A Brief Note on p-adic Analysis, p-Adic Topology and Ostrowski's Theorem

Edward Chernysh*

September 1, 2017

Abstract

We study the p-adic norm for primes p and construct the field of p-adic numbers $\mathbb{Q}_p$. It will be shown that $\mathbb{Q}_p$ may be regarded as an extension to $\mathbb{R}$, in the sense that it is complete. We define the p-adic integers $\mathbb{Z}_p$ and study their fundamental topological properties. We prove moreover that any non-trivial norm on $\mathbb{Q}$ not equivalent to the absolute value is necessarily equivalent to a p-adic norm.[1]Moreover, we shall show that this choice of p-adic norm is unique.

1 Introduction

The p-adic numbers were first introduced and studied by Kurt Hensel in 1879; these numbers serve as an alternative extension to $\mathbb{Q}$, typically different from $\mathbb{R}$ or $\mathbb{C}$. Given a prime number p we may define a metric on $\mathbb{Q}$ different from the standard euclidean norm $|\cdot|$ induced by the absolute value function. We first recall the following definition from topology

Definition 1. *An ultra-metric space is a non-empty set X with a function $d : X \times X \to [0, \infty)$ that satisfies each of the following:*

1. *$d(x, y) = 0$ if and only if $x = y$.*
2. *$d(x, y) = d(y, x)$ for all $x, y \in X$.*

*The author gratefully acknowledges the contributions of Charles Boulanger, Dana Berman and Felix Roussy. It is their patience, support and attention to detail which made this paper possible.

[1]This is *Ostrowski's* theorem.

3. $d(x,y) \leq \max\{d(x,z), d(z,y)\}$ *for all* $x, y, z \in X$.

The inequality in (3) is sometimes called the *strong triangle inequality* and has some interesting consequences. It is clear that (3) implies the usual triangle inequality $d(x,y) \leq d(x,z) + d(z,y)$ and therefore any ultrametric space is a metric space.

Definition 2. *A metric space* (X,d) *is called complete if every Cauchy sequence is convergent in* X*. That is, if every Cauchy sequence has a limit in* X*.*

A norm on a field $\mathbb{F}$ is a mapping $|\cdot| : \mathbb{F} \to [0,\infty)$ such that

1. $|x| = 0$ if and only if $x = 0$.
2. $|x+y| \leq |x| + |y|$ for all $x, y \in \mathbb{F}$.
3. $|xy| = |x|\,|y|$ for all $x, y \in \mathbb{F}$.

Clearly, a norm $|\cdot|$ induces a metric on $\mathbb{F}$ defined by $d(x,y) := |x-y|$ and hence turns $\mathbb{F}$ into a metric space. If a norm $|\cdot|$ on a field $\mathbb{F}$ satisfies the stronger condition

$$|x-y| \leq \max\{|x-z|\,, |z-y|\}$$

for all $x, y, z \in \mathbb{F}$ we shall call it an ultra-norm.

Consider the field of rational numbers $\mathbb{Q}$ together with the usual notion of distance: the absolute value function $|\cdot|$. In the hopes of solving equations such as $x^2 - 2 = 0$ we *completed*[2] the rationals to get a new, larger field $\mathbb{R}$. It is a basic fact from real analysis that $\mathbb{R}$ is a complete metric space when endowed with this absolute value function. The idea with p-adic numbers is reminiscent of the "classical" real numbers, but instead we complete the rationals with respect to a different norm. By this, we simply mean that $\mathbb{Q}_p$ is the set of all equivalence classes of Cauchy sequence with respect to the norm $|\cdot|_p$, where we define an equivalence in the typical way.

The new resulting field, which we shall affectionately denote $\mathbb{Q}_p$, will be complete just as $\mathbb{R}$ is, but we now have a different notion of distance. This new idea of "nearness" is precisely what makes p-adic theory of such great importance. Perhaps one of the greatest contributions of p-adic analysis to modern mathematics lies in the crucial role the theory played in the proof of Fermat's Last Theorem[3].

[2]Here we mean completeness in the sense of metric spaces. It is a well known fact that $\mathbb{R}$ is not algebraically closed, and nor will be $\mathbb{Q}_p$. A proof of this fact may be found in [1, THM-12].

[3]This theorem was first conjectured in 1637 by the lawyer Pierre de Fermat but was only proven in 1994 by Andrew Wiles.

Consider now a prime p. Given a non-zero integer x we define $\mathrm{ord}(x;p)$ to be the *maximal* $n \in \mathbb{N}$ so that p^n divides x. If $x = 0$ we shall agree to write $\mathrm{ord}(x,p) = \infty$ by convention. There exists a natural extension of this definition to all of $\mathbb{Q}$. Of course, if $x = a/b$ where $a, b \in \mathbb{Z}$, with $a, b \neq 0$ then it makes sense to define $\mathrm{ord}(x;p) := \mathrm{ord}(a;p) - \mathrm{ord}(b;p)$. It will later be shown that this is well-defined and that

$$|x|_p := \begin{cases} \frac{1}{p^{\mathrm{ord}(x;p)}} & x \neq 0 \\ 0 & x = 0 \end{cases} \tag{1}$$

is a norm on $\mathbb{Q}$. The aforementioned field $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ under the induced metric, and this will be constructed shortly. Accepting that this is a norm (and hence a valid metric) on $\mathbb{Q}$ gives us a completely new notion of size, and nearness. High powers of this prime p are small in norm, i.e. if $p^n \mid x$ for large n, then $|x|_p$ is small. That is, two integers x, y are *close* provided a large power of p divides $x - y$.

This new approach to number theory and analysis gives way to many applications. Originally, this procedure was carried out in the hopes of using the methods of power-series in number theory. Especially, it allows one to apply methods from analysis in number theory in a unique way. It is as well possible to conduct deep analysis on $\mathbb{Q}_p$, for instance one can define calculus over this field and obtain a perfectly consistent theory of differentiation with very surprising results. Namely, one can have a non-constant differentiable function $f : \mathbb{Q}_p \to \mathbb{Q}_p$ with 0 derivative everywhere; a proof of this fact may be found in [5, §-5.1]. The field of p-adic analysis is still young and ever-expanding, one can even find applications of this theory in physics, especially in *p-adic quantum mechanics*.

Perhaps the most surprising and motivating example for p-adic analysis (and of course p-adic numbers) is Ostrowski's theorem, found in [1, THM-1], which states that any non-trivial norm[4]. on $\mathbb{Q}$ is equivalent to a p-adic norm, where we allow the special case $p = \infty$. By this we only mean:

Definition 3. *Let $\mathbb{F}$ be a field and $|\cdot|_1, |\cdot|_2$ be norms on $\mathbb{F}$. We shall call these two norms equivalent (written $|\cdot|_1 \sim |\cdot|_2$) if and only if there exists a positive real number α so that*

$$|x|_1 = |x|_2^{\alpha} \tag{2}$$

for all $x \in \mathbb{F}$.

[4]Non-trivial means that it does not induce the discrete metric

It is clear by definition that this is an equivalence relation on norms, and hence the $\sim$ notation is justified. Speaking loosely, this theorem tells us that studying p-adic fields gives us insight not only on the fields $\mathbb{Q}_p$ but on all completions of the rationals. By convention, we shall write $|\cdot|_\infty$ to denote $|\cdot|$. Certainly, if two norms are equivalent then we find by the definition above that a sequence is Cauchy with respect to one if and only if it is Cauchy in the other.

2 Approach and Techniques

We shall begin with a rigorous construction of the p-adic numbers, describing in detail the metric they induce. As mentioned previously, the p-adic norm is an *ultra-norm*, which will itself yield beautiful topological properties. It is important to study at first sight the properties of this norm, since it is the intrinsic *strong-triangle inequality* that will make this construction simple. Namely, we work to develop an understanding of $|\cdot|_p$.

Subsequently, we shall use these notions to prove that our new set $\mathbb{Q}_p$, when endowed with a natural extension of this norm on $\mathbb{Q}$, satisfies a collection of desired properties; i.e. that $\mathbb{Q}_p$ is both a field and a complete metric space. This is most certainly an important property, for the purpose of our construction is to develop an analogue to the real numbers and should therefore share a similar foundation. Of course, much of the methods used in our construction of $\mathbb{Q}_p$ are similar to those used in the construction of $\mathbb{R}$, but are simplified using the properties intrinsic to the p-adic norm.

Having established the existence and fundamentals regarding the p-adic numbers, we turn to to the integer counterparts of $\mathbb{Q}_p$, the *p-adic integers*. With natural notions of addition and multiplication it will be clear that these form a ring, and of course inherit a topological structure from $\mathbb{Q}_p$. We shall study these integers and, especially, their unique topological properties. Most importantly, we shall prove that the p-adic integers are *uncountable* and topologically compact: which we establish in the form of *sequential compactness*. These properties are of particular interest to us, since this quickly verifies the staggering differences between $\mathbb{Z}$ and these p-adic integers.

Ultimately, $\mathbb{Q}_p$ will be defined as a *space of equivalence* classes of Cauchy sequences, where we say two sequences are related if their difference tends to 0. Addition, multiplication will be defined in a similar manner as $\mathbb{R}$; we will then use the *strong triangle inequality* to extend the p-adic norm to this space of equivalence classes. Having established the field properties, it will become feasible to study a subset of $\mathbb{Q}_p$ which is of particular interest to us: the p-adic integers. These are most certainly of great interest, as they are a generalization of the integers we are familiar with. Now, we are mostly concerned with their

topological distinctions from $\mathbb{Z}$. We shall begin our study of these integers by showing that they have a unique expansion as the sum prime-powers, and once we have established this we will be able to show their compactness and uncountability by elementary methods. Amazingly, this last staggering result is a simple application of *Cantor's Diagonal Argument*.

Perhaps the most astounding result is *Ostrowski's theorem*, which we have stated above. To prove this, we consider separately the cases $\|n\| \leq 1$ and $\|n\| \not\leq 1$ for all $n \in \mathbb{N}$. As we shall see, in the latter case we simply pick a minimal integer ν with $\|\nu\| > 1$, write any integer in base-ν and take limits; establishing that $\|\cdot\|$ is equivalent to the absolute value norm. In the case where $\|n\| \leq 1$ for all n, we choose a minimal $p > 0$ such that $\|p\| < 1$, show that this is a prime and prove that $\|\cdot\| \sim |\cdot|_p$ for this p.

3 The p-adic Numbers $\mathbb{Q}_p$

We devote this section to the construction of the p-adic numbers and their integer counter-parts. As previously mentioned, we shall follow closely the construction of the real numbers from the rationals. We should first verify that the p-adic norm is well defined. We first note that if x, y are integers than $\operatorname{ord}(xy; p) = \operatorname{ord}(x; p) + \operatorname{ord}(y; p)$. Indeed, this is a direct consequence of the definition of $\operatorname{ord}(\cdot, p)$ as the maximal power of p that divides the argument. Now, by uniqueness of prime factorization $\operatorname{ord}(\cdot, p)$ is well defined for $\mathbb{Z}$. To see that this is again the case for non-zero rationals write $x = a/b$ for a, b in reduced terms. If $c \neq 0$ is any other integers then

$$\operatorname{ord}\left(\frac{ac}{bc}; p\right) = \operatorname{ord}(ac; p) - \operatorname{ord}(bc; p) = \operatorname{ord}(a; p) + \operatorname{ord}(c; p) - \operatorname{ord}(b; p) - \operatorname{ord}(c; p)$$

which is precisely the quantity $\operatorname{ord}(a/b; p)$. This implies that our norm $|\cdot|_p$ is well defined for rationals. Now, we make the following claim:

Proposition 3.1. *Fix a prime $p < \infty$. The map $|\cdot|_p$ is an ultra-norm on $\mathbb{Q}$.*

Proof. Property (1) is immediate by the definition of $|\cdot|_p$. The second property is trivial if $x = 0$ or $y = 0$ since then $xy = 0$ implying by property (1) that $|xy| = 0 = |x|\,|y|$ for then one of $|x|$ or $|y|$ are 0. Otherwise, neither $x, y = 0$ and so $xy \neq 0$. This implies that

$$|xy|_p = p^{-\operatorname{ord}(xy;p)} = p^{-\operatorname{ord}(x;p)-\operatorname{ord}(y;p)} = p^{-\operatorname{ord}(x;p)}p^{-\operatorname{ord}(y;p)} = |x|_p\,|y|_p$$

It remains to show the strong triangle inequality. Note that if x or $y = 0$ we have trivially $|x + y|_p \leq \max\{|x|, |y|\}$. Similarly, if $x + y = 0$ then $|x + y|_p =$

$0 \leq \max\{|x|_p, |y|_p\}$. For the general case let $x, y \neq 0$ and $x + y \neq 0$. We may write $x = a/b, y = c/d$ for integers a, b, c, d all non-zero in reduced terms. Then we have

$$\operatorname{ord}(x+y;p) = \operatorname{ord}\left(\frac{ad+bc}{bd};p\right) = \operatorname{ord}(ad+bc;p) - \operatorname{ord}(b;p) - \operatorname{ord}(d;p)$$

where $ad + bc \neq 0$ by assumption that $x + y \neq 0$. In this case, clearly we have $\operatorname{ord}(ad + bd; p) \geq \min\{\operatorname{ord}(ad; p), \operatorname{ord}(bc; p)\}$. This follows from the fact that if $p^k \mid ad, bc$ then $p^k \mid ad + bc$. Now, we get

$$\begin{aligned}
\operatorname{ord}(x+y;p) &\geq \min\{\operatorname{ord}(ad;p), \operatorname{ord}(bc;p)\} - \operatorname{ord}(b;p) - \operatorname{ord}(d;p) \\
&= \min\{\operatorname{ord}(a;p) + \operatorname{ord}(d;p), \operatorname{ord}(b;p) + \operatorname{ord}(c;p)\} - \operatorname{ord}(b;p) - \operatorname{ord}(d;p) \\
&= \min\{\operatorname{ord}(a;p) - \operatorname{ord}(b;p), \operatorname{ord}(c;p) - \operatorname{ord}(d;p)\} \\
&\stackrel{\text{def}}{=} \min\left\{\operatorname{ord}\left(\frac{a}{b};p\right), \operatorname{ord}\left(\frac{c}{d};p\right)\right\}
\end{aligned}$$

which yields $\operatorname{ord}(x + y; p) \geq \min\{\operatorname{ord}(x; p), \operatorname{ord}(y; p)\}$. This therefore implies that

$$|x+y|_p = \frac{1}{p^{\operatorname{ord}(x+y;p)}} \leq \max\left\{\frac{1}{p^{\operatorname{ord}(x;p)}}, \frac{1}{p^{\operatorname{ord}(y;p)}}\right\} = \max\left\{|x|_p, |y|_p\right\}$$

$\bigcirc$

The argument we have used in proving the strong triangle inequality is standard and may be found in [1, PG-2] or [4, PG-4], although ours uses mostly the ideas from [1]. In any case, we observe that it makes sense to speak of p-adic norms (with $p < \infty$) as ultra-norms. Especially, we see immediately

Corollary 3.2. *$|\cdot|_p$ is a norm on $\mathbb{Q}$ and induces an ultra-metric on $\mathbb{Q}$.*

Obviously after the construction of $\mathbb{Q}_p$ we shall wish to extend our p-adic norm to the entirety of $\mathbb{Q}_p$, and not just $\mathbb{Q}$. Considering $|\cdot|_p$ as an ultra-metric will greatly simplify our work in this regard, and it is for this reason that we strengthen our understanding of the strong-triangle inequality in the following lemma:

Lemma 3.3. *Let (X, d) be an ultra-metric space and $\mathbb{F}$ a field with an ultra-norm $|\cdot|$. We have the following:*

1. *Any open ball $B(x, \varepsilon)$ is both open and closed.*
2. *If $y \in B(x, \varepsilon)$ then $B(y, \varepsilon) = B(x, \varepsilon)$.*

3. *If* $B(x,\varepsilon) \cap B(y,\delta) \neq \varnothing$ *then* $B(x,\varepsilon) \subseteq B(y,\delta)$ *or* $B(x,\varepsilon) \supseteq B(y,\delta)$.

4. $|x+y| = \max\{|x|, |y|\}$ *if* $|x| \neq |y|$.

Proof. We begin with (1). In any metric space the open ball $B(x,\varepsilon)$ is open. To see that it is closed, pick any sequence (y_n) living in $B(x,\varepsilon)$ converging to $y \in X$. Then, $d(y_n, x) < \varepsilon$ for all indices n. Now, since $\lim y_n = y$ there is a natural number N so that $d(y_n, y) < \varepsilon$ whenever $n \geq N$. Then, $d(y,x) \leq \max\{d(y,y_N), d(y_N,x)\} < \varepsilon$ implying $y \in B(x,\varepsilon)$.

For (2) suppose that $y \in B(x,\varepsilon)$. Then $d(x,y) < \varepsilon$. If $d(z,y) < \varepsilon$ then one has $d(x,z) \leq \max\{d(x,y), d(z,y)\} < \varepsilon$ and we get $B(y,\varepsilon) \subseteq B(x,\varepsilon)$. For the reverse inequality, if $d(z,x) < \varepsilon$ then $d(z,y) \leq \max\{d(z,x), d(x,y)\} < \varepsilon$ and $B(x,\varepsilon) = B(y,\varepsilon)$.

In (3) we may assume without loss of generality that $\delta \leq \varepsilon$. Take $z \in B(x,\varepsilon) \cap B(y,\delta)$. By part (2) we know $B(x,\varepsilon) = B(z,\varepsilon) \supseteq B(z,\delta) = B(y,\delta)$.

In (4) since $|x| \neq |y|$ we may presume $|x| > |y|$, switching the roles of x, y in the statement otherwise. Then, we have $|x+y| \leq \max\{|x|, |y|\} = |x|$. On the other hand

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

The above must indeed be $|x+y|$ for otherwise we get $|x| \leq |y|$.

◯

We are now ready to define the p-adic numbers $\mathbb{Q}_p$. The construction that follows may be found in [1, §-I.4] and uses some ideas from [4, §-5]. The main idea is to define an equivalence relation on Cauchy sequences of rationals and use these to "fill in the holes". If $(x_n), (y_n)$ are two Cauchy sequences in $(\mathbb{Q}, |\cdot|_p)$ then we shall write $(x_n) \sim (y_n)$ if and only if $|x_n - y_n|_p \to 0$ as $n \to \infty$. This is obviously an equivalence relation by the triangle inequality.

Definition 4. $\mathbb{Q}_p$, *the p-adic numbers, is* $\mathbb{Q}/\!\sim$.

As previously mentioned we wish to extend $|\cdot|_p$ to an equivalence class of $\mathbb{Q}_p$. Let x be an equivalence class in $\mathbb{Q}_p$ and (x_n) any Cauchy sequence "representing" it. We shall define the norm $|x|_p := \lim_{n\to\infty} |x_n|_p$, where $x_n \in \mathbb{Q}$ for all n. This definition makes sense for

1. If x is the equivalence class of the zero-sequence, it represents 0 and $\lim |x_n|_p = 0$.

2. If $x \neq 0$ ($x \not\sim [(0)_n]$) there is some $\varepsilon_0 > 0$ so that for all $N' \in \mathbb{N}$ there is $n \geq N'$ with $|x_n|_p > \varepsilon_0$. Now, since (x_n) is Cauchy in $\mathbb{Q}$, we may select such N so that for all $m, k \geq N$ one has $|x_k - x_m| < \varepsilon_0$.

In case (2) above pick the least such $n \geq N$, we claim that if $m \geq n$ then $|x_m| = |x_n|$. Indeed, if this were not the case then by Lemma (3.3)-(4) one would find $|x_m - x_n|_p = \max\{|x_m|_p, |x_n|_p\} > \varepsilon_0$: a clear absurdity.

Corollary 3.4. *Let $x \in \mathbb{Q}_p$ with $x \neq 0$. There exists a sequence (x_n) representing x and $\eta > 0$ such that $|x_n|_p \geq \eta$ for all n.*

Proof. This is a consequence of (2) above. Indeed, let (x_n) be a Cauchy sequence in $\mathbb{Q}$ representing x. Since $x \neq 0$, there are infinitely many non-zero terms and therefore we may extract a subsequence of non-zero terms (x_{n_k}). This is again a Cauchy sequence (since it is the subsequence of a Cauchy sequence) and of course represents x since $(x_{n_k}) \sim (x_n)$. Now, from (2) it is clear that the sequence consisting of $|x_{n_k}|_p$ is eventually constant, and since all $|x_{n_k}|_p$ are positive we are done.

$\bigcirc$

It remains to show that this notion of norm on an equivalence class is well-defined. If (x'_n) were any other representative of x then we would have[5]

$$\left| |x_n|_p - |x'_n|_p \right| \leq |x_n - x'_n|_p \xrightarrow{n\to\infty} 0$$

It is now time to define the operations that make $\mathbb{Q}_p$ into a field analogous to $\mathbb{R}$. Let $x, y \in \mathbb{Q}_p$ be equivalence classes with representatives $(x_n), (y_n)$. We define operations $+, \cdot$ as follows:

$$x + y := [(x_n + y_n)], \quad x \cdot y := [(x_n y_n)] \tag{3}$$

These definitions make sense, for sums and products of Cauchy sequences are again Cauchy sequences[6]. To see that these are independent of representation, let $(x'_n), (y'_n)$ be other representatives for x, y respectively. Then we have:

$$|x_n + y_n - x'_n - y'_n|_p \leq |x_n - x'_n|_p + |y_n - y'_n|_p \xrightarrow{n\to\infty} 0$$

and

$$|x_n y_n - x'_n y'_n|_p \leq |x_n|_p \, |y_n - y'_n| + |y'_n|_p \, |x_n - x'_n|_p$$

which vanishes in $n \to \infty$, showing that $(x_n y_n) \sim (x'_n y'_n)$ as well as $(x_n + y_n) \sim (x'_n + y'_n)$. From these arguments it becomes clear that it makes sense to define $-x$ for $x \in \mathbb{Q}_p$ by selecting a representative (x_n) and letting $-x := [(-x_n)]$. In this case it is obvious that $x + (-x) = 0$.

[5] By a general inequality on norms.

[6] Any Cauchy sequence is bounded.

Theorem 3.5. *$\mathbb{Q}_p$ is a field.*

Proof. Note that $\mathbb{Q}_p$ inherits associativity and commutativity from $\mathbb{Q}$ given our definitions above. Since it is clear that $1 \neq 0$ we need only define a multiplicative inverse whenever $x \neq 0$. Let $x \in \mathbb{Q}_p$ with $x \neq 0$, by Corollary 3.4 we may select a representative $(x_n) \subseteq \mathbb{Q}$ with $x_n \neq 0$ for all n and $|x_n|_p > \eta > 0$ for all n. We now define

$$x^{-1} := \left(x_n^{-1}\right)_n$$

This new sequence is Cauchy in $\mathbb{Q}$, indeed,

$$\left|\frac{1}{x_n} - \frac{1}{x_m}\right|_p = \left|\frac{x_n - x_m}{x_n x_m}\right|_p \leq M \left|x_n - x_m\right|_p$$

with $M = 1/\eta$, which tends to 0 as n, m become large. Of course, in this case we then get $(x_n \cdot x_n^{-1}) \sim (1)$ proving the theorem.

$\bigcirc$

We remark that in the case $p = \infty$ we have $\mathbb{Q}_p = \mathbb{R}$ which is also a field. This observation reminds us of our goal to construct a field similar to the reals, and so we also want $\mathbb{Q}_p$ to be a complete metric space with respect to the p-adic norm. We almost have this,

Theorem 3.6. *The pair $(\mathbb{Q}_p, |\cdot|_p)$ is a complete metric space.*

Proof. The proof is an illustration of the sketch given in [1, THM-2]. If (x_n) is a sequence in $\mathbb{Q}_p$ that is Cauchy, then for all fixed n: $(x_{n,m})_m$ is a Cauchy sequence in $\mathbb{Q}$. Hence, there is an $N_n \in \mathbb{N}$ such that $|x_{n,j} - x_{n,\ell}|_p < 2^{-n}$ for all $j, \ell \geq N_n$. This gives us a "diagonal" subsequence (x_{n,N_n}) in $\mathbb{Q}$. Clearly, this subsequence is Cauchy in $\mathbb{Q}$ because

$$\begin{aligned} |x_{n,N_n} - x_{m,N_m}|_p &\leq |x_{n,N_n} - x_{n,\ell}|_p + |x_{n,\ell} - x_{m,N_m}|_p \\ &\leq |x_{n,N_n} - x_{n,\ell}|_p + |x_{n,\ell} - x_{m,\ell}|_p + |x_{m,\ell} - x_{m,N_m}|_p \end{aligned}$$

where this middle term may be made arbitrarily small since (x_n) is Cauchy in $\mathbb{Q}_p$: this follows from the definition of the norm on $\mathbb{Q}_p$. Thus it suffices to take ℓ large in the above.

Now, to see that $(x_n) \to x$ in $\mathbb{Q}_p$ we denote by x the equivalence class of this sequence (x_{n,N_n}) and write

$$\begin{aligned} \lim_{n\to\infty} |x_n - x|_p = \lim_{n\to\infty} |[(x_{n,m})_m - [(x_{n,N_n})]|_p &= \lim_{n\to\infty} |[x_{n,m} - x_{n,N_n}]|_p \\ &\leq \lim_{n\to\infty} 2^{-n} \end{aligned}$$

$\bigcirc$

The subtlety lies in our definition of $|\cdot|_p$ for an equivalence class x in $\mathbb{Q}_p$. Had we not had the *strong triangle inequality* we could not have made sense of the definition as the limit of $|x_n|_p$. The subsequent theorem is a beautiful result due to Ostrowski which, when put loosely, states that the only non-trivial norms on $\mathbb{Q}$ are the p-adic norms, where we allow the case $p = \infty$. It is useful now to recall that we denote by $|\cdot|_\infty$ the Euclidean norm as a special case of the p-adic norms.

We shall now motivate the larger study of p-adic numbers, we begin with a lemma describing a special case of Ostrowski's theorem.

Lemma 3.7. *Let $\|\cdot\|$ be a non-trivial norm on $\mathbb{Q}$ such that there exists a positive integer ν satisfying $\|\nu\| > 1$. Then $\|\cdot\| \sim |\cdot|_\infty$.*

Proof. The proof is from [1, THM-1-(i)]. Pick first a minimal ν, we may express a positive integer n is base-ν: $n = \sum_{j=0}^{m} a_j \nu^j$ where $0 \leq a_j < \nu$ and $a_m \neq 0$. Since $\|\nu\| > 1$ we may find some $\alpha > 0$, real, so that $\|\nu\| = \nu^\alpha$. Now, we may estimate the norm of n as follows:

$$\|n\| \leq \sum_{j=0}^{m} \|a_j\| \, \|\nu\|^j = \sum_{j=0}^{m} \|a_j\| \, \nu^{\alpha j} \leq 1 + \nu^\alpha + \cdots + \nu^{\alpha m}$$

where in this last inequality we used the minimality of ν to conclude that $\|a_j\| \leq 1$ since $a_j < \nu$. On the other-hand, we may refine the above to yield for some $C > 0$

$$\|n\| \leq \nu^{\alpha m}(1 + \nu^{-\alpha} + \cdots + \nu^{-\alpha m}) \leq \nu^{\alpha m} \sum_{j=0}^{\infty} \nu^{-\alpha j} = C\nu^{\alpha m} \leq Cn^\alpha$$

since $n \geq \nu^m$ by our expansion. Since n was arbitrary we may let N large and substitute n^N to deduce $\left\|n^N\right\| = \|n\|^N \leq Cn^{\alpha N}$ whence $\|n\| \leq C^{1/N} n^\alpha$ for all N. Letting $N \to \infty$ we recover our first inequality: $\|n\| \leq n^\alpha$ since $C^{1/N} \to 1$ as $N \to \infty$.

For the reverse inequality, we let n be written as above; we yet again have $\nu^s \leq n < \nu^{s+1}$ and thus $\|\nu^{s+1}\| \leq \|n - \nu^{s+1}\| + \|n\|$. All this together with our first inequality above applied to $\|\nu^{s+1} - n\|$ yields

$$\|n\| \geq \left\|\nu^{s+1}\right\| - \left\|\nu^{s+1} - n\right\| \geq \nu^{(s+1)\alpha} - (\nu^{s+1} - n)^\alpha \geq \nu^{(s+1)\alpha} - (\nu^{s+1} - \nu^s)^\alpha$$

since $\nu^s \leq n$. Now, this implies $\|n\| \geq \nu^{(s+1)\alpha}\left(1 - (1 - 1/\nu)^\alpha\right) \geq n^\alpha C'$ for C' independent of n. Since $n \in \mathbb{N}$ is arbitrary we may repeat the argument in the

first inequality to derive $\sqrt[N]{C'}n^{\alpha} \leq \|n\|$, and hence $n^{\alpha} \leq \|n\|$ for all n. That is, $\|n\| = |n|_{\infty}^{\alpha}$ for all $n \in \mathbb{N}$. We now show that this extends to any $x \in \mathbb{Q}$.

This follows from the observation that if $n \in \mathbb{N}$ then $\|n^{-1}\| = \|n\|^{-1}$. Indeed, first we see that $\|1\| = \|1 \cdot 1\| = \|1\|^2$, and since $\|1\| \neq 0$ we have $\|1\| = 1$. Now, for $x \in \mathbb{Q}^*$ we write $1 = \|1\| = \|x \cdot x^{-1}\| = \|x\| \cdot \|x^{-1}\|$. This lemma is now proven.

$\bigcirc$

Now that we have this lemma, we may now prove the more powerful and elegant side of Ostrowski's theorem which states that other than the absolute value, there are no other norms on $\mathbb{Q}$ than the p-adic ones.

Theorem 3.8 (Ostrowski). *Let $\|\cdot\|$ be a non-trivial norm on $\mathbb{Q}$. Then there is a prime p, possibly $p = \infty$, so that $\|\cdot\| \sim |\cdot|_p$.*

Proof. We give a proof that may be found in [1, THM-1-(ii)]. Since we have already established Lemma 3.7 we need only handle the case where $\|n\| \leq 1$ for all $n \in \mathbb{N}$. We claim there is some *minimal* $p \in \mathbb{N}$ so that $\|p\| < 1$. Certainly, if this were not the case then $\|n\| = 1$ for all $n \in \mathbb{N}$, especially if $x = a/b \neq 0$ for integers a, b we obtain $\|x\| = \|a\| \cdot \|b\|^{-1} = 1$ contradicting our assumption that the norm is non-trivial.

Let p be the minimal positive integer with $\|p\| < 1$. p must be prime, for otherwise $p = ab$ with $1 < a, b < p$ whence $\|p\| = \|a\| \|b\| = 1 \cdot 1 = 1$ by minimality of p.

We claim if q is a prime distinct from p then $\|q\| = 1$. Otherwise, $\|q\| < 1$. Using that $\|p\|^N, \|q\|^N \to 0$ as $N \to \infty$ we may find N large enough so that $\|p\|^N < 1/2$ and $\|q\|^N < 1/2$. Now, since $\gcd(p^N, q^N) = 1$ an application of Bézout's lemma ensures the existence of integers u, v such that $1 = up^N + vq^N$. However,

$$\|1\| = 1 = \left\|up^N + vq^N\right\| \leq \|u\| \|p\|^N + \|v\| \|q\|^N \leq \|p\|^N + \|q\|^N < \frac{1}{2} + \frac{1}{2} = 1$$

which is absurd. By the end of the proof for Lemma 3.7 we remark that it suffices to show that $\|n\| = |n|_p^{\alpha}$ for integers n. For any integer $n \neq 0$, we may write $n = \prod_{j=1}^{k} p_j^{e_j}$ for primes p_j, distinct. If $p \nmid n$ then $\|n\| = 1$ by this remark and so $\|n\| = |n|_p^{\alpha}$ for all $\alpha > 0$. If $p \mid n$ then p is some p_j, say, p_k. Now, passing to the norm all $p_j \neq p_k$ reduce to 1 and we are left with $\|n\| = \|p\|^{e_j} = \varrho^{e_j}$ with $0 < \varrho < 1$. However, $e_j = \mathrm{ord}(n; p)$ and so if we take $\alpha > 0$ so that $p^{-\alpha} = \varrho$ we obtain $\|n\| = p^{-\alpha \cdot \mathrm{ord}(n;p)} = |n|_p^{\alpha}$.

The proof is complete.

$\bigcirc$

This hugely motivates the study of the p-adic norms and $\mathbb{Q}_p$, since it allows us to characterize all norms on $\mathbb{Q}$ and hence the completions of $\mathbb{Q}$. Having established the result in Ostrowski's theorem, it is natural to seek the uniqueness counterpart:

Proposition 3.9. *Let $p, q < \infty$ be primes. Then, $|\cdot|_p \sim |\cdot|_q$ if and only if $p = q$.*

Proof. Suppose by way of contradiction that $|\cdot|_p \sim |\cdot|_q$ but that $p \neq q$. There must exist $\alpha \in \mathbb{R}$ positive ($\alpha > 0$) such that $|x|_p = |x|_q^\alpha$ for all $x \in \mathbb{Q}$. Now consider $x = p$, which is co-prime to q. By definition we have $|p|_p = p^{-1}$, however we have $|p|_q = 1$. Now, this implies

$$\frac{1}{p} = 1^\alpha$$

which is absurd.

○

This complements Ostrowki's theorem in the following way:

Corollary 3.10. *If $\|\cdot\|$ is a non-trivial norm on $\mathbb{Q}$ it is either equivalent to the absolute value or to a p-adic norm for a unique prime p.*

4 The p-adic Integers and Their Topology

We shall devote this section to the p-adic integers, which we denote by $\mathbb{Z}_p$. These are of particular interest to us, especially as they lie in sharp contrast with the ring of integers $\mathbb{Z}$. Loosely speaking, the p-adic integers consist of all expansions of the form $\sum_{n\in\mathbb{N}_0} a_n p^n$ for a prime p and $a_n \in \{0, \ldots, p-1\}$. What is most striking is how different these integers behave. Clearly, as a subset of $\mathbb{Q}_p$ the p-adic integers inherit a metric space topology and in-like for $\mathbb{Z} \subset \mathbb{R}$.

It may be shown directly that $\mathbb{Z}$ is not compact with respect to the usual topology. Certainly, the collection $\left\{\left(x - \frac{1}{2}, x + \frac{1}{2}\right)\right\}_{x\in\mathbb{Z}}$ forms and open-covering of $\mathbb{Z}$ for which there is no finite sub-covering. We shall see that in many situations $\mathbb{Z}_p$ behaves in a completely different manner: unlike $\mathbb{Z}$ the ring $\mathbb{Z}_p$ is compact, and unlike $\mathbb{Z}$ the integers $\mathbb{Z}_p$ are uncountable.

Definition 5 (p-adic Integers). *Let $p < \infty$ be a prime. We define the **p-adic** integers, denoted $\mathbb{Z}_p$, to be the collection of all sums: $\sum_{n=0}^{\infty} a_n p^n$, with $a_n \in \{0, \ldots, p-1\}$. Namely, $\mathbb{Z}_p$ consists of all numbers with no negative powers of p in its expansion.*

Of course, the pair $(\mathbb{Z}_p, |\cdot|_p)$ itself is again a metric space with the same metric as $\mathbb{Q}_p$. We would like to make observation that all p-adic integers are "convergent", and consequently bounded. Certainly, consider some p-adic integer $x = \sum_{n=0}^{\infty} a_n p^n$ and let $x_N := \sum_{n=0}^{N} a_n p^n$. By completeness, it is sufficient to show that (x_N) is Cauchy in $\mathbb{Q}_p$. To see this, let $\varepsilon > 0$ and let $K > 0$ be such that $p^{-K} \leq \varepsilon$. Assume now that $N, M \geq K$ but that $N > M$. Then,

$$\left| \sum_{n=0}^{N} a_n p^n - \sum_{n=0}^{M} a_n p^n \right|_p = \left| \sum_{n=M+1}^{N} a_n p^n \right|_p \leq p^{-M+1} \leq p^{-K} \leq \varepsilon$$

In particular, every p-adic integer has finite norm.

One can define an operation "$+$" corresponding to addition on $\mathbb{Z}_p$. Take now two p-adic integers $x = \sum_{n=0}^{\infty} a_n p^n, y = \sum_{n=0}^{\infty} b_n p^n$. The idea is to "carry-over" onto subsequent indices if $a_k + b_k \geq p$ for some index k. For instance, at the first index k where $a_k + b_k \geq p$ we set $c_k = a_k + b_k - p$ and carry one over to c_{k+1} in the expression $x+y = \sum_{n=0}^{\infty} c_n p^n$ and so forth. This is merely a heuristic explanation, and we shall not explore this further. The reader may refer to [3, §-2] for a rigorous explanation of both addition and multiplication of p-adic integers. It is also shown in [3, PROP-2.3.1] that $\mathbb{Z}_p$ is both a commutative ring and integral domain. Here we are much more interested in the analytic and topological properties of $\mathbb{Z}_p$.

Lemma 4.1. *If $p < \infty$ is a prime and $x = \sum_{n=0}^{\infty} a_n p^n \in \mathbb{Z}$, then $x = 0$ if and only if $a_n = 0$ for all $n \in \mathbb{N}$.*

Proof. One direction is trivial. For the converse, observe that we must then have $|x|_p = 0$. Suppose that not all a_n are 0. Then there is some least $m \geq 0$ such that $a_m \neq 0$. By definition of the norm for an element of $\mathbb{Q}_p$, we note that

$$|x|_p = \left| \sum_{n=0}^{\infty} a_n p^n \right|_p = \lim_{N \to \infty} \left| \sum_{n=0}^{N} a_n p^n \right|_p$$

where $a_n \in \{0, \ldots, p-1\}$ for all n. Now, for all $N \geq m$ it is clear by definition that $\left| \sum_{n=0}^{N} a_n p^n \right|_p = p^{-m} > 0$. In the limit, we obtain $|x|_p > 0$: which is absurd.

$\bigcirc$

Corollary 4.2. *Let $x \in \mathbb{Z}_p$ for $p < \infty$. Then the coefficients of x are uniquely determined.*

PROOF. Let $x \in \mathbb{Z}_p$ and let $\sum_{n=0}^{\infty} a_n p^n = \sum_{n=0}^{\infty} b_n p^n$ be two representations for the integer x. We then have $\sum_{n=0}^{\infty} a_n p^n - \sum_{n=0}^{\infty} b_n p^n = \sum_{n=0}^{\infty} c_n p^n$. By Lemma 4.1 each $c_n = 0$. Now, if there were no "shifts" in the subtraction of a_n and b_n, then each $c_n = a_n - b_n$ and we are done. Otherwise, let m be the first index where a shift occurs. This implies that $a_n - b_n < 0$ and so $c_n = a_n - b_n + p = 0$, implying that $a_n - b_n = -p$, which is absurd because $a_n, b_n \in \{0, \ldots, p-1\}$.

$\bigcirc$

We may now delve into one of the more interesting topological properties regarding the p-adic integers. As mentioned previously, $\mathbb{Z}_p$ differs from $\mathbb{Z}$ in the sense that it is compact in $\mathbb{Q}_p$:

Theorem 4.3. *Let p be a prime with $p < \infty$. The topological ring $\mathbb{Z}_p$ is compact.*

PROOF. The proof given is here may also be found in [2, LEM-4]. Now, let (x_n) be a sequence in $\mathbb{Z}_p$ and for each n we write $x = \sum_{m \geq 0} x_n^{(m)} p^m$. Since each $x_n^{(0)}$ may attain only finitely many values, there is some $y_0 \in \{0, \ldots, p-1\}$ such that $x_n^{(0)} = y_0$ for infinitely many $n \geq 0$. This allows one to extract a subsequence (x_{0n}) such that for each $0n$ one has $x_{0n}^{(0)}$. We repeat the same procedure on this subsequence (x_{0n}), extracting some subsequence x_{1n} such that $x_{1n}^{(0)} = y_0$ and $x_{1n}^{(1)} = y_1$ at each index, where y_1 is as y_0 is. Repeating this indefinitely, we obtain a collection of sequences

$$\{(x_{kn})\}_{k=0}^{\infty}, \quad x_{kn}^{(a)} = y_a \text{ for all } 0 \leq a \leq k$$

We now construct a "diagonal sequence" $(x_m)_{m \geq 0}$ where we set $x_m := x_{mm}$ (i.e take the mth term from the mth subsequence). Then, we set

$$x := \sum_{a \geq 0} y_a p^a \in \mathbb{Z}_p,$$

To see that $\lim x_m = x$, write out:

$$|x_m - x|_p = \left| \sum_{a \geq 0} y_a p^a - \sum_{a \geq 0} x_m^{(a)} p^a \right|_p = \left| \sum_{a > m} x_m^{(a)} p^m \right|_p \leq p^{-(m+1)}$$

which vanishes as we let $m \to \infty$. This shows that $\mathbb{Z}_p$ is indeed compact.

$\bigcirc$

To further illustrate the differences between $\mathbb{Z}_p$ and $\mathbb{Z}$, we show that $\mathbb{Z}_p$ is uncountable.

Theorem 4.4. *For $p < \infty$ there is no bijection $\gamma : \mathbb{N} \to \mathbb{Z}_p$.*

Proof. This proof is by contradiction, and follows closely *Cantor's Diagonal Argument*. Assume that there is a bijection $\gamma : \mathbb{N} \to \mathbb{Z}_p$. Especially, we may enumerate the p-adic integers $\{x_1, x_2, \ldots\}$. Using Proposition 4.2 it is easily seen that each x_n has a unique representation of the form $x_n = \sum_{k \geq 0} x_n^{(k)} p^k$. We shall now construct some p-adic integer not in our enumeration.

Certainly, let for each $m \geq 0$ we define an integer y_k by setting

$$y_k := \begin{cases} 1 & x_k^{(k)} \neq 1 \\ 0 & \text{else} \end{cases}$$

Then, of course $y := \sum_{k \geq 0} y_k p^k$ is a valid element of $\mathbb{Z}_p$. Moreover, we observe that $y \neq x_n$ for all $n \in \mathbb{N}$. Indeed, for each x_n we have that $x_n^{(n)} \neq y_n$ and therefore this follows from the uniqueness ensured by Proposition 4.2.

$\bigcirc$

References

[1] Koblitz, Neal. *P-Adic Numbers, P-Adic Analysis, And Zeta-Functions*. 1st ed. Springer, 1975. Print.

[2] Zinzer, Scott. *Euclidean Models of the p-adic Integers*. Arizona State University. 2012.

[3] Marohnic, Julian. *The p-adics, Hensel's Lemma, and Newton Polygons*. University of Chicago. 2013.

[4] Dunne, Eiseart. *The p-adic Numbers*. Trinity College of Dublin. 2011.

[5] Robert, Alain M.*A Course in p-adic Analysis*, Springer, 200. ISBN 0-387-98669-3