - 1$

Theorem 2.12. *Every element $a \in \mathbb{Z}_p$ can be uniquely written as*

$$a = b_0 + b_1 p + ... + b_n p^n + \dots,$$

with $b_i \in \{0, 1, \dots p-1\}$.

Proof. We'll start with the elements of $\mathbb{Z}_p$. By **Proposition 2.11** for $a \in \mathbb{Z}_p$, we can build a unique sequence of integers converging to a that follows the properties:

- $x_n \equiv a \pmod{p^n}$
- $x_{n+1} \equiv x_n \pmod{p^n}$
- $0 \leq x_n \leq p^n - 1$

We can write these integers in base p and, starting with x_0, we'll obtain that the elements of the sequence are of form $x_n = b_0 + b_1 p + ... + b_n p^n$, with $b_i \in \{0, 1, \dots p-1\}$ unique, which leads to uniquely representing our number a as

$$a = b_0 + b_1 p + ... + b_n p^n + \dots.$$

Since the partial sums x_n of $b_0 + b_1 p + \dots + b_n p^n + \dots$ converge to a, it means that our unique representation is valid. QED

From this, we can get the representation of the elements in $\mathbb{Q}_p$.

Corollary 2.13. *Every element $a \in \mathbb{Q}_p$ can be uniquely written as*

$$a = b_{-n_0} p^{-n_0} + \dots + b_0 + b_1 p + \dots + b_n p^n + \dots,$$

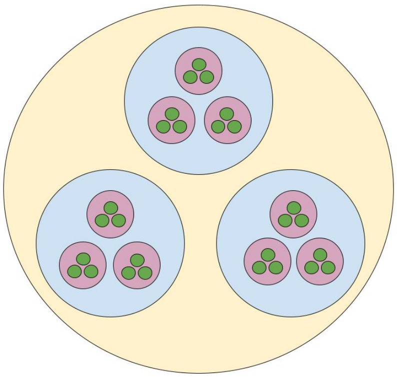
with $b_i \in \{0, 1, \dots p-1\}$ and $-n_0 = v_p(a)$.

3 Exploring the $p-$adic numbers

Our final section will present some topology and geometry results of the $p-$adic numbers, starting with an example of visual representation of the $p-$adic integers. [1]

3.1 Visualising $\mathbb{Z}_3$

In number theory, it was common to build equivalence classes of integers modulo m, forming $\mathbb{Z}/m\mathbb{Z}$. We are going to take a look at the image below, which is a way to visualise the $3-$adic integers, and for that, we will take into consideration classes of integers modulo $3, 3^2, 3^3, \ldots$.



Here, the yellow circle represents an equivalence class modulo 3 (say, $a \equiv 0 \mod 3$). It is further divided into three blue sub-circles, which represent equivalence classes modulo 3^2, still contained in the equivalence class modulo 3 (so, $a \equiv 0, 3, 6 \mod 3^2$). Further, the red sub-circles in one blue circle are the respective equivalence classes modulo 3^3 ($a \equiv 0, 9, 18 \mod 3^3$ in one, $a \equiv 3, 12, 21 \mod 3^3$ in another, and $a \equiv 6, 15, 24 \mod 3^3$ in the last one). We can continue this process and get infinitely small circles. This fractal-like visualisation helps us generalize: $\mathbb{Z}_p$ is disconnected, but not discrete.

3.2 The topology on $\mathbb{Q}_p$

Let's now state some more formal results (most without proof) on the topology of the $p-$adic numbers.

Theorem 3.1. *Any open ball is also a closed ball in $\mathbb{Q}_p$, and vice versa.*

Proof. Let $B(a, r) = \{x \in \mathbb{Q}_p \mid |x - a|_p < r\}$ be an open ball and take the smallest integer n such that $r \leq p^{-n}$.

Since $v_p(x) \in \mathbb{Z}$ for any nonzero rational x, the $p-$adic absolute value takes a discrete set of values, and therefore, in our case, there will not be any numbers in $\mathbb{Q}_p$ with the $p-$adic absolute value between $p^{-(n+1)}$ and p^{-n}. With this in mind, note that

$$B(a, r) = \{x \in \mathbb{Q}_p \mid |x-a|_p < r\} = \{x \in \mathbb{Q}_p \mid |x-a|_p < p^{-n}\} = \{x \in \mathbb{Q}_p \mid |x-a|_p \leq p^{-(n+1)}\},$$

hence $B(a, r)$ is a closed ball.

One can prove that a closed ball in $\mathbb{Q}_p$ is also an open ball by constructing a symmetric argument. QED

Corollary 3.2. *$\mathbb{Z}_p$ is both closed and open in $\mathbb{Q}_p$.*

Corollary 3.3. *$\mathbb{Q}_p$ is a totally disconnected (Hausdorff) topological space.*

Corollary 3.4. *$\mathbb{Z}_p$ is a compact and $\mathbb{Q}_p$ is locally compact.*

3.3 Geometry of the $p-$adic numbers

The final points that we shall introduce in this paper are some interesting geometrical results.

Theorem 3.5. *All triangles are isosceles in $\mathbb{Q}_p$.*

Proof. Let us take three arbitrary distinct points $x, y, z \in \mathbb{Q}_p$. Their triangle will have sides of length $|x-y|_p, |y-z|_p, |x-z|_p$. If $|x-y|_p = |y-z|_p$, the triangle is isosceles. So, assume that $|x-y|_p \neq |y-z|_p$. Then

$$|x-z|_p = |x-y+y-z|_p = \max\{|x-y|_p, |y-z|_p\},$$

meaning that two sides are of equal length and the triangle is isosceles. QED

Corollary 3.6. *No three distinct points are collinear in* $\mathbb{Q}_p$.

Proof. Assume for the sake of contradiction that there exist some distinct $x, y, z \in \mathbb{Q}_p$ that are collinear in that order (without loss of generality), i.e. $|x-z|_p = |x-y|_p + |y-z|_p$. Clearly, $|x-z|_p > |x-y|_p$ and $|x-z|_p > |y-z|_p$, but $|x-z|_p = |x-y+y-z|_p = \max\{|x-y|_p, |y-z|_p\}$ also holds. This yields a contradiction and there are no three distinct collinear points. QED

Corollary 3.7. *There are no right triangles in* $\mathbb{Q}_p$.

Proof. Assume for the sake of contradiction that the distinct points $x, y, z \in \mathbb{Q}_p$ determine a right triangle. We know from **Theorem 3.5** that the triangle is isosceles (assume, without loss of generality, $|x-y|_p = |y-z|_p$). By the Pythagorean theorem, we should obtain $|x-z|_p^2 = |x-y|_p^2 + |y-z|_p^2$, which means that $|x-z|_p$ is the longest side. But now,

$$|x-z|_p = |x-y+y-z|_p = \max\{|x-y|_p, |y-z|_p\} = |x-y|_p = |y-z|_p,$$

which means that the triangle is equilateral, and thus cannot be a right triangle, reaching a contradiction. Therefore, there are no right triangles in $\mathbb{Q}_p$. QED

4 Conclusion

To conclude, this paper showcased some of the most important properties of $p-$adic numbers, starting with the field construction and ending with some interesting results about its topology and geometry. This topic is a very broad one and thus can be further studied by exploring $p-$adic equations or by taking a more algebraic approach and studying the multiplicative group of $\mathbb{Q}_p$, for example.

5 References

[1] Alexa Pomerantz. An introduction to the p-adic numbers.

[2] William J. LeVeque. *Fundamentals of number theory.* Dover Publications, Inc., Mineola, NY, 1996. Reprint of the 1977 original.

[3] Fernando Q. Gouvêa. *p-adic numbers.* Universitext. Springer, Cham, third edition, [2020] ©2020. An introduction.

Websites that were used to understand the topic better and polish the explanations:

Kelsey Houston Edwards. *An Infinite Universe of Number Systems*
Wikipedia, *Ultrametric space* and *p−adic number*