Power of Primes

An Introduction to p-adic Numbers

Accompanying notes for the talk given by

Niko Laaksonen

n.laaksonen@ucl.ac.uk

at UCL Mathematics Undergraduate Colloquium on

18^{th} March 2010

What are p-adic numbers? What are they good for? Why aren't the real numbers enough? These are few of the questions this talk will try to shed light on. We will introduce these curious objects, and learn how to do basic arithmetical manipulations with them. From here we will start exploring all the beautiful and striking phenomena in this so called ultrametric space of p-adic numbers, $\mathbb{Q}_p$, and hopefully see that, at least in some cases, we get more intuitive results than in real analysis! Finally, if time permits, we will have a quick glance at the algebraic side of the p-adic numbers, especially the queer nature of the field extensions of $\mathbb{Q}_p$.

Note! In this text we denote *integers modulo* $n \in \mathbb{N}$ by $\mathbb{Z}/n\mathbb{Z}$, while the usual $\mathbb{Z}_p$ denotes the ring of p-adic integers. Moreover $\mathbb{N} = \mathbb{Z}_+ \cup \{0\}$.

1 Prelude

In this talk we will first approach p-adic numbers from the point of view of p-adic expansions. Historically, this was also the way mathematicians began to realize this field of numbers. As you may know, there is a strong analogy between the integers $\mathbb{Z}$ along with its field of fractions $\mathbb{Q}$, and complex polynomials of one variable $\mathbb{C}[X]$ together with the field of rational functions $\mathbb{C}(X)$. For instance, there is a clear notion of a prime element in both $\mathbb{Z}$ and $\mathbb{C}[X]$. A German mathematician **Kurt Hensel (1861-1941)** was intrigued by this analogue and wanted to extend it further. Take a function $f \in \mathbb{C}[X]$, we know that it's possible to find its Laurent expansion at any point of $\mathbb{C}$. This expansion gives information about the function at and close to that point, such as zeroes or poles. Hensel asked whether it was possible to do something similar for any $x \in \mathbb{Q}$ (actually for algebraic numbers, but this suffices here). This consideration is sometimes called *Hensel's Analogy* and it lead him to introduce the p-adic numbers in the late 19^{th} century.

It is not hard to see how this could work for some $n \in \mathbb{N}$. Take, for example, an integer 24. We are used to writing its base-10, or *decimal*, expansion which would be $4 + 2 * 10$. Now, let us fix a prime (for reasons we will explain later) $p = 5$, for instance, and consider the base-5 expansion of 24. We can see it is

$$24 = 4 + 4 * 5.$$

Similarly,

$$79 = 4 + 3 * 5^2.$$

We will also call these *5-adic* expansions. Simple so far, but how to find the 5-adic expansion of -1 for example? We of course want it to satisfy $-1 + 1 = 0$. Here's a magic trick

$$-1 = 4 + 4 * 5 + 4 * 5^2 + \dots$$

See, now if we add 1 and keep in mind that we are considering something resembling a base-5 expansion we get

$$0 = 5 + 4 * 5 + 4 * 5^2 + \dots$$

But, as in base-10 addition when we reach 10, we must remember to carry into the next slot giving

$$0 = 0 + 5 * 5 + 4 * 5^2 + \dots$$

and repeating this *ad infinitum* leaves us with some arbitrarily big power of 5, which seems to make no sense whatsoever in the way we are used to think about the size of numbers — *unless we say that a number is smaller the more it's divisible by p, or in our case*

5. So we have ended up with something arbitrarily small, that is, 0 which was our goal. Very good! Technically speaking, we have introduced a new absolute value function to replace the standard one in order to make this series converge.

With this train of thought we can see that 24 and 79 are both quite big since neither is divisible by 5. On the other hand, we can consider the difference

$$55 = 79 - 24 = (4 + 3 * 5^2) - (4 + 4 * 5^2) = (5 - 4) * 5 + 2 * 5^2 = 1 * 5 + 2 * 5^2,$$

which seems to be a bit smaller since its divisible by 5 exactly once.

Now, to get a similar representation for the rest of the integers all we need to do is multiply[1] positive integers with this -1. Let's do $-1 * 24$. This looks a bit messy:

$$\begin{array}{rl}
 & 4 + 4 * 5 + 4 * 5^2 + 4 * 5^3 + \dots \\
* & 4 + 4 * 5 \\
\hline
 & (1 + 3 * 5) + (1 + 3 * 5) * 5 + (1 + 3 * 5) * 5^2 + \dots \\
+ & \qquad\qquad (1 + 3 * 5) * 5 + (1 + 3 * 5) * 5^2 + \dots \\
\hline
 & 1 + 4 * 5 + 4 * 5^2 + 4 * 5^3 + \dots \\
+ & \qquad 1 * 5 + 4 * 5^2 + 4 * 5^3 + \dots \\
\hline
 & 1 + 0 * 5 + (4 + 5) * 5^2 + \dots \\
\sim & 1 + 0 + 4 * 5^2 + (4 + 5) * 5^3 + \dots
\end{array}$$

Again, continuing this infinitely gives $-24 = 1+4*5^2+4*5^3+\dots$. Not something we would want to repeat too often. Luckily, one can derive a nice formula for taking negatives. For a p-adic integer[2] we have

$$-(a_0 + a_1 p + a_2 p^2 + \dots) = (p - a_0) + (p - 1 - a_1)p + (p - 1 - a_2)p^2 + \dots$$

if $a_0 \neq 0$. If it is, then we just start from the first nonzero digit and work in a similar way. For example, in the case of $p = 5$ and the numbers 79 and 55 we have

$$\begin{aligned}
-79 = -(4 + 3 * 5^2) &= (5 - 4) + (5 - 1) * 5 + (5 - 1 - 3) * 5^2 + (5 - 1) * 5^3 + \dots \\
&= 1 + 4 * 5 + 1 * 5^2 + 4 * 5^3 + \dots
\end{aligned}$$

$$\begin{aligned}
-55 = -(5 + 2 * 5^2) &= (5 - 1) * 5 + (5 - 1 - 2) * 5^2 + (5 - 1) * 5^4 + \dots \\
&= 4 * 5 + 2 * 5^2 + 4 * 5^3 + \dots .
\end{aligned}$$

[1] Don't even try to think about this rigorously at this point!

[2] Definition soon to follow! And you can generalise this easily for p-adic numbers.

Division can be performed as well, but it will be a bit trickier and *much* messier.[1] We also need to allow negative powers of p in the expansion for this to make any sense. Anyway, let us make all this a bit more formal.

2 p-adic Integers

Fix a prime p.[2] Let us call a power series in p of the form $\sum_{i=0}^{\infty} a_i p^i$, where $0 \leq a_i \leq p-1 \; \forall i$, a p-adic integer. Denote the set of such numbers by $\mathbb{Z}_p$. With this notation, and by the work we did above, we can see $24, 79, -1, -55 \in \mathbb{Z}_p$, however $\frac{1}{5} \notin \mathbb{Z}_p$, for example.

We also wish to make some sense of the statement that the size of a number is measured by its divisibility by p. That is, we wish to define the p-adic absolute value. For this, we will need one additional concept.

Definition 1. *The p-adic valuation on $\mathbb{Z}$ is the function*

$$v_p : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{R}$$

defined as follows: for each integer $n \in \mathbb{Z}, n \neq 0$, let $v_p(n)$ be the unique positive integer satisfying

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

We extend v_p to $\mathbb{Q}$ as follows: if $x = a/b \in \mathbb{Q}^\times$, then

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

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

Note that v_p satisfies the following properties

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

(ii) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$,

for all $x, y \in \mathbb{Q}$. These are quite easy to prove!

[1] If you are interested have a look at this wonderful article on p-adic arithmetic by Koç `http://islab.oregonstate.edu/papers/r09padic.pdf`, or Koblitz for something more similar to what was done here.

[2] Yes, it will be explained soon why we need a prime!

Definition 2. *For any $x \in \mathbb{Q}$ we define the p-adic absolute value of x by*

$$|x|_p = p^{-v_p(x)}.$$

Also set $|0|_p = 0$.

Before moving on, you may notice even from the definition that there is certain discreteness about this absolute value. Indeed, it will make our p-adic numbers have totally disconnected Hausdorff topology.

This absolute value naturally extends to p-adic integers, and for any $x \in \mathbb{Z}_p, x = a_0 + a_1 p + a_2 p^2 + \ldots$ we can show that $|x|_p = p^{-i}$ if $a_j = 0$ for $j < i$.

For example $|24|_5 = |4 + 4 * 5|_5 = 1$. We can also see this by just noting that 5 doesn't divide 24. Another example: $|410|_5 = \left|2 * 5 + 1 * 5^2 + 3 * 5^3\right|_5 = \frac{1}{5}$. This time it is probably quicker to factorise: $|410|_5 = |82 * 5|_5 = \frac{1}{5}$. Notice that for any p-adic integer x we have $|x|_p \leq 1$. In particular $|x|_p = 1$ iff $a_0 \neq 0$.

The aspect which distinguishes p-adic absolute value from the usual one is the following property (which is easy to derive from the properties of the valuation, try it!)

$$|x + y| \leq \max\{|x|, |y|\} \ \forall x, y \in \mathbb{Z}_p.$$

Such absolute values are called *non-archimedean*. It is clear that this is a stronger version of the usual Triangle Inequality, and we will see it gives some interesting properties to the p-adic numbers. The terminology arises from the fact that natural numbers satisfy the Archimedean Property ($\mathbb{N}$ is unbounded above) in $\mathbb{R}$, whereas with respect to the p-adic absolute value we already saw that $|x|_p \leq 1, \forall x \in \mathbb{N}$.

Sometimes we denote our usual archimedean absolute value by $|\cdot|_\infty$, and think of this as corresponding to the p-adic absolute value with the "infinite prime". With this notation we have the following funny fact (again *not* hard to prove!) for any $x \in \mathbb{Q}^\times$

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

3 p-adic Numbers

So far we have only discussed expansions starting with a non-negative power of p. We clearly run into problems even within $\mathbb{Q}$, as with the aforementioned $1/5$ ($|1/5|_5 = 5^{-(0-1)} = 5$ so this is larger than anything in $\mathbb{Z}_p$!). Remember the analogue, however, to Laurent series where it is possible to have negative exponents in the expansion. Similarly, let us allow negative powers of p to get numbers of the form

$$a_{-n_0}p^{-n_0} + \ldots + \sum_{i=0}^{\infty} a_i p^i,$$

where $0 \leq a_i \leq p-1 \; \forall i, n_0 \in \mathbb{N}$. We call these p-adic numbers (finally!) and denote the set of all such numbers by $\mathbb{Q}_p$. It turns out this set is actually a field, and that the p-adic absolute value extends nicely to $\mathbb{Q}_p$. Now, remember we restricted our p to the set of primes, if instead we had chosen a composite number, say, 10 we would end up having zero divisors, which is not nice (in fact we would have zero divisors in $\mathbb{Z}_p$ so we wouldn't even be able to construct the field of fractions in the first place)! [1] The representation of each p-adic number is also unique, which is not true in $\mathbb{R}$ (consider e.g. $0.9999\ldots = 1$).

4 Completing $\mathbb{Q}$

This way of presenting the p-adic numbers might[2] seem a little hand-wavy and far-fetched, although it serves as an understandable and illustrative introduction. There is a very natural reason for the p-adic numbers to arise, though, and this is through completions of $\mathbb{Q}$.

We know that $\mathbb{Q}$ is not complete in the usual sense (with respect to the classical absolute value), for example we can find a Cauchy sequence of rationals converging to $\sqrt{2}$. Thus we form a completion of $\mathbb{Q}$ to get $\mathbb{R}$. This process is somewhat lengthy, though not too difficult, and it works the same way for all metric spaces.

With our p-adic absolute value we can naturally define the p-adic metric as $d_p(x,y) = |x-y|_p$ for all $x, y \in \mathbb{Q}_p$. After you have verified that this actually is a metric, it can be shown that instead of the Triangle Inequality (as for the absolute values) this metric satisfies a stronger property (which is equivalent to the underlying absolute value being

[1] See for example `http://en.wikipedia.org/wiki/P-adic_number#Introduction`

[2] Might?

non-archimedean):

$$d_p(x,y) \leq \max\left\{d_p(x,z), d_p(z,y)\right\},\ \forall x,y,z \in \mathbb{Q}_p.$$

Such metrics (with the obvious generalisation) are called *ultrametrics*. Thus we can say that $\mathbb{Q}_p$ is an ultrametric space. A simple derivation shows the following:

$$x,y \in \mathbb{Q}_p, |x|_p \neq |y|_p \implies |x+y|_p = \max\left\{|x|_p, |y|_p\right\}.$$

This allows us to prove that, for instance, all triangles are isosceles or that all points inside a ball (as defined usually for metric spaces) are at its center. In particular no balls can intersect unless one is contained in the other. Bizarre!

It is possible to show that $\mathbb{Q}$ is not complete with respect to any of the p-adic absolute values either. So it makes sense to consider the completion of $\mathbb{Q}$ with $|\cdot|_p$. It conveniently turns out to yield our $\mathbb{Q}_p$![1]

It is natural to ask whether there is anything else, any other possible completion of $\mathbb{Q}$, that we might have missed. Well, discarding the trivial absolute value (as we conveniently have and will do for the rest of the talk), the answer turns out to be a resounding *no*! The following theorem — due to a Ukrainian mathematician **Alexander Ostrowski (1893-1986)** who was a student of Felix Klein and Kurt Hensel — illustrates why.

Theorem 3. *Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime $p \leq \infty$.*

Notice that we are including the archimedean absolute value with $p = \infty$. Two absolute values are said to be equivalent if they define the same topology on the underlying field. This can be shown to be equivalent to the following (easier) criterion:

> Two absolute values $|\cdot|, \|\cdot\|$ on a field $\Bbbk$ are said to be equivalent if there exists $\alpha \in \mathbb{R}$ such that $\forall x \in \Bbbk\ |x| = \|x\|^\alpha$.

Another question you might be tempted to ask is whether some of these $\mathbb{Q}_p$'s are "the same" (isomorphic). Again, the answer is *no*! A final fundamental property (or a lack of

[1] In particular if you complete $\mathbb{Z}$ with $|\cdot|_p$ you get $\mathbb{Z}_p$

one) of $\mathbb{R}$ is that it's not algebraically closed (e.g. $x^2 - 1 = 0$), instead we have to form the algebraic closure of $\mathbb{R}$ which we denote by $\mathbb{C}$. It turns out that it is enough just to adjoin i to the reals to get this closure, that is $\mathbb{R}(i) = \mathbb{C}$. In particular this is the only proper field extension of $\mathbb{R}$. In the case of p-adic numbers, however, things are not as nice. It is true that none of the $\mathbb{Q}_p$'s are algebraically closed. Moreover, there are infinitely many non-isomorphic field extensions of $\mathbb{Q}_p$ and in particular $[\overline{\mathbb{Q}}_p : \mathbb{Q}_p] = \infty$, where $\overline{\mathbb{Q}}_p$ is the algebraic closure of $\mathbb{Q}_p$.

Now, after adjoining i to $\mathbb{R}$ everything is nice and fine and $\mathbb{C}$ is complete. But $\overline{\mathbb{Q}}_p$ is *not* complete! So we have to repeat the whole process of completing a field again. Having done this we are finally finished and end up with something that is both algebraically closed and complete. We denote this field by $\mathbb{C}_p$, and it is possible to show that it is isomorphic to $\mathbb{C}$. The existence of such an isomorphism relies on the Axiom of Choice, however, and no concrete isomorphism can be constructed. For the rest of the talk we shall descend back to $\mathbb{Q}_p$, as everything we are going to deal with works just fine in there as well.

5 Analysis in $\mathbb{Q}_p$

Recall the definition of a Cauchy sequence in $\mathbb{R}$ (or the general one for metric spaces), in particular that it's not enough that consequent terms get closer to each other, but each term after a given one must get close to it. In some sense this is not too nice property since something which might seem like a Cauchy sequence to us turns out not to be one. Take for example $x_n = \sum_{i=1}^{n} \frac{1}{i}$. The difference of consecutive terms is $\frac{1}{n+1}$ which clearly converges but the actual sequence still fails to converge (as we well know!). In ultrametric spaces (or more generally, with respect to a non-archimedean absolute value), and in particular in $\mathbb{Q}_p$, this turns out to be enough for a sequence to converge. More formally:

Lemma 4. *A sequence $\{x_n\}_{n=0}^{\infty} \subset \mathbb{Q}_p$ is Cauchy if and only if*

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

This makes checking for convergence of a sequence rather nice. Here are a few examples

Example 1. (i) $a_n = n$. Then

$$\begin{aligned}\lim_{n\to\infty}|n+1-n|_p &= \lim_{n\to\infty}|1|_p \\ &= 1.\end{aligned}$$

So the sequence doesn't converge, as we might expect.

(ii) $a_n = \frac{1}{n}$. Then

$$\begin{aligned}\lim_{n\to\infty}\left|\frac{1}{n+1}-\frac{1}{n}\right|_p &= \lim_{n\to\infty}\left|\frac{-1}{n(n+1)}\right|_p \\ &= \lim_{n\to\infty}\frac{|-1|_p}{\left|n(n+1)\right|_p} \\ &= \lim_{n\to\infty} p^{v_p(n(n+1))} \\ &\geq p^0 \neq 0.\end{aligned}$$

So maybe slightly more unexpectedly this sequence diverges.

(iii) $a_n = p^n$. Then

$$\begin{aligned}\lim_{n\to\infty}\left|p^{n+1}-p^n\right|_p &= \lim_{n\to\infty}\left|p^n(p-1)\right|_p \\ &= \left|p-1\right|_p \lim_{n\to\infty}\left|p^n\right|_p \\ &= 0.\end{aligned}$$

We can find a similar striking result for series in $\mathbb{Q}_p$, as well. Something that you perhaps wished was true in $\mathbb{R}$ when you first studied real analysis. As stated before $\sum_{n=1}^{\infty}\frac{1}{n}$ fails to converge in $\mathbb{R}$ even though $\lim_{n\to\infty}\frac{1}{n} = 0$. In $\mathbb{Q}_p$ this criterion is enough:

Theorem 5. *A series* $\sum_{n=0}^{\infty} a_n$ *with* $a_n \in \mathbb{Q}_p$ *converges if and only if*

$$\lim_{n\to\infty} a_n = 0.$$

So investigating general series amounts to investigating sequences (and not just sequences of partial sums). To make it a bit more interesting we can introduce power series (as in real analysis) $\sum_{n=0}^{\infty} a_n X^n$. Most results from real analysis still hold true in $\mathbb{Q}_p$, for example the ratio test.

Example 2. (i) $\sum p^n X^n$. Then

$$\lim_{n\to\infty}\left|\frac{p^{n+1}}{p^n}\right|_p = \lim_{n\to\infty}|p|_p$$
$$= \frac{1}{p}.$$

So the series converges for $x \in \mathbb{Q}_p$ if $|x|_p < p$. Notice that if $|x|_p = p$, e.g. $x = p^{-1}$ then the series diverges (why?).

(ii) $\sum n!X^n$. We need the following estimation: $|n!|_p > p^{\frac{-n}{p-1}}$. Then the series converges if and only if $|n!x^n|_p \longrightarrow 0$. We can rewrite this as $|(n!)^{1/n}x|_p^n \longrightarrow 0$, but we know that for $y \in \mathbb{R}_+, y^n \xrightarrow{n\to\infty} 0 \iff y < 1$. Hence we need $\left|(n!)^{1/n}x\right|_p < 1$, or $|x|_p < |n!|_p^{-1/n} < \left(p^{\frac{n}{p-1}}\right)^{1/n} = p^{\frac{1}{p-1}}$. Show that the series diverges if $|x|_p = p^{\frac{1}{p-1}}$ so that we need the strict inequality.

To prove the identity for $|n!|_p$ one first shows that $v_p(n!) = \frac{n-s_p(n)}{p-1}$, where $s_p(a_0 + a_1p + \ldots + a_kp^k) = a_0 + \ldots + a_k$. And the rest is easy.

It is natural to ask what about differentation in $\mathbb{Q}_p$. Unfortunately it is nowhere near as useful or natural as with $\mathbb{R}$. It is perfectly possible to develop a theory for $\mathbb{Q}_p$, but you will get some very discouraging results. For example, a very important result early on in differentiation on $\mathbb{R}$ is the Mean Value Theorem. In $\mathbb{Q}_p$ it is difficult to state something resembling the classical theorem in the first place, and even then it turns out to be false mainly because there is no concept of ordering in $\mathbb{Q}_p$. Therefore we can construct some pretty nasty functions which are differentiable with zero derivative everywhere (in $\mathbb{Z}_p$) but still fail to be constant (called *pseudo-constant functions*). Or to construct two functions which have the same derivative everywhere but do not differ by a constant. We better leave this area alone for now...

Example 3. $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ defined by $f(a_0 + a_1p + a_2p^2 + a_3p^3 + \ldots) = a_0 + a_1p^2 + a_2p^4 + a_3p^6 + \ldots$ is pseudo-constant. Here's the proof:

The function is clearly not constant. So we need to show that the derivative is 0 everywhere. Let $x, y \in \mathbb{Z}_p, x \neq y$ with $x = a_ip^i, y = b_ip^i$ (this is shorthand notation using Einstein's summation convention). Then for some $k \in \mathbb{Z}$ we have $|x - y|_p = p^{-k}$ so $x \equiv y \pmod{p^k}$. So $a_i = b_i$ for $i \leq k - 1$.Thus

$$|f(x) - f(y)|_p = |(a_k - b_k)p^{2k} + \ldots|_p = p^{-2k}.$$

Hence,

$$\left|\frac{f(x)-f(y)}{x-y}\right|_p = \frac{p^{-2k}}{p^{-k}} = p^{-k}.$$

Now as $x \to y$ then clearly $k \to \infty$. □

Finally, integration works much better than differentiation in $\mathbb{Q}_p$ but it is trickier[1] to get to as with the classical case so we won't spend any time with it here.

6 Applications

You might be eager to know already are there any actual benefits of considering these p-adic numbers. Well, in general there are quite a few applications of p-adic analysis and theory already, even though the area is quite recent (it only started to flourish in the end of the 20^{th} century). A natural application is clearly in number theory, of which we shall give one example. Other early applications included for example Quantum Physics. Nowadays we can even find some applications in economics or in the study of dynamical systems, to name a few.

One early idea with p-adic numbers was Hasse's *Local-Global Principle*. It basically says that it would be nice that if an equation has a solution in all $\mathbb{Q}_p$'s and $\mathbb{R}$ then it has an integral solution[2]. Unfortunately, this principle doesn't hold in general (and thus is only a principle and not a theorem!), however, we can usually gain some insight by studying equations in all these fields. Sometimes it does even work, and here's an example. This is a special case of a theorem by Hasse and Minkowski:

Theorem 6. *Let $f(X,Y) \in \mathbb{Q}[X,Y]$ be a quadratic form. Then the equation $f(X,Y) = 0$ has non-trivial solutions in $\mathbb{Q}$ if and only if it has non-trivial solutions in $\mathbb{Q}_p$ for all $p \leq \infty$.*

This theorem naturally generalises for n variables, and through this you can derive some rules for the coefficients of the variables so that the equation becomes soluble in $\mathbb{Q}$ (at least for small n!).

[1] You need something called p-adic distributions and p-adic measures. For a treatment on the subject see Koblitz.

[2] Study of integral solutions of polynomial equations is known as Diophantine Analysis.

7 Some Algebra

As you might have already noticed, $p\mathbb{Z}_p$ is a maximal principal ideal of $\mathbb{Z}_p$. Moreover, it is unique so that $\mathbb{Z}_p$ is a *local ring*. You may also have noticed that $\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p : |x|_p \leq 1\right\}$ and $p\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p : |x|_p < 1\right\}$.

$\mathbb{Q}_p$ also has a quick algebraic construction, which is trickier than the analytic one, but helps us understand the origins of the power series representation of p-adic numbers. We now give an overview of this construction, which requires the knowledge of a concept of projective limits[1].

Lemma 7. *Let $\{G_n\}$ be a sequence of multiplicative groups, and $\{h_n\}$ a sequence of surjective homomorphisms $h_n : G_n \longrightarrow G_{n-1}$. Let G be the set of sequences of the form $(x_1, x_2, \ldots)$ with $x_i \in G_i$ where $h_{n+1}(x_{n+1}) = x_n$. Define multiplication on these sequences in the obvious way. Then under this operation G is a group and is called the projective limit of the G_i's.*

Theorem 8. *Let $G_n = {}^{\mathbb{Z}}/_{p^n\mathbb{Z}}$ with the natural homomorphisms $h_n : {}^{\mathbb{Z}}/_{p^n\mathbb{Z}} \longrightarrow {}^{\mathbb{Z}}/_{p^{n-1}\mathbb{Z}}$. Then the projective limit of the G_n's is $\mathbb{Z}_p$.*

It takes some work to show that the two constructions are equivalent. Here's a little something which might make it clearer why we get $\mathbb{Z}_p$:

Theorem 9. *For any $n \geq 1$ the sequence*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\phi_n} \mathbb{Z}_p \longrightarrow {}^{\mathbb{Z}}/_{p^n\mathbb{Z}} \longrightarrow 0$$

is exact, where $\phi_n(x) = p^n x$. In particular ${}^{\mathbb{Z}_p}/_{p^n\mathbb{Z}_p} \cong {}^{\mathbb{Z}}/_{p^n\mathbb{Z}}$.

Moreover, we can show that for any $x \in \mathbb{Z}_p$ we can find a unique Cauchy sequence $\{\alpha_n\} \subset \mathbb{Z}$ such that $0 \leq \alpha_n \leq p^n - 1$ and $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$ (also we have $x \equiv \alpha_n \pmod{p^n}$). Such a sequence is called coherent. You should be able to see now how the homomorphisms work to give us the terms of the series expansion of $x \in \mathbb{Z}_p$ as we associate ${}^{\mathbb{Z}_p}/_{p^n\mathbb{Z}_p}$ with ${}^{\mathbb{Z}}/_{p^n\mathbb{Z}}$ in the projective limit. In a way the homomorphisms project the x to all these alphas and as we approach infinity we get closer and closer to our x, hence the term projective limit (or maybe we could say inverse projective limit...). For example for 79 in $\mathbb{Q}_5$ we have the following sequence $(4, 4, 79, 79, 79, \ldots)$.

So we have our $\mathbb{Z}_p$ which is an integral domain, so we can construct its field of fractions. It can be shown that this field is isomorphic to $\mathbb{Q}_p$.

[1] Also known as *inverse limit* but projective limit is more descriptive here.

8 Conclusion

This more or less wraps us the introductory talk leaving only one thing to be said. This is that we have really only scratched the surface. It is possible to develop most of the theory you have seen in real analysis or for metric spaces for this particular case of ultrametric spaces. We have also largely ignored most of the number theoretic aspect of p-adic numbers, and some famous theorems such as *Hensel's Lemma*. Moreover, as this area is comparatively recent all the development is still highly ongoing. In addition to elementary calculus, advances are made in the areas of p-adic Functional Analysis, p-adic Lie Groups, Algebraic Number Theory, or p-adic Probability Theory, and so on. Based on this talk I hope you can imagine how interesting results these areas will yield. Finally, a list of recommended reading is attached for the interested ones.

- Gouvêa, F. Q., *p-adic Numbers: An Introduction*, 2003, Springer.
  A fine introductory book, which got me started on p-adic numbers. Accessible to all undergraduates!
- Koblitz, N., *p-adic Numbers, p-adic Analysis, and Zeta-functions*, 1984, Springer.
  One of the classical books of this subject. This one should work fine after reading Gouvêa as it extends a bit further into analysis and number theory, introducing for example integration in $\mathbb{C}_p$.
- Mahler, K., *p-adic numbers and their functions*, 1981, Cambridge.
  This is slightly different kind of book and maybe a tad harder. There are some good examples of differentiation on $\mathbb{Q}_p$ (for example a more general version of our pseudo-constant function here!) and it is shown that you can get some good results in there albeit the obstructions.