AN INTRODUCTION TO THE p-ADIC NUMBERS

ALEXA POMERANTZ

Abstract. This paper introduces the p-adic numbers with an emphasis on comparison to the real numbers. It is mostly self-contained, but some basic knowledge in number theory, analysis, topology, and geometry is assumed. We begin by defining the p-adic metric and using this metric to construct $\mathbb{Q}_p$ and $\mathbb{Z}_p$. We then move on to sequences and series and writing p-adic expansions. Lastly, we discuss topology and geometry in $\mathbb{Q}_p$.

Contents

1. Introduction

The p-adic numbers, where p is any prime number, come from an alternate way of defining the distance between two rational numbers. The standard distance function, the Euclidean absolute value, gives rise to the real numbers. While the real numbers are more natural to most of us, this paper aims to present the p-adic numbers on an equal footing. For example, both fields are complete metric spaces. Unlike the real numbers, the p-adic numbers are an ultrametric space, leading to a number of fascinating but often counterintuitive results.

The p-adic numbers are useful because they provide another toolset for solving problems, one which is sometimes easier to work with than the real numbers. They have applications in number theory, analysis, algebra, and more. One example is Hensel's lemma for finding roots of a polynomial. Another is Mahler's Theorem, a p-adic analog of the Stone-Weierstrass Theorem. Yet another is Monsky's Theorem, a theorem about triangulating squares whose proof makes use of 2-adic numbers. The reader is encouraged to read more about these in their own time, but the rest of this paper will be focused on introducing p-adic numbers more broadly.

We start off by introducing the p-adic metric and then employing it to construct the p-adic numbers using Cauchy sequences. We then move on to some unique results about sequences and series that do not appear in real analysis. This leads

into a discussion of p-adic expansions, which will help us think about p-adic numbers in a more concrete way. Next, we discuss the topology on $\mathbb{Q}_p$ to get a sense for p-adic spaces. Finally, we look at how p-adic geometry differs from Euclidean geometry.

2. The p-adic Metric

We begin by defining a general notion of absolute value for an arbitrary field $\mathbb{K}$.

Definition 2.1. An *absolute value* on $\mathbb{K}$ is a function $|\cdot|\colon \mathbb{K} \to \mathbb{R}_{\geq 0}$ that satisfies the following properties for all $x, y \in \mathbb{K}$:

(i) $|x| = 0$ if and only if $x = 0$,
(ii) $|xy| = |x||y|$, and
(iii) $|x + y| \leq |x| + |y|$ (Triangle Inequality).

Moreover, an absolute value is *non-Archimedean* if it also satisfies the following property:

(iv) $|x + y| \leq \max\{|x|, |y|\}$ (Strong Triangle Inequality).

An absolute value that does not satisfy property (iv) is *Archimedean*.

Remark 2.2. We note that any function satisfying Property (iv) necessarily satisfies Property (iii).

Definition 2.3. A *metric* on $\mathbb{K}$ is defined by a distance function $d\colon \mathbb{K} \times \mathbb{K} \to \mathbb{R}_{\geq 0}$. An absolute value induces a metric defined by

$$d(x, y) = |x - y| \text{ for all } x, y \in \mathbb{K}.$$

A set on which a metric is defined is called a *metric space*. A set with a metric induced by a non-Archimedean absolute value is called an *ultrametric space*.

Lemma 2.4. *Let $\mathbb{K}$ be an ultrametric space, and let $x, y \in \mathbb{K}$. If $|x| \neq |y|$, $|x+y| = \max\{|x|, |y|\}$.*

Proof. Without loss of generality, we assume that $|x| > |y|$. Since $\mathbb{K}$ is an ultrametric space, $|x+y| \leq \max\{|x|, |y|\} = |x|$ (Definition 2.1 and Definition 2.3). Also, $x = (x + y) + (-y)$, so $|x| \leq \max\{|x + y|, |y|\}$. Since $|x| > |y|$, $|x + y| > |y|$. Thus, we have $|x + y| \leq |x| \leq |x + y|$. It follows that $|x + y| = |x| = \max\{|x|, |y|\}$. □

Exercise 2.5. Check that in a field with a metric induced by an absolute value, the following properties hold for all $x, y, z \in \mathbb{K}$:

- $d(x, y) > 0 \iff x \neq y$,
- $d(x, y) = d(y, x)$, and
- $d(x, z) \leq d(x, y) + d(y, z)$.

We now begin to define the p-adic metric specifically. For the rest of the paper, let p be a fixed prime number.

Definition 2.6. The *p-adic valuation* on $\mathbb{Q}$ is defined by a function $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. Let $x \in \mathbb{Q}$ where $x \neq 0$. If $x \in \mathbb{Z}$, let $v_p(x)$ be the unique positive integer satisfying

$$x = p^{v_p(x)}x', \text{ where } p \nmid x'.$$

For all nonzero $x \in \mathbb{Q}$, we may write $x = \dfrac{a}{b}$ where $a, b \in \mathbb{Z}$. Then we define

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

Lastly, we define $v_p(0) = +\infty$.

Remark 2.7. We can think of the p-adic valuation as describing how divisible by p a number is. In this way, it makes sense to define $v_p(0) = +\infty$ since 0 can be divided by p infinitely many times, yielding an integer (namely 0) each time.

Exercise 2.8. Show that the p-adic valuation does not depend on the representation of a rational number (if $\frac{a}{b} = \frac{a'}{b'}$, then $v_p(a) - v_p(b) = v_p(a') - v_p(b')$).

Exercise 2.9. Prove that if $x \in \mathbb{Q}$, $x = p^{v_p(x)}\dfrac{a'}{b'}$, where $p \nmid a'b'$.

Lemma 2.10. *The following properties hold for all $x, y \in \mathbb{Q}$:*

(i) $v_p(xy) = v_p(x) + v_p(y)$ *and*
(ii) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Proof. Let $x, y \in \mathbb{Q}$. Then $x = \dfrac{a}{b}$ and $y = \dfrac{c}{d}$, where $a, b, c, d \in \mathbb{Z}$.

First, if $x = 0$ or $y = 0$, then $v_p(xy) = v_p(x) + v_p(y) = +\infty$. We therefore consider the case that both x and y are nonzero. Then

$$v_p(x) = v_p(a) - v_p(b), \text{ and } v_p(y) = v_p(c) - v_p(d) \text{ (Definition 2.6).}$$

Moreover, since $xy = \dfrac{ac}{bd}$,

$$v_p(xy) = v_p(ac) - v_p(bd).$$

Since $a, c \in \mathbb{Z}$,

$$a = p^{v_p(a)}a' \text{ and } c = p^{v_p(c)}c', \text{ where } p \nmid a' \text{ and } p \nmid c' \text{ (Definition 2.6).}$$

Then

$$ac = p^{v_p(a)}a' \cdot p^{v_p(c)}c' = p^{v_p(a)+v_p(c)}a'c'.$$

Since $p \nmid a'$ and $p \nmid c'$, $p \nmid a'c'$. Thus, by Definition 2.6, $v_p(ac) = v_p(a) + v_p(c)$. By a similar argument, $v_p(bd) = v_p(b) + v_p(d)$. It follows that

$$v_p(xy) = v_p(ac) - v_p(bd) = v_p(a) + v_p(c) - v_p(b) - v_p(d) = v_p(x) + v_p(y).$$

Hence, the p-adic valuation satisfies the first property.

Next, if $x + y = 0$, then $v_p(x + y) = +\infty \geq \min\{v_p(x), v_p(y)\}$ trivially. We therefore consider the case that $x + y \neq 0$. Without loss of generality, we assume that $v_p(x) \leq v_p(y)$. Then $v_p(x)$ is finite (if this were not the case, then $x + y = 0$ since $x = y = 0$). By Definition 2.6,

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

Also, if $y = 0$, $v_p(x+y) = v_p(x) = \min\{v_p(x), v_p(y)\}$. Thus, we assume that $y \neq 0$, so

$$v_p(y) = v_p(c) - v_p(d).$$

Since $v_p(x) \leq v_p(y)$,

$$v_p(a) - v_p(b) \leq v_p(c) - v_p(d).$$

It follows that

$$v_p(a) + v_p(d) \leq v_p(b) + v_p(c).$$

Equivalently, $v_p(ad) \leq v_p(bc)$ (by part (i)). Since $ad \in \mathbb{Z}$ and $bc \in \mathbb{Z}$,

$$ad = p^{v_p(ad)}m \text{ and } bc = p^{v_p(bc)}n, \text{ where } p \nmid m \text{ and } p \nmid n \text{ (Definition 2.6).}$$

Then

$$ad + bc = p^{v_p(ad)}m + p^{v_p(bc)}n.$$

Since $v_p(ad) \leq v_p(bc)$, $p^{v_p(ad)} \mid p^{v_p(bc)}$. It follows that $p^{v_p(ad)} \mid ad + bc$. Thus, $v_p(ad + bc) \geq v_p(ad)$. We now manipulate this inequality as follows, applying the result from part (i) as necessary:

$$\begin{aligned} v_p(ad + bc) &\geq v_p(ad) \\ \implies v_p(ad + bc) &\geq v_p(a) + v_p(d) \\ \implies v_p(ad + bc) - v_p(d) &\geq v_p(a) \\ \implies v_p(ad + bc) - v_p(b) - v_p(d) &\geq v_p(a) - v_p(b) \\ \implies v_p(ad + bc) - v_p(bd) &\geq v_p(a) - v_p(b) \end{aligned}$$

We recall that $x + y = \dfrac{ad + bc}{bd}$, so

$$v_p(x + y) = v_p(ad + bc) - v_p(bd).$$

Thus, we have $v_p(x + y) \geq v_p(x) = \min\{v_p(x), v_p(y)\}$. In other words, the p-adic valuation satisfies the second property. □

Definition 2.11. Let the *p-adic absolute value* function $|\cdot|_p \colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ be defined by

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

The p-adic absolute value induces the *p-adic metric*, denoted by d_p.

Remark 2.12. Since the p-adic valuation for nonzero rational numbers is always an integer, the p-adic absolute value takes a discrete set of values.

Proposition 2.13. *The p-adic absolute value is a non-Archimedean absolute value on* $\mathbb{Q}$.

Proof. Let $x, y \in \mathbb{Q}$. First, we suppose that $x = 0$. Then $|x|_p = 0$ by Definition 2.11. Now, we suppose that $x \neq 0$. Then $|x|_p = p^{-v_p(x)}$ by Definition 2.11. Since $p \neq 0$, $|x|_p \neq 0$. Thus, the p-adic absolute value satisfies Definition 2.1(i).

Next, we check the second property. In the case that $x = 0$ or $y = 0$, $|xy|_p = |x|_p|y|_p$ trivially. Hence, we consider the case that $x \neq 0$ and $y \neq 0$. Then by Definition 2.11, $|xy|_p = p^{-v_p(xy)}$, and $|x|_p|y|_p = p^{-v_p(x)}p^{-v_p(y)} = p^{-v_p(x)-v_p(y)}$. By Lemma 2.10(i), $-v_p(xy) = -v_p(x) - v_p(y)$. Therefore, $|xy|_p = |x|_p|y|_p$, and the p-adic absolute value satisfies Definition 2.1(ii).

Lastly, we check the third and fourth properties. in the case that $x+y = 0$, $|x+y|_p = 0$ by definition. Then $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ trivially. We consider the case that $x + y \neq 0$. Without loss of generality, we assume that $|x|_p \geq |y|_p$. Then $|x|_p \neq 0$, so $x \neq 0$. It follows that $v_p(x) \leq v_p(y)$. By Definition 2.11, $|x + y|_p = p^{-v_p(x+y)}$ and $|x|_p = p^{-v_p(x)}$. By Lemma 2.10(ii), $v_p(x + y) \geq \min\{v_p(x), v_p(y)\} = v_p(x)$. It follows that $p^{-v_p(x+y)} \leq p^{-v_p(x)}$. Equivalently, $|x + y|_p \leq |x|_p = \max\{|x|_p, |y|_p\}$. Thus, the p-adic absolute value satisfies Definition 2.1(iv) and consequently Definition 2.1(iii). □

Exercise 2.14. Find $\left|\frac{75}{73}\right|_5$, $\left|\frac{16}{81}\right|_3$, and $d_{11}(89, 4082)$.

Exercise 2.15. Prove that $\lim_{n\to\infty} p^n = 0$.

Proof. Let $\epsilon > 0$. By the Archimedean Property, there exists $N \in \mathbb{N}$ such that $\frac{1}{N} < \epsilon$. Since $p^N > N$, $\frac{1}{p^N} < \frac{1}{N} < \epsilon$. Let $n \geq N$. Then $\frac{1}{p^n} \leq \frac{1}{p^N} < \epsilon$. We note that $p^n \neq 0$ and $v_p(p^n) = n$, so $|p^n|_p = p^{-n}$. Hence, we have $|p^n|_p < \epsilon$. It follows that $\lim_{n\to\infty} p^n = 0$. □

Loosely stated, two absolute values are equivalent if they induce the same topology. Before moving on to the construction of the p-adic numbers, we state the following result about absolute values on $\mathbb{Q}$.

Theorem 2.16. *(Ostrowski's Theorem) Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to either the standard absolute value or one of the p-adic absolute values.*

Proof. See [3, p. 56-59]. □

Because of Ostrowski's Theorem, the p-adic absolute value can be viewed as just as important as the standard absolute value. Together, they comprise all possible absolute values on $\mathbb{Q}$. There are a number of results that we will prove later that could apply to any ultrametric space, but we care about the p-adic absolute values in particular because they are essentially the only non-Archimedean absolute values on $\mathbb{Q}$.

3. Construction of $\mathbb{Q}_p$ and $\mathbb{Z}_p$

Next, in order to construct the field of p-adic numbers from the rational numbers, we use a process similar to the construction of the real numbers using Cauchy sequences. We will not include all of the details but aim to provide an outline for this process by including the most relevant definitions and results.

Definition 3.1. A sequence (a_n) is *Cauchy* if for every $\epsilon > 0$, there is some $N \in \mathbb{N}$ such that for all $m, n \geq N$,

$$|a_n - a_m| < \epsilon.$$

Definition 3.2. A metric space X is *complete* under a given metric if every Cauchy sequence in X converges to a point in X.

Proposition 3.3. *The field of rational numbers, $\mathbb{Q}$, is not complete under the p-adic metric.*

Proof. See [3, p. 63-64]. □

Theorem 3.4. *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 $\mathbb{K}$. This completion $\mathbb{K}'$ is unique up to isomorphism. Moreover, on $\mathbb{K}$, $|\cdot|'$ restricts to $|\cdot|$. Lastly, $\mathbb{K}$ is dense in $\mathbb{K}'$.*

Sketch of Proof. We omit this proof since it involves some abstract algebra that is outside the scope of this paper. The reader can see [9, p. 5-6]. The general idea is for each element of $\mathbb{K}'$ to be represented by the limit of a Cauchy sequence of elements in $\mathbb{K}$ (or multiple equivalent Cauchy sequences). Any Cauchy sequence that does not have a limit in $\mathbb{K}$ will have a limit in $\mathbb{K}'$, making $\mathbb{K}'$ complete. □

Definition 3.5. Let the *field of p-adic numbers*, $\mathbb{Q}_p$, be defined by the completion of $\mathbb{Q}$ with respect to the p-adic metric. We know that such a completion exists and is unique (up to isomorphism) due to Theorem 3.4.

Remark 3.6. We note that due to Ostrowski's Theorem, the real numbers and the p-adic numbers are the only completions of the rational numbers.

We have now constructed $\mathbb{Q}_p$ analytically and can construct $\mathbb{Z}_p$ from it. Before defining $\mathbb{Z}_p$, we note that an algebraic construction also exists, in which $\mathbb{Z}_p$ is constructed first and then $\mathbb{Q}_p$ is constructed as its field of fractions. We leave this alternate construction for the reader to explore.

Definition 3.7. Let the *ring of p-adic integers*, $\mathbb{Z}_p$, be defined as follows:

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

Remark 3.8. We note that for all $x \in \mathbb{Z}$, $v_p(x) \geq 0$, so $|x|_p \leq 1$. Thus, $\mathbb{Z} \subset \mathbb{Z}_p$ (just as $\mathbb{Q} \subset \mathbb{Q}_p$).

Before moving on, we note, without proof, that $\mathbb{Z}_p$ is also the completion of $\mathbb{Z}$ with respect to the p-adic metric (see [10]). Under the standard metric, $\mathbb{Z}$ is already complete, as the only Cauchy sequences in $\mathbb{Z}$ are constant sequences. This is because every integer is a distance of at least one away from another integer. However, under the p-adic metric, integers can get arbitrarily close to each other, so there are nontrivial Cauchy sequences. We will see an example of such a sequence in Section 4 (Example 4.4).

4. Sequences and Series in $\mathbb{Q}_p$

In this section, we will take a further look at sequences and series in $\mathbb{Q}_p$. We will see that they are often easier to work with than sequences and series in $\mathbb{R}$. Because $\mathbb{Q}_p$ is an ultrametric space, we can obtain some nice results that only apply partially in $\mathbb{R}$.

Theorem 4.1. *Let (a_n) be a sequence in $\mathbb{Q}_p$. Then (a_n) is Cauchy if and only if for every $\epsilon > 0$, there is some $N \in \mathbb{N}$ such that for all $n \geq N$, $|a_{n+1} - a_n|_p < \epsilon$.*

Proof. First, we assume that (a_n) is Cauchy. Let $\epsilon > 0$. By Definition 3.1, there is some $N \in \mathbb{N}$ such that for all $m, n \geq N$, $|a_n - a_m|_p < \epsilon$. Let $n \geq N$. Then $n + 1 \geq N$, so $|a_{n+1} - a_n|_p < \epsilon$.

Next, we assume that for every $\epsilon > 0$, there is some $N \in \mathbb{N}$ such that for all $n \geq N$, $|a_{n+1} - a_n|_p < \epsilon$. Let $\epsilon > 0$. Then there is some $N \in \mathbb{N}$ such that

$$\text{for all } n \geq N,\ |a_{n+1} - a_n|_p < \epsilon.$$

Let $m, n \geq N$. If $n = m$, $|a_n - a_m|_p = |0|_p = 0 < \epsilon$, so we consider the case that $m \neq n$. Without loss of generality, we assume that $n > m$. Then $n = m + k$ for some $k \in \mathbb{N}$. We can rewrite $|a_n - a_m|_p$ as

$$|(a_{m+k} - a_{m+k-1}) + (a_{m+k-1} - a_{m+k-2}) + \ldots + (a_{m+1} - a_m)|_p.$$

Since the p-adic absolute value is non-Archimedean,

$$|a_n - a_m|_p \leq \max\{|a_{m+i} - a_{m+i-1}|_p \mid 1 \leq i \leq k\} \text{ (Definition 2.1(iv))}.$$

For some $1 \leq i_0 \leq k$,

$$|a_{m+i_0} - a_{m+i_0-1}|_p = \max\{|a_{m+i} - a_{m+i-1}|_p \mid 1 \leq i \leq k\}.$$

Then $|a_n - a_m|_p \leq |a_{m+i_0} - a_{m+i_0-1}|_p$. We recall that $m \geq N$, so by our assumption,

$$|a_{m+i_0} - a_{m+i_0-1}|_p < \epsilon.$$

Hence, $|a_n - a_m|_p < \epsilon$ by transitivity. Therefore, (a_n) is Cauchy (Definition 3.1). □

Corollary 4.2. *Let (a_n) be a sequence in $\mathbb{Q}_p$. Then $\sum_{n=0}^{\infty} a_n$ converges if and only if $\lim_{n\to\infty} a_n = 0$.*

Proof. Let (p_n) be the sequence of partial sums for (a_n).

First, we assume that $\sum_{n=0}^{\infty} a_n$ converges. Then (p_n) converges. It follows that (p_n) is Cauchy. Let $\epsilon > 0$. By Theorem 4.1, there is some $N \in \mathbb{N}$ such that for all $n \geq N$, $|p_{n+1} - p_n|_p < \epsilon$. Equivalently, $|a_{n+1}|_p < \epsilon$ for all $n \geq N$. Let $N' = N + 1$. Then for all $n \geq N'$, $|a_n|_p < \epsilon$.

Next, we assume that $\lim_{n\to\infty} a_n = 0$. Then there is some $N \in \mathbb{N}$ such that for all $n \geq N$, $|a_n|_p < \epsilon$. Then also, $|a_{n+1}|_p < \epsilon$ for all $n \geq N$. Equivalently, $|p_{n+1} - p_n|_p < \epsilon$ for all $n \geq N$. By Theorem 4.1, (p_n) is Cauchy and therefore converges. Hence, $\sum_{n=0}^{\infty} a_n$ converges. □

Remark 4.3. We recall that Theorem 4.1 and Corollary 4.2 are only true in the forward direction in $\mathbb{R}$. In particular, the harmonic series is a well-known counterexample for the other direction. The harmonic sequence's terms get arbitrarily close to 0, but the corresponding series diverges.

Example 4.4. The p-adic series $\sum_{n=0}^{\infty} p^n$ converges, and its sum is $\frac{1}{1-p}$.

Proof. Let (a_n) be the sequence of partial sums for $\sum_{n=0}^{\infty} p^n$. Then for all $n \in \mathbb{N} \cup \{0\}$, $a_n = \sum_{i=0}^{n-1} p^i$. We recall the algebraic fact that $1^n - p^n = (1-p)\sum_{i=0}^{n-1} p^i$. Equivalently, $a_n = \sum_{i=0}^{n-1} p^i = \frac{1-p^n}{1-p}$. We note that $\lim_{n\to\infty} \frac{1}{1-p} = \frac{1}{1-p}$ and $\lim_{n\to\infty} p^n = 0$ (Exercise 2.15). By the algebra of limits,

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} \frac{1}{1-p} - \lim_{n\to\infty} p^n \cdot \lim_{n\to\infty} \frac{1}{1-p} = \frac{1}{1-p} - 0 = \frac{1}{1-p}.$$

Therefore, $\sum_{n=0}^{\infty} p^n = \frac{1}{1-p}$. □

Remark 4.5. This result is analogous to the formula for the sum of a geometric series in $\mathbb{R}$. The result in $\mathbb{R}$ holds for all $x \in \mathbb{R}$ where $|x| < 1$. Similarly, we could extend this result to hold for all $x \in \mathbb{Q}_p$ where $|x|_p < 1$, rather than only for $x = p$. We leave this as an exercise for the reader.

5. p-adic Expansions

Using the formula in Example 4.4, we can obtain some fairly counterintuitive results. For example, in $\mathbb{Q}_2$, $-1 = 1 + 2 + 4 + \cdots$. We aim to make sense of these results and think about p-adic numbers more concretely by introducing the idea of a p-adic expansion. First, we state the following proposition.

Proposition 5.1. *Any series in the form* $\sum_{n=n_0}^{\infty} a_n p^n$, *with* $a_n \in \{0, 1, \cdots p-1\}$ *and* $n_0 \in \mathbb{Z}$, *converges in* $\mathbb{Q}_p$.

Proof. We recall from Example 2.15 that $\lim_{n\to\infty} p^n = 0$. We suppose that $0 \leq a_n < p$ for all $n \geq n_0$. It follows that $\lim_{n\to\infty} a_n p^n = 0$ as well. By Corollary 4.2, $\sum_{n=n_0}^{\infty} a_n p^n$ converges in $\mathbb{Q}_p$ (the starting index being n_0 rather than 0 does not make a difference to whether the series converges). □

Now that we know that any series in this form converges p-adically, we can define the p-adic expansion.

Definition 5.2. The *p-adic expansion* of a number $\alpha \in \mathbb{Q}_p$ is a series in the form

$$\alpha = \sum_{n=n_0}^{\infty} a_n p^n,$$

where $n_0 \in \mathbb{Z} \cup \{\infty\}$, $a_{n_0} \neq 0$, and $0 \leq a_n < p$ for all $n \geq n_0$.

We call the integers a_n the *coefficients* of the expansion.

Remark 5.3. When $\alpha \in \mathbb{N}$, the p-adic expansion of α is the same as the base p representation of α (where there exists some $N \in \mathbb{N}$ such that the coefficients $a_n = 0$ for all $n \geq N$).

Proposition 5.4. *Every p-adic number has a unique p-adic expansion.*

Proof. See [3, p. 82-83]. □

Exercise 5.5. Let $\alpha \in \mathbb{Q}$, and let $\sum_{n=n_0}^{\infty} a_n p^n$ be the p-adic expansion of α. Show that $v_p(\alpha) = n_0$ (we note that for elements of $\mathbb{Q}_p \setminus \mathbb{Q}$, the p-adic valuation is defined this way).

Remark 5.6. We can write p-adic expansions in the same way that we write standard decimal representations of numbers. However, in a p-adic expansion, there are a finite number of negative powers of p, as opposed to a finite number of positive powers of 10. Thus, if we write a p-adic expansion in the usual way, where the powers of p decrease from left to right, the coefficients often extend infinitely to the left.

Examples 5.7. Written in the form described in Remark 5.6, $-1 = \overline{1}_2$, $175 = 1200_5$, and $\frac{194}{7} = 36.5_7$ (subscripts are used to specify the prime).

Before moving on, we go back to our statement that in $\mathbb{Q}_2$, $-1 = 1+2+4+\cdots$. We can make sense of this by adding 1 as follows:

$$\begin{aligned} 1+(-1) &= 1+2^0+2^1+2^2+\cdots \\ \iff 0 &= 0\cdot 2^0+2^1+2^1+2^2+\cdots \\ &= 0\cdot 2^0+0\cdot 2^1+2^2+2^2+\cdots \\ &= 0\cdot 2^0+0\cdot 2^1+0\cdot 2^2+\cdots . \end{aligned}$$

If we continue, every coefficient in the expansion would eventually become 0, making it easier to believe that this series does in fact represent the additive inverse of 1.

Next, in order to help us compute p-adic expansions, we introduce the following lemma.

Lemma 5.8. *Let $\alpha \in \mathbb{Z}_p$ with p-adic expansion $\sum_{n=n_0}^{\infty} a_n p^n$, and let $k \in \mathbb{N}$. Then $\alpha \equiv \sum_{n=n_0}^{k-1} a_n p^n \pmod{p^k}$.*

Proof. We begin with $\alpha \equiv \sum_{n=n_0}^{\infty} a_n p^n \pmod{p^k}$. Also, $\sum_{n=k}^{\infty} a_n p^n \equiv 0 \pmod{p^k}$ since for all $m \geq k$, $p^k \mid p^m$. Lastly, we subtract to obtain $\alpha \equiv \sum_{n=n_0}^{k-1} a_n p^n \pmod{p^k}$. □

Example 5.9. Determine the 5-adic expansion of $\frac{4}{3}$.

Proof. Since $v_p\left(\frac{4}{3}\right) = 0$, $\frac{4}{3} = \sum_{n=0}^{\infty} a_n 5^n$, where $0 \leq a_n \leq 4$ (Definition 5.2 and Exercise 5.5). Also, since $\left|\frac{4}{3}\right|_p = 1$, $\frac{4}{3}$ is a 5-adic integer. By Lemma 5.8, $\frac{4}{3} \equiv a_0 \pmod 5$. Then $4 \equiv 3a_0 \pmod 5$. We multiply by 2 to obtain $a_0 \equiv 3 \pmod 5$. Since $0 \leq a_n \leq 4$, $a_0 = 3$ as well. Next, by Lemma 5.8, $\frac{4}{3} \equiv a_0 + 5a_1 \pmod{25}$. We solve this congruence as follows:

$$\begin{aligned} 4 &\equiv 3a_0+15a_1 \pmod{25} \\ \implies 4 &\equiv 3\cdot 3+15a_1 \pmod{25} \\ \implies 20 &\equiv 15a_1 \pmod{25} \\ \implies 3a_1 &\equiv 4 \pmod 5. \\ \implies a_1 &\equiv 3 \pmod 5. \end{aligned}$$

As before, $a_1 = 3$ as well. Using similar methods, we can solve $\frac{4}{3} \equiv a_0 + 5a_1 + 25a_2 \pmod{125}$ to obtain $a_2 = 1$. After this, the pattern repeats, alternating between 3 and 1. Written in way described by Remark 5.6, the 5-adic expansion of $\frac{4}{3}$ is $\overline{13}3_5$.

We can check this by multiplying by 3 as follows:

$$\begin{aligned} \frac{4}{3} &= 3 \cdot 5^0 + 3 \cdot 5^1 + 1 \cdot 5^2 + \cdots \\ \implies 4 &= 9 \cdot 5^0 + 9 \cdot 5^1 + 3 \cdot 5^2 + \cdots \\ &= 4 \cdot 5^0 + 5^1 + 4 \cdot 5^1 + 5^2 + 3 \cdot 5^2 + \cdots \\ &= 4 \cdot 5^0 + 0 \cdot 5^1 + 5^2 + 5^2 + 3 \cdot 5^2 + \cdots \\ &= 4 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + \cdots . \end{aligned}$$

Every non-zero power of 5 eventually vanishes, leaving only 4. Thus, $\frac{4}{3} \cdot 3 = 4$, as we would expect. □

We saw in the previous example that a rational number had an eventually periodic p-adic expansion. It turns out that this is true in general, just as it is with decimal expansions in $\mathbb{R}$.

Theorem 5.10. *A p-adic number has an eventually periodic p-adic expansion if and only if it is rational.*

Proof. See [1, p. 3-5]. □

We can also define addition and multiplication for p-adic numbers using p-adic expansions. These definitions are similar to how we add and multiply the decimal representations of real numbers, as we add the coefficients and carry any remainders. The reader can see [7, p. 1-3] for more rigorous definitions of these operations. These definitions can also be used to verify that $\mathbb{Q}_p$ is a field and that $\mathbb{Z}_p$ is a commutative ring.

6. The Topology on $\mathbb{Q}_p$

In this section, we discuss the topology induced by the p-adic metric in an attempt to better visualize the p-adic numbers. While the real numbers can be visualized as a line, it is not as simple with the p-adics. In particular, there is an ordering on $\mathbb{R}$ but not on $\mathbb{Q}_p$. Moreover, $\mathbb{R}$ is connected, whereas $\mathbb{Q}_p$ is totally disconnected (this will be further explained and proven later). Before formalizing these details, we examine the image below as one way to visualize the 3-adic integers.

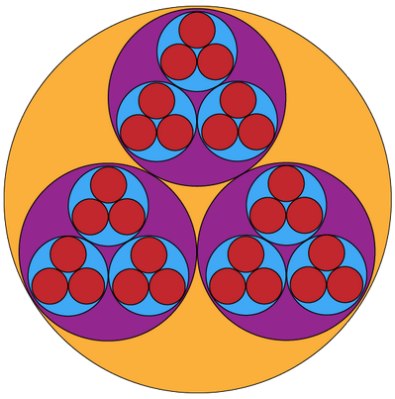

Figure 1. A visualization of the 3-adic integers ([6])

Each circle contains three main sub-circles. The integers within a subcircle of a given circle have a particular 3-adic distance from integers in another subcircle of that circle. For example, the orange circle has purple subcircles. The integers within a purple subcircle are a distance of one away from the integers in a different purple subcircle. The distance corresponding to the largest circle is one since one is the largest possible 3-adic distance between integers. While there are no circles larger than the orange one for $\mathbb{Z}_3$, the circles can get infinitely small, as we can choose numbers that differ by larger and larger powers of 3. In this way, the p-adic integers are not discrete even though they are disconnected. Hence, a good image of the p-adic integers would be fractal-like, as Figure 1 is.

We now proceed to introduce and prove several results about the topology induced by the p-adic metric.

Theorem 6.1. *In $\mathbb{Q}_p$, any open ball is also a closed ball (and vice versa).*

Proof. Let $B(a,r)$ be an open ball in $\mathbb{Q}_p$. Then $B(a,r) = \{x \in \mathbb{Q}_p \mid |x-a|_p < r\}$. Let n be the smallest integer such that $r \leq p^{-n}$. For the reason described in Remark 2.12, there are no p-adic numbers with absolute value between $p^{-(n+1)}$ and p^{-n}. Thus, $B(a,r) = \{x \in \mathbb{Q}_p \mid |x-a|_p < p^{-n}\} = \{x \in \mathbb{Q}_p \mid |x-a|_p \leq p^{-(n+1)}\}$. It follows that B is also a closed ball. A symmetric argument would show that any closed ball is also an open ball in $\mathbb{Q}_p$. □

Corollary 6.2. *The ring $\mathbb{Z}_p$ is both closed and open in $\mathbb{Q}_p$.*

Proof. We recall from Definition 3.7 that $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$. Thus, it is clear that $\mathbb{Z}_p$ is a closed ball and is therefore closed. By Theorem 6.1, $\mathbb{Z}_p$ is also an open ball and is therefore open (specifically, $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p < p\}$). It follows that $\mathbb{Z}_p$ is closed and open in $\mathbb{Q}_p$. □

Corollary 6.3. *The field $\mathbb{Q}_p$ is totally disconnected.*

Proof. Let a and b be distinct points in $\mathbb{Q}_p$. Let $\delta = |a-b|_p$. Let $A = \{x \in \mathbb{Q}_p \mid |x-a|_p < \delta\}$. Then A is an open ball in $\mathbb{Q}_p$, and $a \in A$. For the same reason that $\mathbb{Z}_p$ is both closed and open, A is both closed and open. Therefore, $B := \mathbb{Q}_p \setminus A$ is also both closed and open. Since $|b-a|_p = \delta$, $b \notin A$. Thus, $b \in B$. Since $\mathbb{Q}_p = A \cup B$, where A and B are disjoint open sets with $a \in A$ and $b \in B$, $\mathbb{Q}_p$ is totally disconnected. □

Theorem 6.4. *The ring $\mathbb{Z}_p$ is compact.*

Proof. We recall that a metric space is compact if and only if it is sequentially compact. Thus, we aim to show that $\mathbb{Z}_p$ is sequentially compact using a diagonalization argument.

Let $(\alpha_n)_{n=0}^{\infty}$ be a sequence in $\mathbb{Z}_p$. For each $n \in \mathbb{N} \cup \{0\}$, $\alpha_n = \sum_{i=0}^{\infty} a_{n,i} p^i$, where $0 \leq a_{n,i} < p$. This is clear from Definition 5.2. For elements of $\mathbb{Z}_p$, the starting index of the p-adic expansion is greater than or equal 0, but we can obtain an equivalent sum starting at index 0 by adding 0-terms to the beginning. By the Pigeonhole Principle, there exists $b_0 \in \mathbb{N} \cup \{0\}$ such that $0 \leq b_0 \leq p-1$ and $b_0 = a_{n,0}$ for infinitely many n. We construct a subsequence (α_{0n}) of (α_n), where (α_{0n}) consists of the elements of (α_n) for which $a_{n,0} = b_0$. We now inductively construct a sequence of subsequences. For each $k \in \mathbb{N}$, we will construct a sequence

(α_{kn}) that is a subsequence of $(\alpha_{(k-1)n})$. Let $k \in \mathbb{N}$. Then as before, there exists $b_k \in \mathbb{N} \cup \{0\}$ such that $0 \leq b_k \leq p-1$ and $b_k = a_{n,k}$ for infinitely many n where $\alpha_n = \sum_{i=0}^{\infty} a_{n,i}p^i \in (\alpha_{(k-1)n})$. We note that we have added an additional assumption so that we are not selecting elements of (α_n) that were not present in $(\alpha_{(k-1)n})$. Now, let (α_{kn}) be the subsequence of $(\alpha_{(k-1)n})$ that consists of every element for which $a_{n,k} = b_k$. Let $\beta = \sum_{i=0}^{\infty} b_i p^i$ (so $\beta \in \mathbb{Z}_p$). Then for each $k \in \mathbb{N} \cup \{0\}$, the first $k+1$ coefficients in the p-adic expansion of every element of (α_{kn}) match the first $k+1$ coefficients in the p-adic expansion of β. We finally consider the diagonal subsequence (α_{kk}). This sequence converges to β by construction. Since (α_{kk}) is a convergent subsequence of (α_n), any sequence in $\mathbb{Z}_p$ must contain a convergent subsequence. Hence, $\mathbb{Z}_p$ is sequentially compact and is therefore compact. □

Corollary 6.5. *The field $\mathbb{Q}_p$ is locally compact.*

Proof. Let $x \in \mathbb{Q}_p$. Let $X = \{x + y \mid y \in \mathbb{Z}_p\}$. Since $\mathbb{Z}_p$ is compact (by Theorem 6.4), X is compact as well. Just as $\mathbb{Z}_p$ is a ball centered at 0, X is a ball centered at x. Thus, X is a compact neighborhood of x, and $\mathbb{Q}_p$ is locally compact. □

7. Geometry in $\mathbb{Q}_p$

We close by proving several interesting geometric results that hold in $\mathbb{Q}_p$.

Theorem 7.1. *In $\mathbb{Q}_p$, all triangles are isosceles.*

Proof. Let a, b, and c be distinct points in $\mathbb{Q}_p$. Then $d_p(a,b), d_p(b,c)$, and $d_p(a,c)$ are the lengths of the sides of the triangle determined by those points. If $d_p(a,b) = d_p(b,c)$, the triangle is isosceles. If $d_p(a,b) \neq d_p(b,c)$, $|a-b|_p \neq |b-c|_p$. We note that $(a-b)+(b-c) = a-c$. By Lemma 2.4, $|a-c|_p = \max\{|a-b|_p, |b-c|_p\}$. In other words, either $d_p(a,c) = d_p(a,b)$ or $d_p(a,c) = d_p(b,c)$. Hence, the triangle is isosceles. □

Remark 7.2. We note also that if a triangle in $\mathbb{Q}_p$ is not equilateral, its shortest side is the base of the triangle. This comes from the fact that the maximum function was used to find the two congruent sides.

We note that we did not specify that the points of our triangle were not collinear. We see now that this cannot occur.

Corollary 7.3. *No three distinct points in $\mathbb{Q}_p$ are collinear.*

Proof. We assume, for the sake of contradiction, that there are distinct points a, b, and c that are collinear. Without loss of generality, we assume that $d_p(a,c) = d_p(a,b) + d_p(b,c)$. Then $d_p(a,c) > d_p(a,b)$ and $d_p(a,c) > d(b,c)$ (since $d_p(a,b) > 0$ and $d_p(b,c) > 0$). Since $\overline{ac}$ is the longest segment, it follows from Theorem 7.1 and Remark 7.2 that $\overline{ac}$ is a leg of the isosceles triangle formed by the three points. However, that means $d_p(a,c) = d_p(a,b)$ or $d_p(a,c) = d_p(b,c)$. In either case, we have reached a contradiction. Thus, there are no three distinct points in $\mathbb{Q}_p$ that are collinear. □

We now introduce another corollary.

Corollary 7.4. *There are no right triangles in $\mathbb{Q}_p$.*

Proof. We assume, for the sake of contradiction, that there exist points $a, b, c \in \mathbb{Q}_p$ such that $\triangle abc$ is a right triangle. In other words, the side lengths of the triangle satisfy the Pythagorean Theorem. Without loss of generality, we assume $d_p(a,c)^2 = d_p(a,b)^2 + d_p(b,c)^2$. Then $d_p(a,c) > d_p(a,b)$ and $d_p(a,c) > d_p(b,c)$. Since every triangle in $\mathbb{Q}_p$ is isosceles by Theorem 7.1, $d_p(a,b) = d_p(b,c)$. Hence, we have a triangle in which the base is the longest side. This contradicts Remark 7.2. Therefore, there are no right triangles in $\mathbb{Q}_p$. □

Lastly, we introduce a final theorem.

Theorem 7.5. *At most p distinct points in $\mathbb{Q}_p$ are equidistant from each other.*

Proof. We assume, for the sake of contradiction, that there exist at least $p+1$ distinct points in $\mathbb{Q}_p$ that are all equidistant from each other: $a_1, a_2, \ldots, a_{p+1}$. Let $i, j \in \mathbb{N}$ be such that $1 \leq i, j \leq p+1$ and $i \neq j$. Since the points are distinct, $d_p(a_i, a_j) \neq 0$. It follows from Definition 2.1(i) and Definition 2.11 that $|a_i - a_j|_p = p^{-v_p(a_i - a_j)}$. Let $v_p(a_i - a_j) = m$. Since $a_i, a_j \in \mathbb{Q}_p$, a_i and a_j have p-adic expansions. By Definition 5.2, $a_i = \sum_{n=n_{0i}}^{\infty} a_{i,n}p^n$, where $n_{0i} \in \mathbb{Z}$, $a_{i,n_{0i}} \neq 0$, and $0 \leq a_{i,n} < p$ for all n. Similarly, $a_j = \sum_{n=n_{0j}}^{\infty} a_{j,n}p^n$, where $n_{0j} \in \mathbb{Z}$, $a_{j,n_{0j}} \neq 0$ and $0 \leq a_{j,n} < p$ for all n. We note that $p^m \mid (a_i - a_j)$. It follows that for any $k < m$, $a_{i,k} = a_{j,k}$. Therefore, we can rewrite the difference as follows:

$$\begin{aligned} a_i - a_j &= \sum_{n=n_{0i}}^{\infty} a_{i,n}p^n - \sum_{n=n_{0j}}^{\infty} a_{j,n}p^n \\ &= \sum_{n=m}^{\infty} a_{i,n}p^n - \sum_{n=m}^{\infty} a_{j,n}p^n \\ &= \sum_{n=0}^{\infty} a_{i,n+m}p^{n+m} - \sum_{n=0}^{\infty} a_{j,n+m}p^{n+m} \\ &= p^m \sum_{n=0}^{\infty} a_{i,n+m}p^n - p^m \sum_{n=0}^{\infty} a_{j,n+m}p^n. \end{aligned}$$

Now, let $a_i' = \sum_{n=0}^{\infty} a_{i,n+m}p^n$, and let $a_j' = \sum_{n=0}^{\infty} a_{j,n+m}p^n$. Then we have

$$a_i - a_j = p^m(a_i' - a_j').$$

Since $v_p(a_i - a_j) = m$,

$$v_p(p^m(a_i' - a_j')) = m.$$

By Lemma 2.10(i),

$$v_p(p^m(a_i' - a_j')) = v_p(p^m) + v_p(a_i' - a_j') = m + v_p(a_i' - a_j').$$

Therefore, $v_p(a_i' - a_j') = 0$. Since i and j were arbitrary, we can construct a_i' and a_j' for all $1 \leq i, j \leq p+1$ where $i \neq j$. In each case, $v_p(a_i' - a_j') = 0$. However, since there are $p+1$ points and only p possible values for the coefficients in the p-adic

expansions, there exist distinct $1 \leq i_0, j_0 \leq p+1$ such that $a_{i_0,m} = a_{j_0,m}$ (by the Pigeonhole Principle). Then $p \mid (a'_{i_0} - a'_{j_0})$, so $v_p(a'_{i_0} - a'_{j_0}) \neq 0$. Hence, we have reached a contradiction, so our assumption must be false. There are no more than p points that are all equidistant from each other. □

Remark 7.6. This theorem helps capture the notion that it is easier for points to be equidistant p-adically. We leave verification that p points can be equidistant from each other in $\mathbb{Q}_p$ as an exercise to the reader. By contrast, in $\mathbb{R}$, at most 3 points can all be equidistant from each other. Because the options for the distance between points are more limited in $\mathbb{Q}_p$, up to p points can be equidistant (in every case except $\mathbb{Q}_2$, this is more than 3).

Acknowledgments

It is my pleasure to thank my mentors, Iris Yunxuan Li and Cindy Tan. When I was overwhelmed by all the possible topics, they both helped me narrow down my interests and suggested sources for me to look at. Although I did not end up using most of the topics they showed me, I enjoyed being exposed to different topics by them. I'd also like to thank Iris in particular for helping me so much with writing this paper. Her feedback was truly invaluable. Thank you to Professor Rudenko for leading the Apprentice Program and making lectures and problem sets that introduced me to a lot of cool topics. Lastly, thank you to Dr. Peter May for all the time and effort he put into directing the REU, especially in these difficult circumstances. I really appreciate that I could still spend much of my summer doing math despite the unfortunate fact that it had to be remote.

References

[1] Keith Conrad. The p-adic Expansion of Rational Numbers. https://kconrad.math.uconn.edu/blurbs/gradnumthy/rationalsinQp.pdf
[2] Catherine Crompton. Some Geometry of the p-adic Rationals. https://scholar.rose-hulman.edu/cgi/viewcontent.cgi?article=1183&context=rhumj
[3] Fernando Q. Gouvêa. p-adic Numbers: An Introduction. Springer. 1997.
[4] https://www.cut-the-knot.org/blue/p-adicNumbers.shtml
[5] http://www.cut-the-knot.org/blue/p-adicExpansion.shtml
[6] Evelyn Lamb. The Numbers behind a Fields Medalist's Math. https://blogs.scientificamerican.com/roots-of-unity/the-numbers-behind-a-fields-medalists-math/
[7] David A. Madore. A first introduction to p-adic numbers. http://www.madore.org/ david/math/padics.pdf
[8] Eric Rozon. Quadratic forms over the p-adic fields: a classification problem. https://mysite.science.uottawa.ca/mnevins/papers/EricRozonThesis.pdf
[9] Michael Stoll. p-adic Analysis in Arithmetic Geometry. http://www.mathe2.uni-bayreuth.de/stoll/teaching/pAdicAnalysis-WS2015/Skript-pAdicAnalysis-pub-screen.pdf
[10] Scott Zinzer. Euclidean Models of the p-adic Integers. https://math.la.asu.edu/ paupert/Zinzerproject.pdf