P-adic numbers

Mateo Asin Unlu

April 22, 2024

Contents

1 Foundations

1.1 Introduction

We are all innately familiar with $\mathbb{Q}$, the field of rational numbers. And we know that $\mathbb{Q}$ is naturally contained in $\mathbb{R}$. In fact, using a series of constructions, one can show that:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

Interestingly, it turns out that by changing our definition of the absolute value, we are able to show that $\mathbb{Q}$ is also contained within another family of fields called the p-adic fields, expressed $\mathbb{Q}_p$. Giving us that

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{Q}_p$$

Where $\mathbb{Q}_p$ has properties that closely mimic those of $\mathbb{R}$ In this essay I will try and show how to define the field $\mathbb{Q}_p$, some properties of this new field, and touch on how we can take much of the analysis and algebra that we often unleash on $\mathbb{R}$, and instead apply it to $\mathbb{Q}_p$.

2 Constructing the P-adic fields

We construct the p-adic from $\mathbb{Q}$, by completing $\mathbb{Q}$ with respect to a different absolute value, just like how one can construct $\mathbb{R}$ from $\mathbb{Q}$ using completions. If that doesn't make sense, don't worry, it will all be explained in the upcoming section.

2.1 The p-adic absolute value

If we want to come up with a new absolute value, we must first decide on a set of criterion which we would like to preserve when constructing our absolute value.

Definition 2.1. Suppose $\mathbb{F}$ is a field, then an absolute value on $\mathbb{F}$ is defined as a function $|\ |: \mathbb{F} \to \mathbb{R}^{\geq 0}$. That satisfies the following properties:

- $|x| = 0 \quad$ if and only if $\quad x = 0$
- $|xy| = |x||y| \qquad\qquad \forall\, x, y \in \mathbb{F}$
- $|x + y| \leq |x| + |y| \qquad\qquad \forall\, x, y \in \mathbb{F}$

And additionally an absolute value is said to be *non-archimidean* if it satisfies the strong triangle inequality:

- $|x + y| \leq \max |x|, |y| \qquad\qquad \forall\, x, y \in \mathbb{F}$

Note that an absolute value that does not satisfy the final condition is said to be *archimidean*. We can also see that, somewhat counter intuitively, being a non-archimidean absolute value implies that you are an archimidean absolute value. It is trivial to check that our conventional absolute value, defined here as:

$$|x|_\infty = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

satisfies the properties of an absolute value.

It is also important to note that although this is very similar to the definition of a norm, an absolute value is defined on a field, while a norm is defined on a vector space, meaning an absolute value operates on scalars, while a norm operates on vectors. A norm also uses an absolute value as part of its definition (within the condition that $||\lambda x|| = |\lambda|||x|| \quad \forall\, x \in V, \lambda \in \mathbb{F}$). This gives us the notion that an absolute value is a more fundamental concept than a norm. And indeed changing the way the absolute value is defined changes many fundamentals of the topology and geometry of the field on which it's defined.

It turns out that it's possible to generate a new absolute value function on the field $\mathbb{Q}$ with each prime number p. Suppose we start with an arbitrary $a \in \mathbb{Q}$, and we choose a prime number p around which to base our absolute value.

Since $a \in \mathbb{Q}$ we can write it as a fraction in its lowest terms. Therefore let

$$a = \frac{b}{d} \quad \text{where} \quad b, d \in \mathbb{Z} \quad \text{and} \quad b, d \quad \text{are coprime}$$

We can then factor out as many possible powers of p from our fraction as we can. Leaving us witha number of the form:

$$a = \frac{b}{d} = p^n \frac{b'}{d'} \quad n \in \mathbb{Z} \quad \text{where} \quad p, b', d' \quad \text{are coprime}$$

Note that there are many different terminologies for this, but in this essay I will refer to writing $a \in \mathbb{Q}$ like this as 'p-multiplicity form'. It also comes naturally to define the 'p-multiplicity' of 0 as infinity, since we can infinitely pull out a factor of p from 0, independent of the prime chosen. We can look at a few examples for clarification:

Example 2.1. Expressing $\frac{54}{5}$ and $\frac{7}{9}$ in 3-multiplicity form

$$\frac{54}{5} = 27 \times \frac{2}{5} = 3^3 \times \frac{2}{5}$$
$$\frac{7}{9} = \frac{1}{9} \times 7 \ = 3^{-2} \times 7$$

Note that n can be negative, if the denominator has factors of p as well.

Definition 2.2. (P-adic absolute value)

Suppose $a \in \mathbb{Q}$ and $a = \frac{b}{d} = p^n \frac{b'}{d'}$ when written in 'p-multiplicity form' then the *p-adic absolute value* on a, $|a|_p$, is defined as:

$$|a|_p = \begin{cases} |p^n \frac{b'}{d'}|_p = p^{-n} & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases}$$

Proposition 2.1. *The p-adic absolute value, $|\ |_p$ satisfies the definition of a non-archimidean absolute value*

Proof. In order to prove this, we must check the first two conditions for an absolute value, and then the condition for a non-archimidean absolute value. Recall that the strong triangle inequality implies the triangle inequality therefore we do not need to explicitly check that condition.

1. Starting with the first condition, by the definition we can clearly see that if $a = 0$, then $|0|_p = 0$, furthermore since $p^{-n} \neq 0$ for all $n \in \mathbb{N}$ and p prime, we know that if $|a|_p = 0$ then $a = 0$. Therefore $|a|_p = 0$ if and only if $a = 0$

2. suppose that $a = \frac{b}{d} = p^n \frac{b'}{d'}$ and $e = \frac{f}{g} = p^m \frac{f'}{g'}$, then we know that

$$|a|_p|e|_p = |p^n \frac{b'}{d'}|_p|p^m \frac{f'}{g'}|_p = p^{-n}p^{-m} = p^{-(m+n)}$$

$$|ae|_p = |(p^n \frac{b'}{d'})(p^m \frac{f'}{g'})|_p = |p^{n+m}(\frac{b'}{d'})(\frac{f'}{g'})|_p = p^{-(n+m)}$$

   Note that the last line of the proof follows from the fact that $p \nmid \frac{p'}{q'}$ and $p \nmid \frac{r'}{s'}$, therefore we know that $p \nmid (\frac{p'}{q'})(\frac{r'}{s'})$ since p is prime. In face this gives us the fundamental reason why we are restricted to looking at the 'p multiplicity' of numbers in $\mathbb{Q}$. Since this multiplicative property does not nescessarily hold if we choose some $c \in \mathbb{N}$ where c is composite. This explains why when we start examining elements of $\mathbb{Q}_p$ we are restricted to working in base p.

3. Suppose again that $a = \frac{b}{d} = p^n \frac{b'}{d'}$ and $e = \frac{f}{g} = p^m \frac{f'}{g'}$ but now assume without loss of generality, that $m \geq n$, then we know that

$$|a + e|_p = |p^n \frac{b'}{d'} + p^m \frac{f'}{g'}|_p = |p^n(\frac{b'}{d'} + p^{(m-n)} \frac{f'}{g'})|_p$$

   Recall that since $m \geq n$, we know that $m - n \geq 0$, therefore we know that $p^{m-n} \in \mathbb{N}$, therefore we can add it to the numerator of the fraction. Therefore we get that:

$$|p^n(\frac{b'}{d'} + p^{(m-n)} \frac{f'}{g'})|_p = |p^n(\frac{b'}{d'} + \frac{p^{(m-n)} f'}{g'})|_p = |p^n(\frac{b'g' + p^{m-n}d'f'}{d'g'})|_p \qquad (*)$$

   Again using the fact that p is prime, we realise that since $p \nmid d'$ and $p \nmid g'$ we know that $p \nmid d'g'$ furthermore, since $p \nmid b'g'$ we know that $p \nmid (b'g' + p^{m-n}d'f')$ Therefore there are no more factors of p to take from the numerator or the denominator, therefore the expression in $(*)$ is already in 'p multiplicity form'. Therefore we have that:

$$|p^n(\frac{b'g' + p^{m-n}d'f'}{d'g'})|_p = p^{-n} = \max(p^{-n}, p^{-m}) = \max(|a|_p, |e|_p)$$

   Recall since $m \geq n$ we have that $p^{-n} \geq p^{-m}$ therefore we know that

$$|a + e|_p \leq \max(|a|_p, |e|_p)$$

And we know that our p-adic absolute value satisfies all the necessary conditions to be a non-arhcimidean absolute value. □

Example 2.2. Finding $|45|_5$, $|\frac{2}{7}|_7$ and $|9|_2$

$$|45|_5 = |5^1 \times 9|_5 = 5^{-1} = \frac{1}{5}$$

$$|\frac{2}{7}|_7 = |7^{-1} \times 2|_7 = 7^1 = 7$$

$$|9|_2 = |2^0 \times 9|_2 = 2^0 = 1$$

Although it seems arbitrary to define the p-adic absolute value in this way, there is a beautiful theorem called Ostrowski's theorem that tells us that the way we have defined the absolute value in definition 2.1 restricts us to very few possible options for an absolute value defined on $\mathbb{Q}$.

Theorem 2.1 (Ostrowski's theorem)**.**

The only possible absolutes values defined on $\mathbb{Q}$ are:

- *the conventional absolute value here denoted $|\ |_\infty$.*[1]
- *the trivial absolute value, where $|0| = 0$ and $|x| = 1$ for all $x \neq 0$, often denoted as $|\ |_0$.*
- *a p-adic absolute value for some prime p, i.e. $|\ |_p$.*
- *a variation of one of the previous absolute values of the form $|\ |^\alpha$ for some $\alpha \in \mathbb{R}$.*

Note that an absolute value of the form $|\ |_*^\alpha$ induces the same topology on $\mathbb{Q}$ as $|\ |_*$. Therefore we say that $|\ |_*$ and $|\ |_*^\alpha$ are topologically equivalent. Therefore it's not that arbitrary at all to define the p-adic absolute value like this, not only is it natural, it's the only type of absolute value that is topologically different to $|\ |_\infty$ and $|\ |_0$

The proof is rather long, and requires some more results to be proven about the absolute value, so it has been omitted from the essay, but the mathematics required to prove it is of a level most undergraduates have already mastered.[1, p. 56-59]

Example 2.3. With respect to the 5-adic absolute value. $|628 - 3|_5 < |4 - 2|_5$

$$|628 - 3|_5 = |625|_5 = |5^4 \times 1|_5 = 5^{-4} = \frac{1}{625}$$

$$|4 - 2|_5 = |2|_5 = |5^0 \times 2|_5 = 5^0 = 1$$

$$\text{therefore, since} \quad \frac{1}{625} < 1 \quad \text{it means} \quad |628 - 3|_5 < |4 - 2|_5$$

This gives us the notion that with respect to the 5-adic absolute value, 628 and 3 are closer together than 4 and 2.

[1] We use ∞ because the conventional absolute value can be thought of a p-adic value of an arbitrarily big prime, one so large that it is never a factor of any finite number. It is equivalent to taking the limit as $p \to \infty$

2.2 Completions of $\mathbb{Q}$

We will now show how we can use this new absolute value to create the field of p-adics ($\mathbb{Q}_p$), in order to do this we first need to examine how analysis on a field changed with a different absolute value. We can see that the abstraction of the absolute value gives us a new, more general notion of convergence,

Definition 2.3. Given a field $\mathbb{F}$ and a non-trivial absolute value defined on that field, $|\ |_*$, we say that a sequence x_n in $\mathbb{F}$ converges (with respect to $|\ |_*$) to x if $\quad \forall\, \varepsilon > 0$ there exists $N \in \mathbb{N}$ such that $\quad \forall\, n \geq N \quad |x_n - x|_* \leq \varepsilon$ here in this essay it will be denoted as $x^n \to_* x$.

Example 2.4. From this definition we can see that $p^n \to_p 0$ as $n \to \infty$ for an arbitrary p.

This is interesting since $p^n \to \infty$ with respect to $|\ |_\infty$. We can now start to see a little how the p-adic absolute value can be used to digest the concept of infinity in different ways.

We can use our new ideas of convergence to define a more general way of thinking about Cauchy sequences, which will come in useful in completing the field of p-adics.

Definition 2.4. Suppose that $|\ |_*$ is an absolute value defined on a field $\mathbb{F}$. We say that a sequence x_n is *Cauchy* if $\quad \forall\, \varepsilon > 0$, there exists $N \in \mathbb{N}$ such that if $m, n > N$, then $|x_m - x_n|_* \leq \varepsilon$

Now we can use this new absolute value together with the notion of a Cauchy sequence to construct a new field in which $\mathbb{Q}$ will be contained.

Definition 2.5. A field $\mathbb{F}$ is called complete with respect to an absolute value $|\ |_*$ if every sequence that is Cauchy with respect $|\ |_*$ to has a limit in $\mathbb{F}$.

As an example the rationals, paired up with $|\ |_\infty$ $(\mathbb{Q}, |\ |_\infty)$ is not a complete field. This becomes clear if we look at the sequence:

$$\begin{aligned} x_1 &= 2 \\ x_2 &= 2.7 \\ x_3 &= 2.71 \\ x_4 &= 2.718 \\ &\vdots \end{aligned}$$

Despite it being a crudely constructed sequence we can see that $x_n \to e$ as $n \to \infty$. Supposing $m > n, \quad |x_m - x_n|_\infty \geq$ The n^{th} digit of x_n. And since the absolute value of the n^{th} digit can be made arbitrarily small, the sequence is also Cauchy sequence. Therefore $\mathbb{Q}$ is not complete with respect to $|\ |_\infty$.
It turns out its actually possible to *complete* a field with respect to an absolute value, by including all the limits of all the Cauchy sequences in an incomplete field into a new field.

Definition 2.6. (Completing a field)
The process of completing a field involves some advanced concepts from abstract Algebra, but

nothing that is out of the grasp of an undergraduate student. Having said that, if one does not feel like brushing up on their knowledge of abstract Algebra, they can skip this definition. The added complication comes from the fact that we have not defined the limits of the Cauchy sequences, the trick is to define the limits as the sequences themselves.

Suppose we have a field $\mathbb{F}$ and an absolute value $|\ |_*$ where $\mathbb{F}$ is incomplete with respect to $|\ |_*$. The process of completing $\mathbb{F}$ involves defining

$$\zeta_* = \{(x_n)_{n=0}^{\infty} \in \mathbb{F} : x_n \text{ is Cauchy with respect to} |\ |_*\}$$

We can notice that the set ζ_* is a ring when considering term wise multiplication and addition. Note that ζ_* is not a field since there are infinite zero divisors.

The issue with ζ_* is that there are many elements of ζ_* with the same limit, therefore we need some way to get rid of them. We do this by defining

$$\aleph_* = \{(x_n)_{n=0}^{\infty} \in \zeta_* : x_n \to 0 \text{ as } n \to \infty\}$$

$\aleph_*$ is an ideal since any sequence multiplied by a sequence that tends to zero also tends to zero.

And if we let $\mathbb{F}'$ be the completion of $\mathbb{F}$ since $\aleph_*$ is an ideal and ζ_* is an ideal then we can just take the quotient of ζ_* by $\aleph_*$ to get that:

$$\mathbb{F}' = \zeta_*/\aleph_*$$

This ring quotient might be a bit confusing, but just remember that the ring quotient is the set of all cosets with respect to the ideal $\aleph_*$, therefore the quotient ring $\zeta_*/\aleph_*$ is just the original ring partitioned into equivalence classes of sequences that differ by null-sequences.

Note that there is a lot of legwork required to prove that this definition behaves in the way that we want it to, and to achieve rigour. For example one must prove that ζ_* is indeed a ring,that the completion is indeed a field, that the completion contains the original field and that $\mathbb{F}$ and preserves its structure within the new field. Again proving all of these things is a bit outside the scope of this essay, but a proof can be found in this book. [1, p. 64-67]

Corollary 2.2. *The completion of* $\mathbb{Q}$ *with respect to* $|\ |_\infty$ *yields* $\mathbb{R}$.

Well it turns out that $\mathbb{Q}$ is also incomplete with respect to $|\ |_p$ as well [1, p. 63-64]. This means that it is possible to complete $\mathbb{Q}$ with respect to $|\ |_p$ instead.

Definition 2.7. (The field of p-adic numbers)
The field obtained by completing $\mathbb{Q}$ with respect to $|\ |_p$, i.e the field obtained by including all the possible limits of all the possible sequences which are Cauchy with respect to $|\ |_p$ with elements in the field $\mathbb{Q}$ is called the field of *p-adic numbers* denoted $\mathbb{Q}_p$.

Note that each prime number p generates a distinct absolute value $|\ |_p$ and by extension generates a distinct field $\mathbb{Q}_p$, the term 'field of p adic numbers' can often be confusing since it is an infinite family of fields, not just one.

3 Examining $\mathbb{Q}_p$

3.1 How to express a p-adic

We can see that $p^n \to_p 0$ as $n \to \infty$ and also that $p^{-n} \to_p \infty$ as $n \to \infty$ for any chosen p (Recall that $|p^n|_p = p^{-n}$). This has interesting implications. It turns out that all series of the form

$$\sum_{i=k}^{\infty} a_i p^i \quad \text{for some} \quad k \in \mathbb{Z}$$

will always converge in $\mathbb{Q}_p$.

As it turns out, any $x_p \in \mathbb{Q}_p$, can be expressed as a *unique* sequence of the form $\sum_{i=k}^{\infty} a_i p^i$ for some $k \in \mathbb{Z}$. So within $\mathbb{Q}_p$ we uniquely determine each number by just referring to its infinite series.

This seems like an odd thing to do, until we realise that we do something very similar when expressing a number in $\mathbb{R}$, just with a series of the form $\sum_{i=k}^{\infty} a_i (10)^{-i}$ for some $k \in \mathbb{Z}$ instead. This is just the decimal expansion of any number in $\mathbb{R}$. For example:

$$\pi = 3.1415\cdots = 3(10)^0 + 1(10)^{-1} + 4(10)^{-2} + 1(10)^{-3} + 5(10)^{-4} + \ldots \quad \text{In this case} \quad k = 0$$
$$\sqrt{777} = 27.874\cdots = 2(10)^1 + 7(10)^0 + 8(10)^{-1} + 7(10)^{-2} + 4(10)^{-3} + \ldots \quad \text{In this case} \quad k = 1$$

We just dont realise this is an infinite series due to the notation of digits that we normally use.

In general, in a p-adic space, if we express a number as a sequence of digits in base p, each digit decreases in value left of the decimal point, and increases in value to the right of the decimal point.

$$\text{in } \mathbb{R}: \quad \underbrace{\ldots a_3 p^3 + a_2 p^2 + a_1 p}_{\text{digits increase in value}} + a_0 + \underbrace{a_{-1} p^{-1} + a_{-2} p^{-2} + a_{-3} p^{-3} \ldots}_{\text{digits decrease in value}}$$
$$\text{in } \mathbb{Q}_p: \quad \underbrace{\ldots a_3 p^3 + a_2 p^2 + a_1 p}_{\text{digits } \textit{decrease} \text{ in value}} + a_0 + \underbrace{a_{-1} p^{-1} + a_{-2} p^{-2} + a_{-3} p^{-3} \ldots}_{\text{digits } \textit{increase} \text{ in value}}$$

where each a_i is an integer between 0 and p.

As an example, let us consider:

$$\sum_{i=1}^{\infty} 4(5)^i \in \mathbb{Q}_5$$

Which is equivalent to the sum:

$$4(5)^0 + 4(5)^1 + 4(5)^2 \ldots \tag{1}$$

But since it is cumbersome to constantly write out this infinite sum, we can just resort to writing it out as digits in base 5, similarly to how we express an infinite sum of decreasing

powers of 10 in $\mathbb{R}$ as digits in base 10. But since the infinite sum (1) is composed of increasing powers of 5, we have to write it as an infinite string of 5's trailing of to the left instead of the right. In this essay I will use bold and a subscript to denote numbers written in a different base.

$$\ldots\mathbf{4444}_5 = 4(5)^0 + 4(5)^1 + 4(5)^2 + 4(5)^3 \cdots = \sum_{i=1}^{\infty} 4(5)^i \in \mathbb{Q}_5 \tag{2}$$

Which *is* exactly the equation that was specified in (1). Therefore it makes sense to write $\ldots\mathbf{4444}_5$, when trying to write down an element of $\mathbb{Q}_5$.

Interestingly, $\ldots\mathbf{4444}_5$ is not just any random element of $\mathbb{Q}_5$, in fact we can prove in 2 separate ways that $\ldots\mathbf{4444}_5 = -1$

Proposition 3.1. $-1 = \ldots\mathbf{4444}_5$ *in* $\mathbb{Q}_5$

Proof. let $\ldots\mathbf{4444}_5 = x$

$$\begin{aligned}\ldots\mathbf{4444}_5 &= x\\ \ldots\mathbf{4440}_5 &= 5x\end{aligned}$$

Note that since we are working in base 5 we multiplication by 5 causes all digits to move 1 to the left, now if we subtract the two equations

$$\begin{aligned}\ldots\mathbf{0004}_5 &= -4x\\ 4 &= -4x\\ x &= -1\end{aligned}$$

□

This is very similar to the method learned in secondary scool that was used to prove that $0.333\cdots = \frac{1}{3}$ in $\mathbb{R}$

Proof. the second proof is much simpler, we just add 1!

$$\begin{array}{r} \ldots\mathbf{^1 4^1 4^1 4^1 4^1 4}\ \mathbf{4}_5 \\ + \qquad\qquad\qquad \mathbf{1}_5 \\ \hline \ldots\ \mathbf{0\ 0\ 0\ 0\ 0\ 1} \end{array}$$

And since $\ldots\mathbf{4444}_5 + 1 = 0$ it naturally follows that $\ldots\mathbf{4444}_5 = -1$.

□

Let us refer back to (1) one last time. Notice that:

$$|\ldots\mathbf{4444}_5|_5 = |4(5)^0 + 4(5)^1 + 4(5)^2 + 4(5)^3 \ldots|_5$$

$$\leq \max[|4(5)^0|_5, |4(5)^1|_5, |4(5)^2|_5, |4(5)^3|_5 \ldots] \quad \text{By the strong triangle inequality}$$

$$= |4(5)^0|_5 = 5^0 = 1$$

Therefore we have that

$$|\ldots \mathbf{4444}_5|_5 = 1 = |-1|_5$$

Which is what we want, considering that we just proved that in $\mathbb{Q}_5$, $\ldots \mathbf{4444}_5 = -1$. Now instead let us calculate:

$$|\mathbf{4.444}_5 \ldots|_5 = |4(5)^0 + 4(5)^{-1} + 4(5)^{-2} + 4(5)^{-3} \ldots|_5$$
$$\leq \max[\, |4(5)^0|_5, |4(5)^{-1}|_5, |4(5)^{-2}|_5, |4(5)^{-3}|_5 \ldots]$$

Now recall that $|p^{-n}|_p \to \infty$ as $n \to \infty$, therefore we know that:

$$\max[\, |4(5)^0|_5, |4(5)^{-1}|_5, |4(5)^{-2}|_5, |4(5)^{-3}|_5 \ldots] = \lim_{n\to\infty} |5^{-n}|_5 = \infty$$

This all helps us see that with respect to the 5-adic absolute value:

$$|\mathbf{4.444}_5 \ldots|_5 = \infty$$
$$|\ldots \mathbf{4444}_5|_5 \neq \infty$$

And with respect to the conventional absolute value:

$$|\ldots \mathbf{4444}_5|_\infty = \infty$$
$$|\mathbf{4.444}_5 \ldots|_\infty \neq \infty$$

Interestingly the similarities between $\mathbb{Q}_p$ and $\mathbb{R}$ continue. We can show that periodic strings of digits are rational in $\mathbb{Q}_p$ just as they are also rational in $\mathbb{R}$.

Suppose that

$$a = \ldots \mathbf{a^4 a^3 a^2 a^1}_p \quad \text{is an expansion in } \mathbb{Q}_p$$
$$b = \quad b^1 b^2 b^3 b_p^4 \ldots \quad \text{is an expansion in } \mathbb{R} \text{ (in base p)}$$

Then we know that:

$$\text{if } (b_n)_{n=0}^{\infty} \text{ is eventually periodic, then } b \in \mathbb{Q}$$
$$\text{and if } (b_n)_{n=0}^{\infty} \text{ is never periodic, then } b \notin \mathbb{Q}$$

Similarly with $\mathbb{Q}_p$

$$\text{if } (a_n)_{n=0}^{\infty} \text{ is eventually periodic, then } a \in \mathbb{Q}$$
$$\text{and if } (a_n)_{n=0}^{\infty} \text{ is never periodic, then } a \notin \mathbb{Q}$$

The proof is omitted, since it has to be proved for many separate cases, but it follows the same lines as the methods used to prove that periodic sequences of digits correspond to a rational number in $\mathbb{R}$.

3.2 Calculations with the p-adics

The computations required to perform operations on the p-adics can sometimes be a little involved, but very often follow the same algorithms for operations on elements of $\mathbb{R}$

Example 3.1. (P-adic addition) Let us try and add $\ldots\mathbf{3333}_5$ and $\ldots\mathbf{2424}_5$ in $\mathbb{Q}_5$. We will use the same methods as one would use when performing column addition on two numbers, remembering to 'carry the 1' when one of our coefficients exceed 5, since we are working in base 5.

$$\begin{array}{r} \ldots{}^{\mathbf{1}}\mathbf{3}^{\mathbf{1}}\mathbf{3}^{\mathbf{1}}\mathbf{3}^{\mathbf{1}}\mathbf{3}^{\mathbf{1}}\mathbf{3}\ \mathbf{3}_5 \\ +\ldots\ \mathbf{2\ 4\ 2\ 4\ 2\ 4}_5 \\ \hline \ldots\ \mathbf{1\ 3\ 1\ 3\ 1\ 2}_5 \end{array}$$

Using the same method, we can also subtract the same 2 integers, however we have to note that sometimes we have to 'bring the 1 down' from the next column in order to not get a negative number. Since we are working in base 5, this is akin to adding 5 to the result in the column. Either way, performing the subtraction we get:

Example 3.2. (P-adic subtraction)

$$\begin{array}{r} \ldots\mathbf{333333}_5 \\ -\ldots\mathbf{242424}_5 \\ \hline \ldots\mathbf{040404}_5 \end{array}$$

We can also easily check our answers using the addition defined in (3.1) to find that $\ldots\mathbf{0404}_5 + \ldots\mathbf{2424}_5 = \ldots\mathbf{3333}_5$ verifying our findings.

It is even possible to multiply, noting that each column is only affected by a finite number of coefficients. For example, the third column is affected only by coefficients in the first 3 columns of the answer. We will again use the methods of column multiplication that we are familiar with from $\mathbb{R}$.

Example 3.3. (P-adic multiplication)

$$\begin{array}{r} \ldots\mathbf{3333}_5 \\ \times\ldots\mathbf{2424}_5 \\ \hline \ldots\mathbf{4442}_5 \\ \ldots\mathbf{2210}_5 \\ \ldots\mathbf{4200}_5 \\ +\ldots\mathbf{1000}_5 \\ \hline \ldots\mathbf{2402}_5 \end{array}$$

Example 3.4. $\frac{1}{2} = \ldots\mathbf{1112}_3$ in $\mathbb{Q}_3$

We will prove this by proving that $\ldots\mathbf{1112}_3 \times \ldots\mathbf{0002}_3 = 1$

$$\begin{array}{r} \ldots\mathbf{1112}_3 \\ \times \qquad \mathbf{2}_3 \\ \hline \ldots\mathbf{0001}_5 \end{array}$$

If one finds it hard to remember column multiplication we can also use a rewriting trick for this specific case.

$$\begin{aligned} \ldots\mathbf{1112}_3 &= \ldots\mathbf{1110}_3 + \mathbf{2}_3 \\ 2 \times \ldots\mathbf{1112}_3 &= 2(\ldots\mathbf{1110}_3 + \mathbf{2}_3) \\ 2 \times \ldots\mathbf{1112}_3 &= 2 \times \ldots\mathbf{1110}_3 + 2 \times \mathbf{2}_3 \\ &= \ldots\mathbf{2220}_3 + \mathbf{11}_3 \\ &= \ldots\mathbf{0001}_3 = \mathbf{1}_3 \end{aligned}$$

Division is slightly more involved. Instead of being able to directly divide $\ldots\mathbf{2424}_5$ by $\ldots\mathbf{3333}_5$, it is instead easier to ask the question: What number, when multiplied by $\ldots\mathbf{3333}_5$ yields $\ldots\mathbf{2424}_5$?. We will denote the digits of this new number as $\ldots a_3a_2a_1a_0$.

Example 3.5. (P-adic division)

$$\begin{array}{r} \ldots\ \mathbf{3\ 3\ 3\ 3}_5 \\ \times \ldots a_3a_2a_1a_0 \\ \hline \ldots\ \mathbf{2\ 4\ 2\ 4}_5 \end{array}$$

We can just work backwards to figure out each digit. Noting that each a_i must be an integer between 0 and 4. We can see that in order to find a_0 we have to solve the congruence equation $3a_0 \equiv 4 \pmod 5$. Giving us that $a_0 = 3$. We can now use a trick to calculate the next digit. We know that:

$$\begin{aligned} a_3a_2a_1a_0 &= a_3a_2a_1\mathbf{0}_5 + a_0 \\ a_3a_2a_1a_0 &= a_3a_2a_1\mathbf{0}_5 + \mathbf{3}_5 \\ (\ldots\mathbf{3333}_5)(a_3a_2a_1a_0) &= (\ldots\mathbf{3333}_5)(a_3a_2a_1\mathbf{0}_5 + \mathbf{3}_5) \end{aligned}$$

Recalling that $(\ldots\mathbf{3333}_5)(\ldots a_3a_2a_1a_0) = \ldots\mathbf{2424}_5$ As per the condition we set at the start of the question, therefore:

$$\begin{aligned} \ldots\mathbf{2424}_5 &= (\ldots\mathbf{3333}_5)(a_3a_2a_1\mathbf{0}_5 + \mathbf{3}_5) \\ \ldots\mathbf{2424}_5 &= (\ldots\mathbf{3333}_5)(a_3a_2a_1\mathbf{0}_5) + (\ldots\mathbf{3333}_5)(\mathbf{3}_5) \end{aligned}$$

We can calculate $\ldots\mathbf{3333}_5 \times \mathbf{3}_5$ using the multiplication we already know to get:

$$\ldots\mathbf{2424}_5 = (\ldots\mathbf{3333}_5)(a_3a_2a_1\mathbf{0}_5) + \ldots\mathbf{1104}_5$$
$$\ldots\mathbf{1320}_5 = (\ldots\mathbf{3333}_5)(a_3a_2a_1\mathbf{0}_5)$$

We can then repeat the original step except in the second column to find a_1

$$\begin{array}{r} \ldots\ \mathbf{3\ 3\ 3\ 3}_5 \\ \times\ldots a_3a_2a_1\mathbf{0}_5 \\ \hline \ldots\ \mathbf{1\ 3\ 2\ 0}_5 \end{array}$$

The manipulation of the numbers has helped us to get a 0 in the units column of the unknown number, reducing the calculations of a_1 to just another congruence equation, namely $3a_1 \equiv 2 \pmod 5$ giving us that $a_1 = 4$.

As we can see this process is quite intensive, but it can be repeated infinitely to find all the digits and to find that; (Up to the first 4 digits)

$$\ldots\mathbf{3333}_5 \times \ldots\mathbf{2343}_5 = \ldots\mathbf{2424}_5$$

And by extension:

$$\frac{\ldots\mathbf{2424}_5}{\ldots\mathbf{3333}_5} = \ldots\mathbf{2343}_5$$

This again shows us why it is so important to restrict ourselves to bases of prime numbers, since the congruence equations required to find the values of the digits are only guaranteed to have unique solutions if we are working modulo a prime number.

Interestingly in all the above examples I chose periodic p-adic numbers to do my calculations, as I showed before, rational numbers yield periodic expansions in $\mathbb{Q}_p$, and since $\mathbb{Q}$ is a field we know it is closed under addition, subtraction, multiplication and division. That explains why 2 periodic p-adic numbers under one of the four basic arithmetic operations yields another periodic p-adic number.

As it turns out we can use these methods to compute any negative number in any p-adic field using the method of subtraction, defined in (3.2), or by multiplying -1 by the desired number using the multiplication defined in (3.3).

But it's not only negative numbers, using the methods of division defined in (3.5) we can divide 2 finite integers to obtain a fraction in $\mathbb{Q}_p$ that is an infinite string of digits. The process of computing p-adic fractions is quite cumbersome (its just p-adic division of 2 finite numbers) but the verification is rather easy, we just have to multiply by the denominator and verify that we have the desired finite integer, much akin to what we did for example (3.4).

4 Uses of p-adics

4.1 The future of P-adics

We now have a grasp of what the elements in the field of p-adics looks like, and how we can perform some basic operations on them but there is still so much left to unlock from $\mathbb{Q}_p$.

The analytical techniques that work in $\mathbb{R}$ also work in $\mathbb{Q}_p$, allowing us to define functions, continuity and derivatives in $\mathbb{Q}_p$. We can then use these ideas to explore more complex ideas like power series and integration in $\mathbb{Q}_p$.

It is possible to create vector spaces over $\mathbb{Q}_p$, allowing us to meet the p-adic brother of linear algebra.

A lot of the current focus of p-adic revolves around p-adic polynomials, i.e. polynomials with coefficients and solutions in $\mathbb{Q}_p$.[2]. With arguably the cornerstone of the p-adic space being Hensel's Lemma, guaranteeing the existence of roots of these polynomials in most cases.

$\mathbb{Q}_p$ can also be extended to $\mathbb{C}_p$, allowing solutions for the aforementioned functions in the p-adic complex plane. It is also possible to perform analysis on p-adic complex functions. $\mathbb{C}_p$ leads to the idea of a Newton polygon, allowing us to better visualise the graphs of p-adic functions.

Really, there is so much more beyond this essay to learn about the p-adics, and I highly recommend looking at some of the sources in the bibliography for further reading.

4.2 Uses within Greater Mathematics

Although it might seem like we just arbitrarily constructed $|\ |_p$ we find that p-adic tools are a very versatile tool in our mathematical arsenal. Their non-archimidean topology makes them particularly good at solving Diophantine equations. Diophantine equations are equations in which we are only looking for solutions in $\mathbb{Q}$. For example:

$$x^2 + x^4 + x^8 = y^2 \qquad x, y \in \mathbb{Q}$$

While we can easily sketch a graph of the equation in $\mathbb{R}^2$ to find an uncountable infinity of solutions, finding solutions in $\mathbb{Q}$ is a more difficult affair. It turns out that the p-adics are the perfect tool for this. Look to [2, 13:01] for a beautifully animated example of how p-adics can be used to solve this exact problem.

p-adics are also a powerful tool for solving congruence equations, allowing for rapid computation of solutions to equivalence relations.

4.3 Applied uses

Due to their use in number theory and finding solutions to problems in $\mathbb{Q}_p$, p-adics are used a lot in cryptography, since in modern cryptography involves trying to find integer solutions [3] to

[2] More specifically $\mathbb{Z}_p$ which is defined as a *valuation ring* on $\mathbb{Q}_p$

[3] Think large primes

equations. Modern cryptography also makes use of congruence equations modulo large primes, another thing that the p-adics excel at solving.

p-adic numbers also have (while understandably more limited than $\mathbb{R}$) applications in physics. p-adic numbers have found applications in the study of spin glasses, which are disordered magnetic systems that happen to exhibit novel behaviour. p-adic numbers provide a mathematical framework to model and analyze certain aspects of spin glass systems. The use of the p-adics in physics, and their appearance in nature solidifies the authenticity of the p-adic field as an important part of mathematics.

The imaginary unit $\mathbf{i}$ used to be a mathematical oddity, only used by other mathematicians in theoretical calculations, until Schrodinger famously used it in his wave equation to model the motion of small particles, at which point the it was accepted that $\mathbf{i}$ was more than just a mathematical construct. In fact, the fact that p-adic numbers have started to appear in isolated pockets of physics showing that the p-adic fields are far more than mathematical constructs.

In fact, there is a hypothesis called the Vladimirov Hypothesis, that postulates that the fundamental geometry of space time, at the Planck level, follows $\mathbb{Q}_p^d$ rather than $\mathbb{R}^d$. Of course, this is just a theory, with no substantial proof behind it, however it is more than possible that the p-adic topology is more prevalent in our world than we think!

References

[1] Fernando Q Gouvêa. *p-adic numbers*. Springer, Waterville, ME, USA, 2020. A good introduction with a lot of problems.

[2] Derek Muller. Mathematicians use numbers differently from the rest of us. `https://www.youtube.com/watch?v=tRaq4aYPzCc&t=1221s`, 2023. A fantastic overview with clear graphics, excellent for a beginner.

[3] Jonathan Rokker. Introduction to p-adic numbers. `https://www.youtube.com/watch?v=vdjYiU6skgE`, 2011. Explains some of the more technical details in a video format.