Introduction to the p-adic Numbers

Sean Fox

October 24, 2016

Abstract

Let p be any prime number and x be a rational number. We denote by $|x|_p$ the highest power of p that divides x. We show that $|x|_p$ is a norm on $\mathbb{Q}$ and that $\mathbb{Q}$ can be completed with respect to this norm to form the p-adic numbers. We examine the basic analytic, algebraic, and topological properties and implications of the p-adic norm and p-adic numbers.

1 Introduction

In most applications of arithmetic, we write our numbers in base 10, otherwise known as the decimal system. This means that any integer in base 10 can be represented as a summation

$$\sum_{n=0}^{\infty} a_n 10^n = a_0 10^0 + a_1 10 + ... + a_{n-1} 10^{n-1} + a_n 10^n + ..., \quad a_n \in \mathbb{Z}_{10}$$

Furthermore, for any rational number, we can use negative numbers in the summation to get

$$\sum_{n=-\infty}^{\infty} a_n 10^n = ... + a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0 10^0 + a_{-1} 10^{-1} + ...$$

To give an example, we can expand the integer 532 as such:

$$532 = 5 * 10^2 + 3 * 10^1 + 2 * 10^0 = 5 * 100 + 3 * 10 + 2 * 1$$

In different studies, it can be useful to work in different bases. For example, computers make heavy use of the binary system (base 2) in order to perform computations. In number theory, the set of prime numbers are a significant area of study. Occasionally, it has become useful in parts of number theory to represent numbers in base p, where p is some fixed prime number.

These numbers in base-p are called p-adic numbers, and they were first described by Kurt Hensel in 1897 with earlier work by Ernst Kummer hinting at their existence when he proved cases of Fermat's Last Theorem for prime exponents. Hensel's motivation for describing the p-adic numbers came from the relationship between the integers and the polynomials with complex coefficients. It is known by the Fundamental Theorem of Algebra that any non-constant polynomial of one variable has at least one root in the set of complex numbers. What this means is that we can write a polynomial as such

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

where $a, \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{C}$. Furthermore, we know that this decomposition is unique. If this sounds familiar, it should. It is also well know by the Fundamental Theorem of Arithmetic that any integer can be written uniquely as a product of prime numbers. What all of this implies is that both the set of integers and set of polynomials of single variables are both factorable.

Hensel noticed this relationship, but he also noticed something more. Given a particular complex number α, we can write a polynomial $P(X)$ as a Taylor series from Calculus II.

$$P(X) = \sum_{i=0}^{n} a_i (X - \alpha)^i = \alpha_0 + \alpha_1 (X - \alpha) + \alpha_2 (X - \alpha)^2 + \dots + \alpha_n (X - \alpha)^n$$

Similarly, as we started to show earlier, integers can be expanded depending on a set base. Since integers are all uniquely factorable by prime numbers, we can set up something similar to a Taylor series expansion for a fixed prime number p and an integer m.

$$m = \sum_{i=0}^{n} a_i p^i = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n, \quad a_i \in \mathbb{Z} \text{ and } 0 \leq a_i \leq p-1$$

We recall from Calculus II that a Taylor series has a radius of convergence. That is, there exists some number R such that our expansion will only converge to a number if $|x - \alpha| < R$. This means that a Taylor series gives us information only in a local area around α. For example, we know that if $X = \alpha$, then our polynomial will vanish.

It turns out that a p-adic expansion (expanding an integer in base p) also gives us information local to our prime number p. But rather than a vanishing point, it tells us the divisibility of a number up to some order of p. For example, let's expand the number 72 with $p = 3$.

$$72 = 0 + 0 * 3 + 2 * 3^2 + 2 * 3^3$$

From looking at the expansion, we can easily see that 72 is divisible by $3^2 = 9$. Furthermore, it turns out that we can use the same line of reasoning for the rational numbers since they are the field of fractions of the integers - in other words, since any rational number can be represented as a fraction whose numerator and denominator are both integers. It was shown earlier that a rational number can be expanded if we include negative numbers for our index. So instead of the Taylor series expansion, we can compare the expansion of a rational number to a Laurent series from Intro to Complex Analysis.

It turns out that these numbers have found their place in many applications since their discovery. The p-adic numbers have their own type of calculus due to a special absolute value, they are currently being studied alongside elliptic curves in the area of cryptography, and they even have their own fields of study in quantum physics and complex dynamics. But one of the most basic uses is in number theory in which they allow us to easily solve equations modulo every power of a prime number p.

However, before we jump into uses of p-adic numbers, we need to have a few questions answered. For example, we know when a Taylor series and a Laurent series converge. But how do we know when the p-adic expansion of a number converges? When we write the p-adic expansion of a number, it makes sense that the sum of numbers in base p should converge if they are going to equal a number. The result is that, in p-adic numbers, p^n gets smaller as n grows. We will show why this is, but first, we have to talk about how we will measure the size of a p-adic number - with absolute values.

2 Absolute Values

2.1 Real Absolute Value

Before we dive into absolute values and valuations, we remind ourselves of the definition of a ring from Intro to Modern Algebra.

Definition (Rings)**.** A **ring** is a set of numbers R under two operations, usually denoted as + (addition) and * (multiplication), such that, for $a, b, c \in R$ it fulfills the following properties:

1. $a + b \in R$
2. $a * b \in R$
3. $(a + b) + c = a + (b + c)$
4. $(a * b) * c = a * (b * c)$
5. $a + b = b + a$
6. There exists an element $0_R \in R$ such that $a + 0_R = a = 0_R + a$ for all $a \in R$.
7. There exists an element $-a \in R$ such that $a + (-a) = 0_R = (-a) + a$ for all $a \in R$.

8. $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$

Furthermore, R is a **commutative ring** if

9. $a * b = b * a$ for all $a, b \in R$

R is a **ring with identity** if there exists an element $1_R \in R$ called the identity such that

10. $a * 1_R = a = 1_R * a \quad \forall\, a \in R$

R is an **integral domain** if it is a commutative ring with identity $1_R \neq 0_R$ that contains no zero divisors. That is,

11. $a * b = 0_R \Rightarrow a = 0_R$ or $b = 0_R$

And finally, R is a **field** if it is an integral domain such that,

12. For all $a \in R$, there exists $a^{-1} \in R$ where $a * a^{-1} = 1_R = a^{-1} * a$.

We will be dealing more with fields in depth after we formally construct the p-adic numbers. For now, we wanted to remind ourselves of the definition of a ring so that we can fully understand the definitions to come throughout this section. To actually understand how we will construct the p-adic numbers, we will have to go back to our years in middle school and generalize one of the more basic concepts of algebra.

Definition (Absolute Values)**.** Let K be a field and $a, b \in K$. Then an **absolute value** (also called a **norm**) is a mapping $|\cdot| : K \to \mathbb{R}_+$ with the properties

1. $|a| = 0$, if and only if $a = 0_K$
2. $|ab| = |a| * |b|$ for all $a, b \in K$
3. $|a + b| \leq |a| + |b|$

Specifically, $|\cdot|$ is called an **archimedian absolute value**. Instead of property 3 (known as the Triangle Inequality), if $|\cdot|$ has the property that

$$3'. \quad |a \pm b| \leq \max\{|a|, |b|\}$$

which is known as the Strong Triangle Inequality, then $|\cdot|$ is $\mathbf{non-archimedian}$.

The absolute value that we are probably most familiar with is defined below:

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases} \qquad \forall\, x \in K$$

This absolute value is used often, and it has several names. It has been called the real absolute value and the euclidean absolute value or euclidean norm. However, we are trying to generalize this concept and will be introducing several different types of absolute values. Because of this, it is common to distinguish this function in p-adic analysis and valuation theory by $|\cdot|_\infty$ and call it the absolute value at infinity. The reason for this is mostly notational, but it will become clear later. For the purposes of this paper, we will refer to it as the real absolute value.

Properties (Real Absolute Value)**.** Written below are some well-known properties of the real absolute value for the sake of later comparison.

1. $|0|_\infty = 0$
2. $|a|_\infty = |-a|_\infty = a > 0 \;\; \forall a \in \mathbb{R}$
3. $|a \pm b|_\infty \leq |a|_\infty + |b|_\infty$

4. $|ab|_\infty = |a|_\infty * |b|_\infty$

By comparing the real absolute value to our definition of a general absolute value, we can see that the real absolute value is an archimedean absolute value.

The real absolute value is often used to denote distances and magnitudes between numbers. If applied to a single number, the real absolute value gives the distance of the number from 0. It does not take much to extend that idea to other absolute values as well. For example, if we extend the real absolute value from the real numbers to the complex numbers, which is referred to as the modulus, we get the distance of a number from the origin.

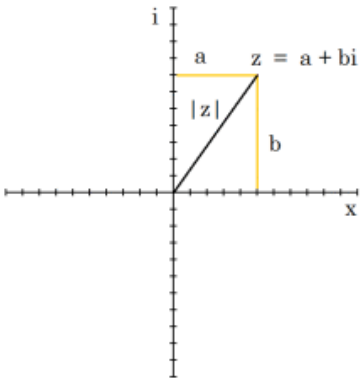

Figure 1: The modulus of the complex number z represented by $|z|$.

To further our understanding of absolute values, we will cover the most basic of absolute values: the trivial absolute value.

Definition (Trivial Absolute Value)**.** Let K be a field. $|\cdot| : K \to \mathbb{R}$ is the trivial absolute value defined by

$$|x| = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases} \qquad \forall\, x \in K$$

The real absolute value and the modulus are both examples of archimedean absolute values. That is, they only satisfy the triangle inequality. The trivial absolute value, however, is a non-archimedean absolute value because it satisfies the strong triangle inequality as shown below.

Theorem. The trivial absolute value is non-archimedean.

Proof. Let K be any field, $x, y \in K$, and let $|\cdot|$ be the trivial absolute value.

1. Suppose that $x, y \neq 0_K$, the additive identity of K. If $x \pm y \neq 0_K$, it follows that
$$|x \pm y| = 1 \Rightarrow |x \pm y| = \max\{|x|, |y|\}$$
2. Suppose that $x, y \neq 0_K$. If $x \pm y = 0_K$, it follows that
$$x \pm y = 0_K \Rightarrow 0 = |x \pm y| < \max\{|x|, |y|\} = 1$$
3. Suppose that $x, y = 0_K$. It follows that
$$|x \pm y| = 0 = \max\{|x|, |y|\}$$
Therefore, for all $x, y \in K$, $|x \pm y| \leq \max\{|x|, |y|\}$ which means the trivial absolute value satisfies the strong archimedean equality and is a non-archemedian absolute value.

□

As a side note, one other interesting fact about the trivial absolute value is that it is the only absolute value that can be applied to a finite field.

Theorem. The only absolute value on a field with finitely many elements is the trivial absolute value.

Proof. Let K be a finite field. As K is a field, K contains the identity elements $0_K, 1_K$. Let $|\cdot|$ be an arbitrary absolute value on K. Clearly by definition of absolute value, $|0_k| = 0$. Since 1_K is the multiplicative identity, $1_K = 1_K * 1_K \Rightarrow |1_K| = |1_K * 1_K| \leq |1_k| * |1_K|$. Since $|1_K| > 0$, it follows that $|1_k| = 1$. Now let $x \in K,\ x \neq 0_K$. Because K is finite, there exists some integer n such that $x^n = x$ (we can let n be the number of elements in K). By taking the absolute value of both sides, we have $|x^n| = |x|^n = |x|$. Since $|x| > 0$, then the only solution is that $|x|^n = |x| = 1$. Therefore, $|\cdot|$ on a finite field K can only be the trivial absolute value. □

2.2 P-adic Absoute Value

The trivial absolute value is not the only non-archimedean absolute value. There is one more significant non-archimedean absolute value that we will discuss that will be the foundation of building the field of p-adic numbers. However, we must first define the p-adic valuation.

Definition (Valuation)**.** A **valuation** on a field K is a real-valued function on $K\backslash\{0\}$ satisfying:

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

Definition (p-adic Valuation)**.** Let p be a fixed prime in $\mathbb{Z}$. The $\mathbf{p-adic\ valuation}$ on $\mathbb{Z}$ is the function $v_p : \mathbb{Z}\backslash\{0\} \to \mathbb{R}$ defined as follows: for each nonzero $n \in \mathbb{Z}$, let v_p be the unique positive integer satisfying

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

Furthermore, we extend v_p to the field of rational numbers as such: if $\frac{a}{b} = x \in \mathbb{Q}^x$, then

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

By convention, we let $v_p(0) = +\infty$. We can see why if we plug in the values into our definition.

$$0 = p^{v_p(0)}n' \Rightarrow p^{v_p(0)} \big| 0 \Rightarrow p^{\infty} | 0$$

As we can see, any prime number will divide 0 infinitely many times. This choice will also make a lot of things easier when we form the p-adic absolute value. Furthermore, the definition of the p-adic valuation can be extended to the rational numbers such that for $x \in \mathbb{Q}^x$ by $x = p^{v_p(x)}\frac{a}{b}$ where $p \nmid ab$. We also have the following trick to help when computing the p-adic valuation of a rational number.

Theorem. For any $x \in \mathbb{Q}^x$, the value of $v_p(x)$ does not depend on the representation of x. In other words, if $x = \frac{a}{b} = \frac{c}{d}$, then $v_p(a) - v_p(b) = v_p(c) - v_p(d)$.

To help make all of this clear, we will compute $v_5(400)$ and $v_3(\frac{123}{48})$.

a) $v_5(400):\ \ 400 = 5^{v_5(400)} * n \Rightarrow 5^{v_5(400)} = \frac{400}{n} \Rightarrow 5^2 = \frac{400}{16} \Rightarrow v_5(400) = 2$

b) $v_3\left(\frac{123}{48}\right) = v_3\left(\frac{41}{16}\right) = v_3(41) - v_3(16)$
$41 = 3^{v_3(41)}n_1 \Rightarrow 41 = 3^0 * 41 \Rightarrow v_3(41) = 0$
$16 = 3^{v_3(16)}n_2 = 3^0 * 16 \Rightarrow v_3(16) = 0$
$v_3\left(\frac{41}{16}\right) = 0 - 0 = 0$

It turns out that valuations and absolute values are very similar. They both are generalized functions that allow us to measure various things. With absolute values, it turns out be distance. For valuations, it turns out to be divisibility and multiplicity. But if we look closer, the similarities are what we will use to construct an absolute value for the p-adic numbers.

After looking at the above examples and the definition for the p-adic valuation, it is clear that another way to think of the p-adic valuation is that it answers the question of how divisible a number x is by a

prime number p. A large value for $v_p(x)$ means that x is highly divisible by p, and the opposite is true for small values of $v_p(x)$. In a way, the p-adic valuation measures a different kind of magnitude.

As the p-adic valuation is a valuation, it satisfies the properties that are in the valuation definition. We wish to now compare those properties to 2. and 3. in the definition of absolute value. They are listed below:

Valuation	Absolute Value
1. $v(xy) = v(x) + v(y)$	2. $\|xy\| = \|x\| * \|y\|$
2. $v(x+y) \geq \min\{v(x), v(y)\}$	3. $\|x+y\| \leq \|x\| + \|y\|$

Since the p-adic valuation measures a magnitude of divisibility by a prime number p, we can make our valuation act as an absolute value by changing the direction of the sign in the second valuation property. This is done by multiplying both sides of the inequality by -1. Also, if we make our valuation an exponent to some base number, we can fulfill the first property of a valuation and the second property of an absolute value. After manipulating the definition for the p-adic valuation with these in mind, we get the p-adic absolute value.

Definition (p-adic Absolute Value)**.** For any $x \in \mathbb{Q}$, we define the $\mathbf{p-adic\ absolute\ value}$ or $\mathbf{p-adic\ norm}$ of x by

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

The p-adic absolute value has an interesting definition, so there are a few things worth noting. First, we can finally see why we made sure to set the convention that $v_p(0) = +\infty$. When this is the case,

$$|0|_p = p^{-v_p(0)} = p^{-(+\infty)} = \frac{1}{p^{\infty}} = 0$$

Thus, we have a reason to say that $|0|_p = 0$ which follows from our definition of an absolute value. It is also worth nothing that, for integers, $|x|_p \leq 1$ for all $x \in \mathbb{Z}$. This may not necessarily be the case for rational numbers, but we will talk about these results later.

As we hinted at earlier, the p-adic absolute value is non-archimedean. This has some unique properties when actually applied to different numbers, but this may be easier to appreciate if we first show some examples of how to take the p-adic absolute value of some numbers. This will become a lot easier, and more compact to write, if we make use of the following theorem from Number Theory.

Theorem (The Fundamental Theorem of Arithmetic)**.** Every integer greater than 1 is either prime itself or can be uniquely, up the order of factors, represented as a product of primes.

For example, $24 = 2^3 * 3$ and $39 = 3 * 13$. We can also see that any rational number can be expressed as a product of primes if it is represented as a fraction of integers. Observe that $\frac{39}{8} = 3 * 13 * 2^{-3}$. With this in mind, we can decompose any rational number into its prime factorization to find the p-adic absolute value for any prime number p.

Consider the number $\frac{63}{550}$. It's prime factorization can be written as $\frac{63}{550} = 2^{-1} * 3^2 * 5^{-2} * 7 * 11^{-1}$. We then write the p-adic absolute value to be

$$\left|\frac{63}{550}\right|_p = \begin{cases} 2 & p = 2 \\ \frac{1}{9} & p = 3 \\ 25 & p = 5 \\ \frac{1}{7} & p = 7 \\ 11 & p = 11 \\ 1 & \text{All other primes} \end{cases}$$

Normally p would be a fixed prime, but we considered all p's in the above example not only to show several examples, but to also notice a pattern. The number $\frac{63}{550}$ is very divisible by 3 and 7 if we look

at the prime factorization. We can also see that our number is not very divisible by 2, 5, or 11. But if we look at out p-adic absolute values, we can see that the more divisible that a number is by a prime p, the smaller its p-adic absolute value will be. Our smallest value ends up being the 3-adic absolute value while the largest one is the 5-adic absolute value.

This time, let's compare the p-adic absolute value for two numbers with a fixed p, say $p = 3$. Let's compare the numbers 82 and 1. If we use the real absolute value to analyze the difference, we see that $|82 - 1|_\infty = 81$ which tells us that the two numbers are far apart on the real number line. However, if we use the p-adic absolute value with $p = 3$, we get

$$|82 - 1|_3 = |81|_3 = 3^{-v_3(81)} = 3^{-4} = \frac{1}{81}$$

If we use the p-adic absolute value to denote distance as we do with the real absolute value, we can see that 1 and 82, which are far apart in the real numbers, are close together in the 3-adic number system because their difference, 81, is divisible by 3. We will be dealing more with these implications when we discuss metrics.

3 Completing $\mathbb{Q}$

3.1 The Real Numbers

Now that we have introduced the p-adic absolute value, we have answered our question of convergence. Because of the p-adic absolute value, we can see that, in a p-adic number system, p^n gets smaller as n increases. As a result, we can finally start to construct the field of p-adic numbers. Formally, this field, denoted $\mathbb{Q}_p$, can be thought of as an alternate completion of the rational numbers to the real numbers.

Remark. Throughout this paper, we we will write $\mathbb{Q}_p$ for the set of p-adic numbers and $\mathbb{Z}_p$ for the set of p-adic integers - not to be confused with the set of integers modulo p, which we write as the quotient ring $\mathbb{Z}/p\mathbb{Z}$. All of these will be defined formally later, but their symbols will be used throughout the next section.

To start the process of constructing completions of the rational numbers, we have to first introduce a few definitions.

Definition (Completion)**.** A field K, or more generally a metric space, is called **complete** with respect to an absolute value $|\cdot|$ if every Cauchy sequence of elements in K has a limit.

Definition (Cauchy Sequence)**.** A sequence of elements x_n in a field K is called a **Cauchy sequence** if for every $\epsilon > 0$ one can find a bound M such that we have $|x_n - x_m| < \epsilon$ whenever $n, m \geq M$.

The general idea is that every Cauchy sequence of elements of a completed field should have a limit inside of that field. If we measure the distances according to the real absolute value between every two consecutive elements of a Cauchy sequence, the distance should gradually get less and less to the point where the distance is almost negligible. So reaching a limit makes sense. However, it should be easy then to see that $\mathbb{Q}$ is not complete.

Consider the sequence of rational numbers $\{3, 3.1, 3.14, 3.141, 3.1415, 3.14159, ...\}$. It should be clear that this sequence is Cauchy as the distance between two subsequent elements gets smaller and smaller. However, our sequence approaches π which is not a rational number. A similar sequence can be made for $\sqrt{2}$: $\{1, 1.4, 1.41, 1.414, 1.4142, 1.41421, ...\}$. The elements are all rational numbers, but the limit of the sequence is not.

This is the idea behind one way of defining the set of real numbers - by completing $\mathbb{Q}$ with respect to $|\cdot|_\infty$ by forming a union of $\mathbb{Q}$ and the limits of every Cauchy sequence in $\mathbb{Q}$. But what if we changed up the process slightly? Instead of completing $\mathbb{Q}$ with respect to $|\cdot|_\infty$, an archimedean absolute value, what if we completed $\mathbb{Q}$ with respect to our non-archimedean p-adic absolute value?

3.2 Forming $\mathbb{Q}_p$

We have now seen that $\mathbb{Q}$ is not complete with respect to $|\cdot|_\infty$; and, while it will not be shown here, $\mathbb{Q}$ is not complete with respect to the p-adic absolute value either. It turns out that we can actually form another completion by a similar method to how we formed the real numbers but by using the p-adic absolute value. However, there is something to consider before we start forming Cauchy sequences. With the real absolute value, it is easier for us to understand a sequence of numbers that gets closer and closer together, but it is important to realize that the following does not imply a sequence is Cauchy:

$$\lim_{n\to\infty} |x_{n+1} - x_n|_\infty = 0$$

One would think that it would make perfect sense for a sequence whose distances between subsequent terms decreases to 0 to be Cauchy and therefore convergent. However, we recall that the harmonic series from Calculus II is an example of such a series that is divergent.

Theorem. The **harmonic series** is defined by

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + ...$$

The harmonic series diverges.

This is interesting because the distance between any two subsequent terms of the sequence $(|x_{n+1} - x_n|_\infty)$ will get smaller and smaller as n tends to infinity. However, the series of that sequence will never converge. So this tells us that the sequence $\{\frac{1}{n}\}$ will never, in fact, approach a number. One fun fact about non-archimedean norms though, is that this type of sequence will always be Cauchy under a non-archimedean norm.

Lemma. A sequence $\{x_n\}$ of rational numbers is a Cauchy sequence with respect to a non-archimedean norm $|\cdot|$ if and only if

$$\lim_{x\to\infty} |x_{n+1} - x_n| = 0$$

Proof. If $m = n + r > n$, we get by the properties of a non-archimedean norm that

$$\begin{aligned} |x_m - x_n| &= |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \cdots + x_{n+1} - x_n| \\ &\leq \max\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \ldots, |x_{n+1} - x_n|\} \end{aligned}$$

It follows as a result that the lemma must hold true. □

The result of all of this being that it is easier to construct Cauchy sequences with $|\cdot|_p$ than it is with $|\cdot|_\infty$. Again, our goal is to complete $\mathbb{Q}$ with respect to $|\cdot|_p$ by adding the limits of all of the Cauchy sequences in $\mathbb{Q}$ formed by $|\cdot|_p$ to $\mathbb{Q}$. However, as we are creating a field from the perspective of $\mathbb{Q}$, it does not make sense to create numbers that do not exist (the limits). Rather than make up numbers, we will instead use the Cauchy sequences themselves.

Definition. Let $|\cdot|_p$ by the non-archimedean p-adic norm on $\mathbb{Q}$. We denote by $\mathcal{C}_p(\mathbb{Q})$ the set of all Cauchy Sequences of rational numbers:

$$\mathcal{C}_p(\mathbb{Q}) := \Big\{\{x_n\} : \{x_n\} \text{ is a Cauchy sequence with respect to } |\cdot|_p\Big\}$$

Furthermore, we can see that $\mathcal{C}_p(\mathbb{Q})$ is a ring. Addition and multiplication in $\mathcal{C}_p(\mathbb{Q})$ is closed and defined below.

$$\{x_n\} + \{y_n\} = \{x_n + y_n\}$$
$$\{x_n\} * \{y_n\} = \{x_n * y_n\}$$

The zero element is $\{0, 0, 0, 0, ...\}$ and the identity element is $\{1, 1, 1, 1, ...\}$. Since these sequences are formed of rational numbers, it follows that $\mathcal{C}_p(\mathbb{Q})$ is a commutative ring.

But we do have to make sure of something. We just formed a ring that we claim is about to extend the rational numbers. So before we move forward, we should make sure that $\mathbb{Q} \hookrightarrow \mathcal{C}_p(\mathbb{Q})$, that the rational

numbers are embedded in our ring. Well, this is actually easy to show based on our recently proven lemma. If construct a constant sequence - that is, for $x \in \mathbb{Q}$, we form $\{x_n\} = \{x, x, x, x, \dots\}$ - then this sequence will be Cauchy under $|\cdot|_p$ because $\lim_{n\to\infty} |x_{n+1} - x_n|_p = \lim_{n\to\infty} |0|_p = 0$. Thus, $\mathbb{Q} \hookrightarrow \mathcal{C}_p(\mathbb{Q})$.

We are not quite done yet. It turns out that we can create several Cauchy sequences that converge to the same number. While, for our purposes, these sequences are essentially the same (we care about their limits, not necessarily the sequences), they are still different objects in $\mathcal{C}_p(\mathbb{Q})$. In order to create an equivalence for these sequences that converge to the same number, we remind ourselves of some ring theory concepts from Intro to Modern Algebra.

Definition (Ideal Ring)**.** An **ideal** I of a ring R is a subring such that for any element $r \in R$ and any element $i \in I$, $i * r \in I$ and $r * i \in I$. Furthermore, we say that two elements $a, b \in R$ are **congruent modulo I**, written $a \equiv b \pmod{I}$, provided that $a - b \in I$.

Definition (Maximal Ideal)**.** A **maximal ideal** M is an ideal of a ring R such that for any ideal $I \in R$, we know that $I \subset M$ and $M \neq R$.

Definition (Quotient Ring)**.** Let R be a ring and I be an ideal in R. A **quotient ring**, written R/I is a ring equipped with a congruence defined by the ideal whose elements are the cosets $a + I$.

Definition. We define $\mathcal{N} \subset \mathcal{C}_p(\mathbb{Q})$ to be the ideal

$$\mathcal{N} = \left\{\{x_n\} : x_n \to 0\right\} = \left\{\{x_n\} : \lim_{x\to\infty} |x_n|_p \to 0\right\}$$

of sequences that tend to 0 with respect to the p-adic norm. Furthermore, $\mathcal{N}$ is a maximal ideal of $\mathcal{C}_p(\mathbb{Q})$

What we have just done is create a subring of $\mathcal{C}_p(\mathbb{Q})$ in which the Cauchy sequences that converge to zero under the p-adic norm are equivalent objects. Thus might sound strange until we realize that the difference between two Cauchy sequences that individually converge to the same number will converge to zero. So really, two sequences in $\mathcal{C}_p(\mathbb{Q})$ are equivalent with respect to $\mathcal{N}$ if they converge to the same number. In symbols, $a \equiv b \pmod{I} \Rightarrow a - b \in I \Rightarrow a - b \to 0$.

With our new ideal, we now have the ability to separate the Cauchy sequences in $\mathcal{C}_p(\mathbb{Q})$ by sequences that converge to the same number. We do this by taking the quotient ring of $\mathcal{C}_p(\mathbb{Q})$ by $\mathcal{N}$. Additionally, one property of quotient rings is that taking a quotient ring by a maximal ideal results in a field.

Definition ($\mathbb{Q}_p$)**.** We define the $\mathbf{p-adic\ numbers}$ to be the quotient of the ring $\mathcal{C}_p(\mathbb{Q})$ by its maximal ideal $\mathcal{N}$:

$$\mathbb{Q}_p = \mathcal{C}_p(\mathbb{Q})/\mathcal{N}$$

It is important to notice that any constant sequence in $\mathcal{C}_p(\mathbb{Q})$ will not differ by an element of $\mathcal{N}$. In other words, every constant sequence has its own equivalence class in $\mathbb{Q}_p$. Thus, $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. All that remains now it prove that $\mathbb{Q}_p$ is actually a complete space. In order to that, however, we must first see that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Definition (Dense Subset)**.** Let K be a field and $|\cdot|$ be an absolute value on that field. A subset $S \subset K$ is called dense in K if every open ball around every element of K contains an element of S; in symbols, if for every $x \in k$ and every $\epsilon > 0$ we have

$$B_\epsilon(x) \cap S \neq \emptyset$$

Proposition. The image of $\mathbb{Q}$ in the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ is a dense subset of $\mathbb{Q}_p$

Proof. Let $\lambda \in \mathbb{Q}_p$. By the construction of $\mathbb{Q}_p$, we know that there exists a sequence $\{x_n\}$ representing λ. For each fixed positive $m \in \mathbb{N}$, we denote the constant sequence $\{x_m\}$. In other words, $\{x_m\}$ is a rational number in p-adic form where x_m is some number from the sequence $\{x_n\}$. Thus, we write the sequence $\{x_n - x_m\}_{n=1}^{\infty}$. We see that this is equivalent to writing $\lambda - \{x_m\}$. Since $\{x_n\}$ is Cauchy, we see that

$$\lim_{n\to\infty} |\lambda - \{x_m\}|_p = \lim_{n\to\infty} |x_n - x_m|_p = 0$$

Therefore, it follows that every p-adic number is sufficiently close to a rational number. It follows then that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. □

Before we prove that $\mathbb{Q}_p$ is complete with respect to the p-adic absolute value, we have to settle the slightly confusing issue of convergence of sequences in $\mathbb{Q}_p$. Remember that $\mathbb{Q}_p$ is a quotient ring of Cauchy sequences. So a sequence of elements in $\mathbb{Q}_p$ is a sequence of sequences.

Definition. If $\lambda \in \mathbb{Q}_p$ is an element of $\mathbb{Q}_p$, and $\{x_n\}$ is any Cauchy sequence representing λ, we define

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p$$

Proposition. $\mathbb{Q}_p$ is complete with respect to $|\cdot|_p$.

Proof. Let $\{\lambda_n\}$ be a Cauchy sequence of elements of $\mathbb{Q}_p$. If $\mathbb{Q}_p$ is complete, then this Cauchy sequence must converge. From the fact that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, we know that for every λ_n we can choose a rational number a_n to create a constant sequence such that

$$|\lambda_n - \{a_n\}|_p = \lim_{n\to\infty} |\lambda_n - \{a_n\}|_p < \frac{1}{n}$$

From the proof of the density of $\mathbb{Q}$ in $\mathbb{Q}_p$, we can easily see $\{\lambda_n - a_n\}$ is a Cauchy sequence in $\mathbb{Q}_p$. Furthermore, we see that

$$\{a_n\} = \{\lambda_n\} - \{\lambda_n - a_n\}$$

and as a result $\{a_n\}$ is a Cauchy sequence. However, we recall that $\{a_n\}$ is a constant sequence where $a_n \in \mathbb{Q}$. We will denote its representation in $\mathbb{Q}_p$ as $\widehat{a_n}$. We want to show that $\widehat{a_n} = \lim_{n\to\infty}\{\lambda_n\}$. We start by seeing that

$$\{\widehat{a_n} - \lambda_n\} = \{\widehat{a_n} - \{a_n\}\} - \{\lambda_n - \{a_n\}\}$$

However, we have previously shown that both sequences on the right will converge to 0. This implies that

$$\lim_{n\to\infty} |\widehat{a_n} - \lambda_n|_p = 0$$

However, as $\widehat{a_n}$ is a constant number, then it stands to reason that

$$\lim_{n\to\infty} \lambda_n = \widehat{a_n}$$

What this states is that any Cauchy sequence in $\mathbb{Q}_p$ will have a limit in $\mathbb{Q}_p$. Therefore, $\mathbb{Q}_p$ is a complete space. □

3.3 Otrowski's Theorem and the Product Formula

Before we start looking at properties of the p-adic number, there is an important question that we would like to answer. Why would swapping $|\cdot|_\infty$ with $|\cdot|_p$ be significant? Are there not more types of absolute values that we could construct in order to form new extensions of the rational numbers? Well, due to an important theorem, it turns out that every absolute value on $\mathbb{Q}$ is equivalent to one of these two.

Definition. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ are considered **equivalent** if they define the same topology on K, that is, every open set with respect to one is open with respect to the other.

This definition may be easy to say, but it can be a lot harder to show. To help prove equivalence of absolute values, we will make use of the following theorem.

Theorem. Let $|\cdot|_1$ and $|\cdot|_2$ be equivalent absolute values on a field K. Then there is a positive real number c such that $|\cdot|_1 = |\cdot|_2^c$.

Theorem (Ostrowski)**.** Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to one of the absolute values $|\cdot|_p$, where p is a prime number or $p = \infty$.

Proof. Assume that $|\cdot|$ is non-trivial. Then we will examine the cases where $|\cdot|$ is archimedean and non-archimedean.

Case I Suppose that $|\cdot|$ is archimedean. Our goal is to show that $|\cdot|$ is equivalent to $|\cdot|_\infty$. Since $1 < |2| \leq |1| + |1| = 2$, there is a number $c \in \mathbb{R}$, $0 < c \leq 1$ for which

$$|2| = 2^c$$

For $n \in \mathbb{N}$, we shall prove that

$$|n| = n^c$$

Thus, let $n \in \mathbb{N}$, $n \geq 2$, and write n using the base 2 notation

$$n = a_0 + a_1 * 2 + \cdots + a_s * 2^s, \quad a_0, a_1, \cdots \in \{0, 1\}, \;\; a_s = 1$$

Then $2^s \leq n < 2^{s+1}$ so that

$$2^{sc} \leq n^c < 2^{c(s+1)} \qquad (*)$$

We first prove that $|n| \leq |n|^c$ as follows. Applying (*) we get

$$|n| \leq \sum_{i=0}^{s} |a_i| \, |2|^i \leq \sum_{i=0}^{s} 2^{ic} = 2^{sc}(1 + 2^{-c} + \cdots + 2^{-sc}) \leq n^c M$$

where $M := \sum_{i=0}^{\infty} 2^{-ic}$ does not depend on n. Since n was arbitrary, we have also

$$|n^k| \leq n^{kc} M, \quad k \in \mathbb{N}$$

so that

$$|n| \leq \lim_{k \to \infty} n^c \sqrt[k]{M} = n^c \qquad (**)$$

To prove the opposite inequality, observe that

$$|n| = |2^{s+1} - (2^{s+1} - n)| \geq |2^{s+1}| - |2^{s+1} - n|$$

Now $|2^{s+1}| = |2|^{s+1} = 2^{c(s+1)}$. By (*) and (**),

$$|2^{s+1} - n| \leq (s^{s+1} - n)^c \leq (s^{s+1} - 2^s)^c = 2^{sc}$$

so that

$$|n| \geq 2^{c(s+1)} - 2^{cs} = 2^{c(s+1)}(1 - 2^{-c})$$

Again, by (*), $2^{c(s+1)} > n^c$; with $M' := 1 - 2^{-c}$ we obtain

$$|n| \geq n^c M'$$

The kth power tick yields

$$|n| \geq \lim_{k \to \infty} n^c \sqrt[k]{M'} = n^c$$

which, together with (**), proves $|n| = n^c$. Thus, all archimedean absolute values are equivalent.

Case II Now suppose that $|\cdot|$ is non-archimedean. For the theorem to hold true, it makes sense that $|\cdot|$ is equivalent to $|\cdot|_p$. As a result of $|\cdot|$ being non-archimedean, the set $\{n \in \mathbb{N} : |n| < 1\}$ is nonempty. Let p be its minimum element. We claim that p is a prime number. In fact, $p \neq 1$. If $p = ab$ for some $a, b \in \mathbb{N}$, $a < p, b < p$, then $|a| = |b| = 1$, so $|p| = |ab| = 1$, a contradiction. Next, we show that $|q| = 1$ for any $q \in \mathbb{N}$ that is not divisible by p. By the division algorithm $q = ap + r$ where $a \in \{0, 1, 2, \dots\}$ and $1 \leq r < p$. Then $|r| = 1$ and $|ap| = |a| * |p| \leq |p| < 1$. By the strong triangle inequality, $1 = |r| \leq \max\{|ap + r|, |-ap|\} = \max\{|q|, |ap|\} = |q|$. So $|q| \geq 1$, i.e. $|q| = 1$. It follows that for each natural number n,

$$|n| = |p|^k$$

where k is the number of factors p of n. We see that for each $n \in \mathbb{N}$

$$|n| = |n|_p^c$$

where $c = -\log |p| (\log(p))^{-1}$. It follows easily that

$$|x| = |x|_p^c \quad x \in \mathbb{Q}$$

Therefore, all absolute values on $\mathbb{Q}$ are equivalent to either the real absolute value or the p-adic norm. $\square$

Ostrowski's theorem tells us that we can only perform arithmetic in $\mathbb{Q}$ with two types of absolute values: the real absolute value and the p-adic absolute value. This is important to us because it tells us that even if we created another absolute value and tried to use it to extend the rational numbers, we would get a set of numbers equivalent to either the set of real numbers of the p-adic numbers. Furthermore, one useful result of Ostroski's theorem is that we have a way to relate all of the absolute values on $\mathbb{Q}$.

Theorem (Product Formula)**.** For any $x \in \mathbb{Q}^x$, we have

$$\prod_{p \leq \infty} |x|_p = 1$$

where $p \leq \infty$ means that we take the product over all the primes of $\mathbb{Q}$ including the prime at infinity (which is the real absolute value, $|\cdot|_\infty$).

Proof. For the sake of brevity, we prove this for the case that $x \in \mathbb{Z}$. The general case will follow suite. By the fundamental theorem of arithmetic, we can decompose a positive x into $x = p_1^{a_1} * p_2^{a_2} * \cdots * p_k^{a_k}$. It follows that

$$\begin{cases} |x|_q = 1 & \text{if } q \neq p_i \\ |x|_p = p^{-a_i} & \text{for } i = 1, 2, \ldots, k \\ |x|_\infty = p_1^{a_1} * p_2^{a_2} * \cdots * p_k^{a_k} \end{cases}$$

Then as a result, we have

$$\prod_{p \leq \infty} |x|_p = (p^{-a_1}) * (p^{-a_2}) * \cdots * (p_1^{a_1} * p_2^{a_2} * \cdots * p_k^{a_k}) = 1$$

□

The product formula has many applications (many of which are beyond the scope of this paper) including uses in the theory of heights on algebraic varieties and the application of Hasse's local-global principle.

4 Exploring $\mathbb{Q}_p$

In this section, we will discuss the basic arithmetic operations on the p-adic numbers. Through this, we will also expose some interesting properties of these number systems and compare them to the real numbers.

4.1 Writing p-adic Numbers

Up until now, we have focused on the p-adic numbers as a system as a whole rather than as individual numbers. We take the time now to formally define the elements of $\mathbb{Q}_p$. We recall that a p-adic number is a number that is written in base p (where p is a prime number) rather then in the more commonly used 10-ary or decimal system. As such, we write the general p-adic numbers as a p-adic expansion; that is,

$$\sum_{k=-n}^{\infty} a_k p^k = a_n p^{-n} + a_{n+1} p^{-n+1} + \cdots + a_0 + a_1 p + a_2 p^2 + \ldots, \quad a_k \in \{0, 1, 2, \ldots, p-1\}$$

As a result of the way we construct the Cauchy sequences that form the p-adic numbers, we also have the properties that $x_n - x_{n-1} = a_n p^n$, where x_n is the partial sum of the first n elements of the p-adic expansion, and $x_n \equiv x_{n-1} \pmod{p^n}$. From the definition of congruence modulo p^n, it turns out that we can recover coefficients of our p-adic expansion if we have the partial sums. We know that

$$p^n | x_n - x_{n-1} \Rightarrow x_n - x_{n-1} = cp^n \Rightarrow c = a_n = \frac{x_n - x_{n-1}}{p^n}$$

Note that in the p-adic expansion, when k is a negative number, these terms form the denominator of a rational number. Alternatively, these are equivalent to decimal places of the decimal number. If the number is in $\mathbb{Z}_p$, then there will be no negative indices. Additionally, if we are writing a number in $\mathbb{Q}_p$, then it must have a finite number of negative indices. We also notice that, in order to write a p-adic number in summation form, it looks backwards to how we normally write numbers. As an alternative to writing a p-adic number as we normally would, we can also express the number in p-ary form.

$$x = (\ldots a_3 a_2 a_1 a_0 . a_{-1} a_{-2} \ldots)_p, \quad a_i \in \{0, 1, \ldots, p-1\} \forall\, i \in \mathbb{Z}$$

The final p at the end of the chain of numbers just notes that we are writing the number in base-p. Throughout this section, we will write p-adic numbers in both forms to help adjust to the backwards notation of a p-adic number.

To make sure that we can confidently read a p-adic number, let's convert a few numbers from $\mathbb{Q}$ to $\mathbb{Q}_p$. As an example, we will convert 328 to its 5-adic form. We observe that

$$328 = 2 * 5^3 + 3 * 5^2 + 3 = (2303)_5$$

We arrived at this conclusion by continuously dividing the number 328 by 5. The remainder that we get by dividing by 5 (which must be less than 5 by the division algorithm) is the first digit of the p-adic number. It is the coefficient multiplied by p^0. In p-ary form, it is the first digit on the right.

Decimal	5-ary	5-adic
$328 = 3 + 5(65)$	$(3)_5$	$3p^0$
$65 = 5(13)$	$(03)_5$	$3p^0 + 0p$
$13 = 3 + 5(2)$	$(303)_5$	$3p^0 + 0p + 3p^2$
$2 = 2 + 5(0)$	$(2303)_5$	$3p^0 + 0p + 3p^2 + 2p^3$

While the process is a little longer for rational numbers, the idea is still the same. The main difference is that we have two integers to convert rather than one. Let $\frac{a}{b} \in \mathbb{Q}$. If $\frac{a}{b}$ is not a proper fraction, make it proper and convert the integer part as shown above. If b is divisible by p, than the first digit's place will be whatever power of p most divides the denominator, in other words $v_p(b)$. Once $p^{v_p(b)}$ has been factored out of b (so $p \nmid b$) expand the fraction by the same division algorithm as shown as above. Two examples of this process are below.

Example. In this example, we convert $\frac{242}{25}$ into its 5-adic form. Note that our number is not proper, so we write $\frac{242}{25} = 9\frac{17}{25}$. Furthermore, $25 = 5^2$, so we know that our first digit will be in the 5^{-2} spot. If we factor out 5^{-2}, we get $\frac{17}{1} = 17$. To find the 5-adic form of our number, we need to convert 9 and 17 and add the results together.

Decimal	5-ary	5-adic
$9 = 4 + 5(1)$	$(4)_5$	$4p^0$
$1 = 5(0) + 1$	$(14)_5$	$4p^0 + 1p^1$

Decimal	5-ary	5-adic
$17 = 2 + 5(3)$	$(2)_5$	$2p^{-2}$
$3 = 5(0) + 3$	$(32)_5$	$2p^{-2} + 3p^{-1}$

Now we see that

$$9\frac{17}{25} = \frac{225 + 17}{25} = 2p^{-2} + 3p^{-1} + 4p^0 + 1p^1 = (14.32)_5$$

Example. In this example, we will convert $\frac{24}{17}$ into its 3-adic form. Since this number is both in proper form and does not have a denominator divisible by 3, we can just proceed into the division algorithm.

Decimal	3-ary	3-adic
$\frac{24}{17} = 3(\frac{8}{17})$	$(0)_3$	$0p^0$
$\frac{8}{17} = 1 + 3(-3/17)$	$(10)_3$	$1p$
$\frac{-3}{17} = 3(-1/17)$	$(010)_3$	$p + 0p^2$
$\frac{-1}{17} = 1 + 3(-6/17)$	$(1010)_3$	$p + 1p^3$
$\frac{-6}{17} = 3(-2/17)$	$(01010)_3$	$p + p^3 + 0p^4$
$\frac{-2}{17} = 2 + 3(-12/17)$	$(201010)_3$	$p + p^3 + 2p^5$
$\frac{-12}{17} = 3(-4/17)$	$(0201010)_3$	$p + p^3 + 2p^5 + 0p^6$
$\frac{-4}{17} = 1 + 3(-7/17)$	$(10201010)_3$	$p + p^3 + 2p^5 + 1p^7$
$\frac{-7}{17} = 1 + 3(-8/17)$	$(110201010)_3$	$p + p^3 + 2p^5 + p^7 + 1p^8$
$\frac{-8}{17} = 2 + 3(-14/17)$	$(2110201010)_3$	$p + p^3 + 2p^5 + p^7 + p^8 + 2p^9$

If we were to continue our calculations, we would eventually see that the digits start to repeat. We completely write the number as

$$\frac{24}{17} = (...\overline{0112021221102010}10)_3 = p + p^3 + 2p^5 + p^7 + p^8 + 2p^9 + 2p^{10} + p^{11} + 2p^{12} + 2p^{14} + p^{16} + p^{17} + \dots$$

The overlined part of our 3-ary number is the period of our number. In other words, if we keep writing out the number to the left, our period would keep repeating the pattern. In the p-adic representation, there is no universal notation to denote a period. However, the coefficients of the period would still cycle with the more terms we write out. In the decimal system, all rational numbers either have a finite number of digits to the right of the decimal point, or they have a period and repeat a pattern of numbers. The same thing happens to rational numbers when they are converted to a p-adic form, but in reverse. In p-ary form, they will have a finite number of digits to the right of the decimal point, but they can have either finite or a periodic string of numbers to the left of the decimal point. In p-adic form, this translates to a finite number of terms with a negative index and either a set of finite or periodic terms with positive indices.

As shown in the last couple of examples, small and simply-written numbers in the decimal system can look odd in a p-adic form. For instance, we claim that -1 is equivalent to $(...2222222.0)_3$. To show this, we will find the distance between -1 and $(...2222222.0)_3$.

$$\lim_{n\to\infty} |(2 + 2 * 3^1 + 2 * 3^2 + 2 * 3^3 + \dots + 2 * 3^n) - (-1)|_3 =$$
$$\lim_{n\to\infty} |3 + 2 * 3^1 + 2 * 3^2 + 2 * 3^3 + \dots + 2 * 3^n|_3 =$$
$$\lim_{n\to\infty} |3^{n+1}|_3 = |0|_3 = 3^{-v_3(0)} = 3^{-\infty} = 0$$

We can also show that, after we talk about arithmetic operations in $\mathbb{Q}_p$, that $(...2222222.0)_3 + (...00000001)_3 = 0$.

4.2 Arithmetic Operations

$\mathbb{Q}_p$ is a field which means that all of the arithmetic operations that work in $\mathbb{Q}$ will also work on the p-adic numbers. The good news is even though these numbers may appear exotic, the normal operations are still very simple, albeit a bit tedious.

Addition works the same way that we learned it in elementary school. We line up the numbers of the same power of p in the same column and add them. But as our digits are in $\mathbb{Z}/p\mathbb{Z}$, they must be in the set $\{0, 1, 2, \dots, p-1\}$. If two numbers sum up to more than p, it is replaced in the sum by its congruence modulo p and the integral part of the sum is divided by p is added to the next column.

Example. Below, we add the 3-adic numbers $\dots 000000001.0_3$ and 222222222.0_3.

$$\begin{array}{r} \dots 000000001.0_3 \\ + \dots 222222222.0_3 \\ \hline \dots 333333333.0_3 \\ = 000000000.0_3 \end{array}$$

The same method works for subtraction is we use the borrowing principle from elementary school. Furthermore, multiplication and division (in the sense of multiplying by the inverse of a number) can be performed in a similar manner. We can also use multiplication to find the negative version of a number (the multiplicative inverse).

Example. Below, we multiply the 5-adic numbers $\frac{1}{3} = \overline{13}2.0_5$ and $-1 = \ldots 444444444.0_5$.

$$\begin{array}{r} \ldots 131313132.0_5 \\ \times \ldots 444444444.0_5 \\ \hline \ldots 131313133 \\ \ldots 313131330 \\ \ldots 131313300 \\ + \ldots\ldots\ldots\ldots \\ \hline = \ldots 313131313.0_5 \\ = \overline{13}.0_5 \end{array}$$

4.3 Structure of $\mathbb{Q}_p$ and $\mathbb{Z}_p$

In this section, we will discuss some of the algebraic properties and structures involving the p-adic numbers. We will introduce the concept of a valuation ring, and the units in $\mathbb{Z}_p$.

Definition (Valuation Ring)**.** Let K be a field. A subring $\mathfrak{o}$ of K is called a **valuation ring** if it has the property that for any $x \in K$, we have $x \in \mathfrak{o}$ or $x^{-1} \in \mathfrak{o}$.

Definition. Let $(K, |\cdot|)$ be a valued field with a non-archimedean valuation. The subset

$$\mathcal{O} = \overline{B}_1(0) = \{x \in K : |x| \leq 1\} \subset K$$

is called the **valuation ring** of $|\cdot|$. Its subset

$$\mathcal{B} = B_1(0) = \{x \in K : |x| < 1\}$$

is an ideal of $\mathcal{O}$ called the **valuation ideal**. Furthermore, the valuation ideal is a maximal ideal in $\mathcal{O}$ and every element of the complement $\mathcal{O} - \mathcal{B}$ is invertible in $\mathcal{O}$. The quotient ring

$$\kappa = \mathcal{O}/\mathcal{B}$$

is called the **residue field** of $|\cdot|$.

If we consider the valued field $(\mathbb{Q}, |\cdot|_p)$, then we know the following:

1. The associated valuation ring is $\mathcal{O} = \mathbb{Z}_p = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$.
2. Its valuation ideal is $\mathcal{B} = p\mathbb{Z}_p = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b \text{ and } p|a\}$.
3. The residue field is $\kappa = \mathbb{F}_p$ (the field with p elements).

Before moving on to $\mathbb{Q}_p$, we would first like to formally define the p-adic integers.

Definition (p-adic Integer)**.** The **ring of p − adic integers**, is the valuation ring

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

Recall that $|x|_p = p^{-v_p(x)}$. We have seen earlier that an element of $\mathbb{Q}_p$ takes the form of a finite-tailed Laurent series. That is, the p-adic expansion has a finite number of digits with a negative index. Consider the p-adic number $x = \cdots + a_{-2}p^{-2} + a_{-1}p^{-1} + a_0p^0 + a_1p^1 + a_2p^2 + \ldots$ where $a_{-1} \not\equiv 0 \pmod{p}$. Thus, p^{-1} can be factored out of x. So $|x|_p = p^{-v_p(x)} = p^1 > 1$. It stands to reason that, if we have any negative indices with coefficients not equal to 0 in our p-adic expansion, our p-adic absolute value will give us a value greater than one. So any p-adic integer, in order to satisfy the above definition, will consist of nonnegative powers of p.

If we consider the valuation ideal of $\mathbb{Z}_p$, we can determine the units of the p-adic integers.

Definition (Unit)**.** Let R be a ring with unity. An element $a \in R$ is a **unit** if a has a multiplicative inverse in R. That is, $a^{-1} \in R$ such that $a * a^{-1} = 1_R = a^{-1} * 1$.

One fact about the ring of p-adic integers is that they form a special type of ring known as a local ring.

Definition (Local Ring)**.** A **local ring** is a ring that contains a unique maximal ideal whose complement consists of invertible elements.

This tells us the maximal ideal of the p-adic integers, $p\mathbb{Z}_p$, is unique and it does not contain any units of $\mathbb{Z}_p$. So if the ring of p-adic integers contains any units, it would be in the complement of $p\mathbb{Z}_p$; that is, they would be contained in the set

$$\{x \in \mathbb{Q}_p : |x|_p = 1\}$$

Let's consider a finite p-adic integer $x = a_0 + a_1p + a_2p^2 + \cdots + a_np^n$. We write the following:

$$|x|_p = 1 \Rightarrow |a_0 + a_1p + a_2p^2 + \cdots + a_np^n|_p = 1$$
$$\Rightarrow \frac{1}{p^{v_p(x)}} = 1 \Rightarrow v_p(x) = v_p(a_0 + a_1p + a_2p^2 + \cdots + a_np^n) = 0$$

Recall that each coefficient $a_i \in \{0, 1, \ldots, p-1\}$. If $a_0 = 0$, then we could, at a minimum, factor p out of x which would mean that $v_p(x) \neq 0$. Thus, for x to be a unit in Z_p, $a_0 \not\equiv 0 \pmod{p}$. In fact, the relation works both ways, and we can restate this as a theorem.

Theorem. A p-adic integer x is a unit if and only if $a_0 \not\equiv 0 \pmod{p}$

As a result, we have a new way to represent p-adic integers. A number $x \in \mathbb{Z}_p$ can be written as $x = up^n$ where u is a unit in $\mathbb{Z}_p$ and $n \in \mathbb{Z}$. This result can also be extended to $\mathbb{Q}_p$.

Furthermore, we have shown that $\mathbb{Z}_p$ contains elements which do not have multiplicative inverses in $\mathbb{Z}_p$. This means that $\mathbb{Z}_p$ cannot be a field. However, as $\mathbb{Z}_p \subset \mathbb{Q}_p$ and $\mathbb{Q}_p$ is a field, then $\mathbb{Z}_p$ cannot contain zero divisors. Thus, it follows that $\mathbb{Z}_p$ is an integral domain. But more specifically, we know that $\mathbb{Z}_p$ is a principle ideal domain and, as a result, a unique factorization domain.

Definition (Principle Ideal Domain)**.** A **principle ideal domain** is an integral domain in which every ideal is principal, that is, generated by a single element.

Definition (Unique Factorization Domain)**.** A **unique factorization domain** is an integral domain R satisfying the following properties:

1. Every nonzero element $a \in R$ can be expressed as $a = p_1 \ldots p_n$, where u is a unit and p_i are irreducible. That is, p_i cannot be represented as a product of nonunits.
2. If a has another factorization , sat $a = vq_1 \ldots q_m$ where v is a unit and the q_i are irreducible, then $n = m$ and, after reordering if necessary, p_i and q_i are associates for each i. That is $p_i = sq_i$ for some unit $s \in R$.

Theorem. Every principle ideal domain is a unique factorization domain.

While the implications of these facts are numerous, we choose to end this section focusing on the ideals of $\mathbb{Z}_p$.

Proposition. The ring $\mathbb{Z}_p$ is a principle ideal domain. More precisely, its ideals are the principle ideals $\{0\}$ and $p^k\mathbb{Z}_p$ for all $k \in \mathbb{N}$.

Proof. Let $I \neq \{0\}$ be an ideal in $p\mathbb{Z}_p$, and let $0 \neq a \in I$ be an element of maximum absolute value. We know this is possible because $|\cdot|_p$ forms a set of discrete values. Suppose that $|a|_p = p^{-k}$ for some $k \in \mathbb{N}$. Then $a = up^k$, u is a unit of $\mathbb{Z}_p$. Then $p^k = u^{-1}a \subset I$, and hence $(p^k) = p^k\mathbb{Z}_p \subset I$. Conversely, for any $b \in I$, $|b|_p = p^{-w} \leq p^{-k}$. We can write

$$b = p^w u' = p^k p^{w-k} u' \in p^k\mathbb{Z}_p$$

Therefore, $I \subset p^k\mathbb{Z}_p$, and hence $I = p^k\mathbb{Z}_p$. □

4.4 Algebraically Closed Sets

In this section, will demonstrate how, like the real numbers, $\mathbb{Q}_p$ are not algebraically closed. We will also go over the extensions of $\mathbb{Q}_p$ that allow it to become closed. First, we must define what we mean by algebraically closed.

Definition (Algebraically Closed)**.** A field K is **algebraically closed** if it contains a root for every polynomial in $K[x]$.

It is well known that $\mathbb{R}$ is not algebraically closed. Consider the equation

$$x^2 + 1 = 0$$

It does not take much to realize that there is no number in $\mathbb{R}$ that satisfies $x^2 = -1$. Eventually, mathematicians represented the solution to this equation as the letter i; in other words, $i^2 = -1$. With the discovery of i came the discovery of the complex numbers which, as it turns out, is algebraically closed. In fact, it is the smallest field that is algebraically closed that contains $\mathbb{R}$.

Well, it turns out that $\mathbb{Q}_p$ is not algebraically closed. For example, in $\mathbb{Q}_5$, the equation $x^2 = 2$ has no solution. We will further discuss solving equations in $\mathbb{Q}_p$ in the section on Hensel's Lemma.

The point that we want to make in this section is that it is not guaranteed that $\mathbb{Q}_p$ is algebraically closed for every prime number p. So the question is if there is an extension for $\mathbb{Q}_p$ that is analogous to $\mathbb{C}$. Well, it turns out that such a field does exist, and it is denoted $\mathbb{C}_p$. It is beyond the scope of this paper to form this field or to work inside of it. However, modern p-adic analysis takes place in $\mathbb{C}_p$ rather than $\mathbb{Z}_p$ or $\mathbb{Q}_p$ due to its property of closure, so we wish to at least mention it for the benefit of the reader.

5 Effects of Absolute Values on Fields

5.1 Ultrametric Space

It has been mentioned several times that an absolute value gives a notion of size, magnitude, or distance. In this short discussion, we will examine the effects of absolute values on a field, and we start by formalizing the idea of distance as we did in Advanced Calculus of Several Variables.

Definition (Metric)**.** A **metric** on a set X is a function $d : X \times X \to \mathbb{R}$ having the following properties:

1. $d(x, y) \geq 0$ for all $x, y \in X$; equality holds if and only if $x = y$.
2. $d(x, y) = d(y, x)$ for all $x, y, \in X$
3. The triangle equality holds for all $x, y \in X$

The function $d(x, y)$ is often called the **distance** between x and y. The set X equipped with a metric d is written as (X, d) and is called a **Metric Space**.

When working with absolute values, our metric d is defined by $d(x, y) = |x - y|$. Furthermore, if a metric $d(x, y)$ satisfies the strong triangle inequality (i.e. $d(x, y) \leq \max\{d(x, z), d(z, y)\}$), or in other words, $d(x, y)$ is defined by a non-archimedean absolute value, then we call (X, d) an **ultrametric space**. As we know, the p-adic absolute value is non-archimedean. As a result, $(\mathbb{Q}_p, |\cdot|_p)$ is an ultrametric space. So as we explore the idea and properties of an ulatrametric space, all of the results will hold true for $\mathbb{Q}_p$.

Theorem. Let K be a field equipped with $|\cdot|$, a non-archimedean absolute value. If $x, y \in K$ and $|x| \neq |y|$, then

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

Proof. Without loss of generality, we assume that $|x| > |y|$. As a result, by the properties of non-archimedean absolute values,

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

However, note that $x = (x + y) - y$. So we have

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

Since $|x| > |y|$, this can only be true in the case that

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

This gives us $|x| \leq |x + y|$, and as $|x + y| < x$, we know that $|x + y| = |x|$ □

From this theorem, we get an interesting corollary:

Corollary. In an ultrametric space, all "triangles" are isosceles.

Proof. Let x, y, z be the three elements of our ultrametric space that form the vertices of our triangle. The length of the sides of the triangle are

$$d(x, y) = |x - y|$$
$$d(y, z) = |y - z|$$
$$d(x, z) = |x - z|$$

Clearly, $(x - y) + (y - z) = (x - z)$. By our new theorem, we know that if $|x - y| \neq |y - z|$, then $|x - z| = \max\{|x - y|, |y - z|\}$. Thus, two sides of our triangle are equal. □

The above theorem demonstrates how geometry in the p-adic numbers is very different from euclidean geometry in $\mathbb{R}$. However, open and closed balls are more widely used in topology and analysis. So at this point, we are going to explore the geometry of balls in the p-adic numbers.

5.2 Balls

Definition (Balls)**.** Let K be a field with an absolute value $|\cdot|$. Let $a \in K$ and $r \in \mathbb{R}_+$. The **open ball** of radius r and center a is the set

$$B_r(a) = \{x \in K : d(x, a) < r\} = \{x \in K : |x - a| < r\}$$

The **closed ball** of radius r and center a is the set

$$\overline{B}_r(a) = \{x \in K : d(x, a) \leq r\} = \{x \in K : |x - a| \leq r\}$$

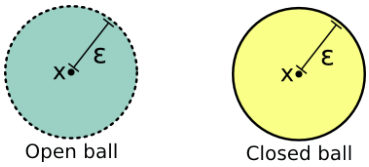

Figure 2: The open and closed balls on the 2D plane with a radius of ϵ

The open and closed balls are often used for analyzing metric spaces. There are used to show if a set is open or closed. However, in an ultrametric space, due to the non-archimedean properties of the absolute value being used, they act a bit differently.

Theorem. Let $(K, |\cdot|)$ be a valued field with a non-archimedean absolute value.

I) If $b \in B_r(a)$, then $B_r(a) = B_r(b)$; in other words, every point that is contained in a open ball is the center of that ball.

II) If $b \in \overline{B}_r(a)$, then $\overline{B}_r(a) = \overline{B}_r(b)$; in other words, every point that is contained in a closed ball is the center of that ball.

III) The set $B_r(a)$ is clopen, that is, it is both open and closed.

IV) If $r \neq 0$, the set $\overline{B}_r(a)$ is clopen.

V) If $a, b \in K$ and $r, s \in \mathbb{R}_+^x$, we have $B_r(a) \cap B_s(b)$ if and only if $B_r(a) \subset B_s(b)$ or $B_r(a) \supset B_s(b)$; in other words, any two open balls are either disjoint or contained in one another.

VI) If $a, b \in K$ and $r, s \in \mathbb{R}_+^x$, we have $\overline{B}_r(a) \cap \overline{B}_s(b)$ if and only if $\overline{B}_r(a) \subset \overline{B}_s(b)$ or $\overline{B}_r(a) \supset \overline{B}_s(b)$; in other words, any two closed balls are either disjoint or contained in one another.

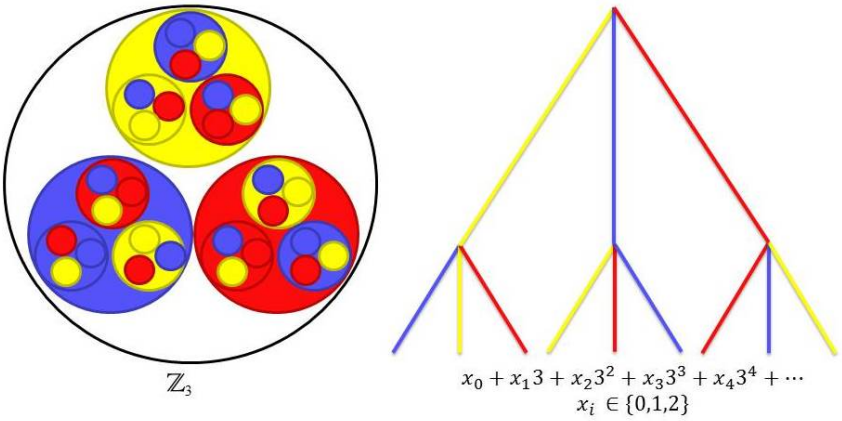

Figure 3: Visualization of the balls in Q_3

5.3 Topological Properties

For the rest of this section, we wish to topologically describe $\mathbb{Q}_p$ and $\mathbb{Z}_p$. We will not prove anything; we only wish to leave the reader with definitions and theorems to describe properties of our new numbers - several of which hold true for $\mathbb{R}$ as we discovered in Advanced Calculus of a Single Variable.

Theorem. In a valued field $(K, |\cdot|)$ with a non-archimedean norm, the connected component of any point $x \in K$ is the set $\{x\}$ consisting of only that point. In other words, $\mathbb{Q}_p$ is totally disconnected.

Corollary. $\mathbb{Q}_p$ is complete and separable.

The idea of connectedness is that, if we chose any two numbers of a set on a graph or plane, we could draw a path between those two numbers without leaving the set. In more formal terms, a connected space is one that cannot be broken up into a collection of disjoint, open sets.

For example, consider the real numbers which form a connected set. If we looked at any open interval $(a, b) \subset \mathbb{R}$ such that $c \in (a, b)$, then we know that $(a, b) \neq (a, c) \cup (c, b)$ because $c \in (a, c) \cup (c, b)$. However, the same thing cannot be said for $\mathbb{Q}_p$ because it is totally disconnected. Formally, $\mathbb{Q}_p$ forms a Hausdorff space - a space in which distinct points have disjoint neighborhoods.

Definition (Compact Set)**.** A set is **compact** if every sequence in the set has a subsequence that converges inside of the set. Furthermore, a compact set is closed and bounded.

Theorem. $\mathbb{Z}_p$ is compact.

Corollary. $\mathbb{Z}_p$ is complete.

Theorem. $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

Theorem. $\mathbb{Q}_p$ is locally compact; $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

It is interesting to note that $\mathbb{Q}_p$ is not compact. Rather, it is locally compact. What this means is that every point in $\mathbb{Q}_p$ has a neighborhood that is compact. So while $\mathbb{Q}_p$ is not compact, for any p-adic number, there exists a subset of $\mathbb{Q}_p$ containing that number that is compact. This makes sense as $\mathbb{Q}_p$ is totally disconnected. It follows from this fact that the neighborhood for any $x \in \mathbb{Q}_p$ can only be $\{x\}$. Any sequence formed in a set of one element is a constant sequence that clearly converges to itself, which makes $\{x\}$ compact.

6 Applications of $\mathbb{Q}_p$

6.1 Hensel's Lemma

Theorem (Hensel's Lemma)**.** Let $F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ be a polynomial in $\mathbb{Z}_p[X]$ - the ring of polynomials whose coefficients are in $\mathbb{Z}_p$. Suppose that there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ such that

$$F(\alpha_1) \equiv 0 \pmod{p\mathbb{Z}_p}$$

and

$$F'(\alpha_1) \not\equiv 0 \pmod{p\mathbb{Z}_p}$$

where $F'(X)$ is the derivative of $F(X)$. Then there exists a p-adic integer $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$ and $F(\alpha) = 0$.

Remark. Before we move on, we wish to mention that when we are referring to the derivative of a polynomial in $\mathbb{Z}[p]$, we mean the power rule for derivatives in $\mathbb{R}[x]$. The formal definition of a derivative is harder to execute due to the fact that $\mathbb{Q}_p$ is a disconnected space.

Hensel's lemma is one of the most import tools in elementary p-adic analysis. While it does not work for every equation, it does work for many simple ones. It allows us to not only determine if a solution exists, but to also determine an exact solution if it exists by following the process of its proof. This process is actually similar to Newton's Method which we learned about in Calculus I.

Before we prove Hensel's Lemma, we remind ourselves of Newton's method so that we can observe the parallels between it and the proof. Let x_n be an approximate solution to $f(x) = 0$. If $f'(x_n) \neq 0$, then the next approximation x_{n+1} is given by

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

Proof. Our goal is to construct a Cauchy sequence whose limit is the root α that satisfies the hypothesis for the lemma. More specifically, we will form a sequence of integers $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that

$$F(\alpha_n) \equiv 0 \pmod{p^n}$$
$$\alpha_n \equiv \alpha_{n+1} \pmod{p^n}$$

To start, we assume that an α_1 exists. To find α_2 we note that by the above conditions,

$$\alpha_1 \equiv \alpha_2 \pmod{p} \Rightarrow \alpha_2 \equiv \alpha_1 \pmod{p} \Rightarrow \alpha_2 = \alpha_1 + b_1p, \quad b_1 \in \mathbb{Z}_p$$

by the definition of congruence modulo p. By plugging the above into our function and expanding it into a Taylor Series, we get

$$F(\alpha_2) = F(\alpha_1 + b_1p) = F(\alpha_1) + F'(\alpha_1)b_1p + \cdots \equiv F(\alpha_1) + F'(\alpha_1)b_1p \pmod{p^2}$$

It follows that, in order to prove show we can find α_2, we must solve

$$F(\alpha_1) + F'(\alpha_1)b_1p \equiv 0 \pmod{p^2}$$

By our hypothesis that $F(\alpha_1) \equiv 0 \pmod{p}$, we know that $F(\alpha_1) = px$ for some x. By substitution,

$$px + F'(\alpha_1)b_1p \equiv 0 \pmod{p^2} \Rightarrow x + F'(\alpha_1)b_1 \equiv 0 \pmod{p}$$

From the condition that $F'(\alpha_1) \not\equiv 0 \pmod{p}$, we know that p does not divide $F'(\alpha_1)$. As a result, we know that $F'(\alpha_1)$ is invertible in $\mathbb{Z}_p$. So we take

$$b_1 \equiv -x(F'(\alpha_1))^{-1} \pmod{p}$$

Furthermore, we can choose a b_1 in $\mathbb{Z}$ such that $0 \leq b_1 \leq p-1$ so that b_1 is uniquely determined. For this choice of b_1, we set $\alpha_2 = \alpha_1 + b_1p$ which satisfy the above properties. From here we can uniquely determine successive values of α_n and α_{n+1} which constructs our sequence and proves our theorem. $\square$

For higher values of n, the formulas are restated below.

1. $F(\alpha_n) = p^n x \pmod{p^{n+1}}$
2. $x + F'(\alpha_1)b_n \equiv 0 \pmod{p}$
3. $\alpha_{n+1} = \alpha_n + b_n p$

Compare the above equations to the process in the proof, and note that for all values of n, the derivative can always be calculated at α_1. This is because, if we look at the Taylor series expansion,

$$F'(\alpha_n) = F'(\alpha_1) + F''(\alpha_2)b_2 p + \cdots \equiv F'(\alpha_1) \pmod{p}$$

So due to the modulo p, we can reuse the same value in 2. above for our iterations.

Example. To help show the process for using Hensel's Lemma, we solve

$$x^2 = 7, \quad x \in \mathbb{Q}_3$$

Solution. We define our function by $f(x) = x^2 - 7$ where $x \in \mathbb{Q}_3$. First we need to solve

$$\alpha_1^2 \equiv 7 \equiv 1 \pmod{3}$$

which we can clearly solve by $\alpha_1 = 1, 2$. We choose $\alpha_1 = 1$ to start our solution (starting with $\alpha_1 = 2$ simply gives another solution). We then write

$$f(\alpha_1) = f(1) = -6 \equiv 3 \pmod{3^2} = 3(1) = px$$

We also note that $f'(x) = 2x \Rightarrow f'(1) \equiv 2 \pmod{3}$. It follows that

$$px + f'(\alpha_1)b_1 p \equiv 0 \pmod{p^2} \Rightarrow x + f'(\alpha_1)b_1 \equiv 0 \pmod{p} \Rightarrow 1 + (2)b_1 \equiv 0 \pmod{3} \Rightarrow b_1 = 1$$

So by our equation for α_2, we write

$$\alpha_2 = \alpha_1 + b_1 p = 1 + 1 * 3 = 4$$

Repeating for our next iteration, we find that

$$\begin{gathered} f'(\alpha_2) \equiv 1 \pmod{3}, \\ f(\alpha_2) = 16 - 7 \equiv 9(1) \equiv p^2 x \pmod{3^3} \Rightarrow x \equiv 1 \pmod{3}, \\ x + f'(\alpha_2)b_2 \equiv 0 \pmod{3} \Rightarrow 1 + b_2 \equiv 0 \pmod{3} \Rightarrow b_2 = 2, \\ \alpha_3 = \alpha_2 + b_2 p = 4 + 2 * 3 = 10 \end{gathered}$$

Continuing this process allows us to solve uniquely for α_n provided that the derivative at α_n is nonzero. After continuing for four iterations and reducing the coefficients modulo 3, we get

$$\alpha_4 = 1 + 1 * 3 + 1 * 3^2 + 0 * 3^3 + 2 * 3^4 + \ldots$$

□

As a result of Hensel's Lemma, we can now determine several properties of p-adic numbers such as determining what numbers are quadratic residues, square roots, squares, and roots of unity - types of numbers that we learning about in Intro to Complex Analysis and Number Theory. First, we will see how to determine if a p-adic number is a quadratic residue.

Theorem. A polynomial with integer coefficients (an element of $\mathbb{Z}[X]$) has a root in $\mathbb{Z}_p$ if and only if it has a root modulo p^k for some integer $k \geq 1$.

Definition (Quadratic Residue)**.** Let $a, x, m \in \mathbb{Z}$. We say that x is a **quadratic residue** with respect to m if it satisfies the equation

$$x^2 \equiv a \pmod{m}$$

Proposition. Let $a \in \mathbb{Z}$ and $p \neq 2$ be prime such that $p \nmid a$. a has a square root in $\mathbb{Z}_p$ if and only if a is a quadratic residue modulo p.

Proof. Let $P(x) \equiv x^2 - a$. Then $P'(x) = 2x$. Suppose that a is a quadratic residue of p. Then we know

$$a \equiv a_0^2 \pmod{p}, \qquad a_0 \in \{0, 1, 2, \ldots, p-1\}$$

As a result, $P(a_0) = 0 \pmod{p}$. However, $P'(a_0) = 2a_0 \not\equiv 0 \pmod{p}$ because $p \nmid a_0 \Rightarrow \gcd(p, a_0) = 1$. Hence, by Hensel's lemma, $P(x)$ has a solution in $\mathbb{Z}_p$ which means that a has a square root in $\mathbb{Z}_p$. Conversely, if a is a non-quadratic residue with respect to p, then by the previous theorem, it has no square root in $\mathbb{Z}_p$. □

As a result of this proposition, we can see that the imaginary number, $\sqrt{-1}$, is an element of $\mathbb{Z}_5$. This is because $-1 = 4 - 5 \equiv 4 \pmod{5} \equiv 2^2 \pmod{5}$. Since $-1 \equiv 4 \pmod{5}$ and 4 is a quadratic residue with respect to 5, then by our proposition, -1 has a square root in $\mathbb{Z}_p$. Now, we will examine the roots of unity of $\mathbb{Q}_p$.

Definition (Primitive Root Modulo n)**.** Let $g, a, n \in \mathbb{Z}$. We say that g is a **primitive root modulo n** if, for every integer a relatively prime to n, a is congruent to some power of g. In symbols, $a \equiv g^k \pmod{n}$ where $\gcd(a, n) = 1$ and $k \in \mathbb{Z}$.

Definition (Roots of Unity)**.** We call ρ an nth root of unity if $\rho^n = 1$. Additionally, we say that ρ is a primitive nth root of unity if $\rho^n = 1$ such that $\rho^k \neq 1$ for all $k < n$.

Before going over the next proposition, we must first recall the idea of groups and cyclic groups that we learned in Modern Algebra.

Definition (Group)**.** A **group** is a set of numbers G under a single binary operation, denoted by $*$, such that, for all $a, b, c \in G$, it fulfills the following properties:

1. $a * b \in G$ and $b * a \in G$
2. There exists a unique element $e \in G$ such that $e * a = a = a * e$
3. For any $a \in G$, there exists a unique element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Definition (Subgroup)**.** Let G be group. Then a subset $H \subseteq G$ is a **subgroup** of G, written $H \leq G$, if H forms a group under the same binary operation of G.

Definition (Cyclic Group Generated by a)**.** Let a be an element of group G. We write $\langle a \rangle$ to be the **cyclic group** generated by a defined by $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. Furthermore, $\langle a \rangle \leq G$.

Definition (Order of a Group)**.** Let G be a group. The **order** of G, written as $|G|$, is the number of elements in the group.

Proposition. For any prime p and any coprime positive integer m, there exists a primitive mth root of unity in $\mathbb{Q}_p$ if and only if $m|(p-1)$. In the latter case, every mth root of unity is also a $(p-1)$th root of unity. The set of $(p-1)$th roots of unity is a cyclic subgroup of $\mathbb{Z}_p^x$, the units of $\mathbb{Z}_p$, of order $(p-1)$

Proof. Let $m|(p-1)$; then $p - 1 = km$ for $k \geq 1$, and therefore any mth root of 1 is also a $(p-1)$th root of 1. Let

$$f(x) = x^{p-1} - 1, \quad f'(x) = (p-1)x^{p-2}$$

Take $x_0 \in \mathbb{Z}_p^x$ to be any rational integer satisfying $1 \leq x_o \leq p - 1$. Then

$$f(x_0) \equiv 0 \pmod{p} \quad f'(x_0) \not\equiv 0 \pmod{p}$$

since $|f'(x_0)|_p = 1$, and Hensel' lemma applies, giving exactly $p - 1$ solutions, which are the $(p-1)$th roots of 1. The first digits of these roots are $1, 2 \ldots, p - 1$. Conversely, is $\alpha \in \mathbb{Q}_p$ is an mth root of 1, $\alpha^m \equiv 1 \pmod{p}$; hence m divies $p - 1$, the order of $(\mathbb{Z}/p\mathbb{Z})^x$. Since a polynomial with coefficients in a field can only have as many roots as its degree, the polynomial $x^{p-1} - 1$ cannot have more than $p - 1$ roots, and these roots must be the roots of unity in $\mathbb{Q}_p$. It is clear that these roots of unity form a group under multiplcation. Finally, since any finite group of the multiplicative group of any field is cyclic, the group of $(p-1)$th roots of unity is a cyclic subgroup of $\mathbb{Z}_p^x$ of order $p - 1$. □

6.2 Local Analysis and Hasse's Principle

Throughout this paper, we have been looking at $\mathbb{Q}_p$ as a whole. In this section, we wish to emphasize that $\mathbb{Q}_p$ is different for every value of p. With Hensel's lemma, we solved polynomials with p-adic integer coefficients. Things get a little harder when we try to solve a p-adic equation with rational coefficients.

However, there is an important relationship between $\mathbb{Q}$ and each $\mathbb{Q}_p$. That is the fact that $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. Suppose that a polynomial had a root in $\mathbb{Q}$. Then it would be obvious that the polynomial would have a root in each $\mathbb{Q}_p$. We want to consider the converse. What if we could know that the root of a polynomial existed in every $\mathbb{Q}_p$. That is, what if we knew that the root existed locally. That would imply that the root existed in the rational numbers - that it exists globally.

The whole point of finding roots locally in order to find information about the root globally is that it can be easier to find a root locally. We have an example of this below.

Proposition. A number $x \in \mathbb{Q}$ is square if and only if it is a square in every $\mathbb{Q}_p$, $p \leq \infty$.

Solution. For any $x \in \mathbb{Q}_p$, we know from a slight derivation to the product formula that

$$x = \pm \prod_{p<\infty} p^{v_p(x)}.$$

If x is square at infinity (in $\mathbb{R}$), then it is positive. If it is a square at a prime p, then $v_p(x)$ is even. It follows by writing out the prime factorization that x is a square. □

Definition (Diophantine Equations)**.** A **diophantine equation** is an equation in which only integer solutions are allowed. It can have several variables, and the most common form is

$$X^2 + Y^2 = Z^2$$

The diophantine equations are an excellent example of analysis on a local and global scale. Consider the equation

$$X^2 + Y^2 + Z^2 = 0$$

In $\mathbb{R}$, it is clear that this equation does not have a non-trivial solution (that is, $X = Y = Z = 0$). Thus, the result is the same for $\mathbb{Q}$. Likewise, we can check that for the following equation

$$X^2 + Y^2 - Z^2 = 0$$

has a solution in $\mathbb{Q}$ (for example, $X = 4$, $Y = 3$, $Z = 5$) which implies that each field $\mathbb{Q}_p$ also contains a solution. This local-global relationship results in the following principle.

Definition (Local-Global Principle)**.** The existence or non-existence of solutions in $\mathbb{Q}$ (global solutions) of a diophantine equation can be detected by studying, for each $p \leq \infty$, the solutions of the equation in $\mathbb{Q}_p$.

If it was not already clear, the Local-Global Principle is a bit vague. While it is not a theorem, it does provide a plan to study, analyze, and solve certain types of diophantine equations. And as a result, we have several findings due to local analysis such as the following major theorem.

Theorem (Hasse-Minkowski)**.** Let

$$F(X_1, X_2, \ldots, X_n) \in \mathbb{Q}[X_1, X_2, \ldots, X_n]$$

be a quadratic form (that is, homogenious polynomial of degree 2 in n variables). The equation

$$F(X_1, X_2, \ldots, X_n) = 0$$

has non-trivial solutions in $\mathbb{Q}$ if and only if it has non-trivial solutions in $\mathbb{Q}_p$ for each $p \leq \infty$.

The proof of this theorem requires many ideas in the study of quadratic forms, so we will not prove it here. However, the theorem is a major tool in local analysis, and is of great use in modern number theory and diophantine analysis.

6.3 Fermat's Last Theorem

Theorem (Fermat's Last Theorem)**.** For all natural numbers $n > 2$, the equation

$$X^n + Y^n = Z^n$$

has no integral solutions other than the trivial solution where one of the integers X,Y,Z is equal to 0.

Originally conjectured by Pierre de Fermat around 1637, it was not until 1995 when the theorem was completely proven by Andrew Wiles. In the 350 years that it took to prove, this theorem was one of the greatest mysteries and challenges of number theory. It took several discoveries and research by hundreds of individuals in areas including modular forms, elliptic curves, and Galois theory before Wiles could connect the dots.

Throughout the complex proof, p-adic numbers were used constantly to help prove cases of Fermat's last theorem when n was a prime number p or p^m for any $m \in \mathbb{Z}$. Properties of the p-adic norm and the numbers in general allowed several shortcuts and gave us valuable information when the equation was calculated modulo p^m. Unfortunately, it would take an entire paper just to explain all the nuances of the proof due to all the background in the fields it takes to understand it. While we will not be discussing the proof, it is worth mentioning how the p-adic number played such an integral part in proving one of mathematics' most famous theorems.

7 References

1. Katok, Svetlana. 2007. p-adic Analysis Compared with Real. Providence, Rhode Island: American Mathematical Society.
2. Gouvea, Fernando. 1997. p-adic Number. Switzerland: Springer International Publishing.
3. Lang, Serge. 2002. Algebra. Switzerland: Springer International Publishing.
4. Schikhof, Wilhelmus. 2007. Ultrametric Calculus: An Introduction. Cambridge, United Kingdom: Cambridge University Press.
5. Mahler, Kurt. 1973. An Introduction to p-adic Numbers and their Functions. Cambridge, United Kingdom: Cambridge University Press.
6. Ribenboim, Paulo. 2000. Fermat's Last Theorem for Amateurs. Switzerland: Springer International Publishing.
7. Ash, Robert. 2006. Basic Abstract Algebra for Graduate Students and Advanced Undergraduates. Mineola, New York: Dover Publications.
8. Munkres, James. 2015. Topology. London, United Kingdom: Pearson.
9. Hungerford, Thomas. 2012. Abstract Algebra: An Introduction. Independence, Kentucky: Cengage Learning.
10. Gallian, Joseph. 2012. Contemporary Abstract Algebra. Independence, Kentucky: Cengage Learning.

.