The Analytic Development of the p-adic Numbers

Benjamin Inch

Abstract

This paper seeks to explore the wonders of the p-adic universe in terms of its analytic construction. After sketching the algebraic development of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ we will introduce the machinery of the p-adic norm and its corresponding metric along with a few of the topological curiousities of fields with non-Archimedean metrics. From here we will proceed to a proof of Ostrowski's theorem, illustrating its consequences for metric completions of the rationals and conclude by proving that $\mathbb{Q}_p$ with its norm is indeed a complete metric space. The aim throughout will be to remark on the similarities and differences with the usual completion of the rationals by the reals.

1 Introduction to the p-adic Numbers

1.1 The Algebraic Route

The p-adic numbers - where p will always and forever indicate a prime number - occupy a curious place within the intersection of number theory and analysis. In this way, their construction begets of both an algebraic and analytic approach. While I shall focus almost exclusively on the latter, any introduction to this unique subject would be found wanting were it to leave its algebraic conception completely untouched. Indeed, it provides a serendipitous point of entry their study.

Kurt Hensel was the first to introduce explicitly the p-adic numbers in his 1897 paper *Über eine neue Begründung der Theorie der algebraischen Zahlen* ("On a new grounding of the theory of algebraic numbers") and it is thus to him that we owe the famed Hensel's lemma. To wit:

Lemma 1. *(Hensel) Let $f(x) \in \mathbb{Z}[x]$ and $a \in \mathbb{Z}$ such that $f(a) \equiv 0 \ mod\ p^j$, for some $j \in \mathbb{Z}$. Assume $f'(a) \not\equiv 0 \ mod\ p$, ie. $\exists \lambda \in \mathbb{Z}/p\,\mathbb{Z} : \lambda f'(a) \equiv 1 \ mod\ p$. Then $\tilde{a} = a - \lambda f(a)$ satisfies $f(\tilde{a}) \equiv 0 \ mod\ p^{j+1}$.*

That is to say, if a polynomial with integer coefficients has a zero modulo some power of a prime with non-zero derivative at that point, then we can 'lift' said zero to a new one modulo the next integer power of that prime. This language of lifting is apt, since were we to 'lower' the zero back down again, ie. consider $\tilde{a}$ mod p^j, we would see immediately that

we get back our original term a. Moreover, as $f(a)$ is divisible by p^j, it is certainly divisible by p, such that $\tilde{a} = a - \lambda f(a) \equiv a \bmod p$ and so $f'(\tilde{a}) \equiv_p f'(a) \not\equiv_p 0$ and we can apply the lemma again to obtain zeroes of $f(x)$ for arbitrarily grand powers of p. In this sense, were we to start with $j = 1$, we would establish a sequence $(a_1, \ldots, a_n, \ldots)$ of zeroes of ~~some~~ polynomial modulo each prime power that were in a way 'coherent', that is:

$$a_n \equiv a_{n-1} \bmod p^{n-1}, \forall\, n > 1$$

This coherence is essential, as it allows us to take seriously the infinite length of our sequence and indeed the utility of Hensel's lemma is that it is applicable in this limit case, wherein we find the p-adic integers themselves. Consider the map $\varphi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$ given by $\varphi_n(a) = a \bmod p^{n-1}$, which is a surjective homomorphism with kernel $p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$. We establish a sequence of groups via these maps as such:

$$\ldots \overset{\varphi_{n+1}}{\to} \mathbb{Z}/p^n\mathbb{Z} \overset{\varphi_n}{\to} \mathbb{Z}/p^{n-1}\mathbb{Z} \overset{\varphi_{n-1}}{\to} \ldots \overset{\varphi_3}{\to} \mathbb{Z}/p^2\mathbb{Z} \overset{\varphi_2}{\to} \mathbb{Z}/p\,\mathbb{Z}$$

The p-adic integers, $\mathbb{Z}_p$ are algebraically conceived of as the *projective limit* of this system of groups and maps,[1] such that its elements are just those sequences $(a_1, \ldots, a_n, \ldots)$ that are coherent in the manner illustrated above, with $a_k \in \mathbb{Z}/p^k\mathbb{Z}$. Since addition and multiplication are well-defined under the modulus as operations on the representatives of equivalence classes, elements of $\mathbb{Z}_p$ permit coordinate-wise addition and multiplication, making it a subring of the direct product $\mathbb{Z}/p\,\mathbb{Z} \times \cdots \times \mathbb{Z}/p^n\mathbb{Z} \times \cdots$.

For an example of such a sequence, consider 37 as an element of $\mathbb{Z}_3$:

$$37 = ([37]_3, [37]_{3^2}, [37]_{3^3}, [37]_{3^4}, [37]_{3^5}, \ldots) = (1, 1, 10, 37, 37, \ldots) \in \mathbb{Z}_3$$

Notice that $37 = 1 + 0 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 0 \cdot 3^4 + \ldots$ in its base 3 expansion, where the partial sums correspond to the entries in the sequence. In the shorthand expression for this expansion, it is convenient to write $37 = \ldots 01101_3$ or simply 1101_3, where the zeroes implicitly continue to the left (much as $37 = 37.000\ldots$ in its decimal expansion). The p-adic integers are accordingly those numbers whose p-adic expansions contain no negative powers of p. Clearly $\mathbb{Z} \subset \mathbb{Z}_p$. Curiously enough, many rational numbers are also p-adic integers, ex. $\frac{1}{5} = \ldots 12102_3$, although this is less surprising when we recall that $\mathbb{Z}/p\,\mathbb{Z}$ is a field and so equations of the form $bx - a = 0, a, b \neq 0 : \gcd(b, p) = 1$ are by all means solvable modulo p and can accordingly be lifted with Hensel's lemma in order to give a solution in $\mathbb{Z}_p$ (whereas $\frac{1}{9} = 1 \cdot 3^{-2} = 0.01_3 \notin \mathbb{Z}_3$).

Not every element of $\mathbb{Z}_p$ has a multiplicative inverse - it is just a ring, or more precisely, an integral domain (no two non-zero elements can multiply to give the zero sequence; this is evident at least when the first entries are non-zero, as $\mathbb{Z}/p\,\mathbb{Z}$ is a field). The p-adic numbers proper, $\mathbb{Q}_p$ are thus realized as the field of fractions of $\mathbb{Z}_p$, where we formally afix the inverse

[1] We denote $\mathbb{Z}_p = \lim(\mathbb{Z}/p^n\mathbb{Z}, \varphi_n)$, where this limit goes 'to the left' and remark formally that, if R is a ring for which there exist homomorphisms ψ_n such that $R \overset{\psi_n}{\to} \mathbb{Z}/p^n\mathbb{Z} \overset{\varphi_n}{\to} \mathbb{Z}/p^{n-1}\mathbb{Z}$ gives the same map as (or 'commutes with') $R \overset{\psi_{n-1}}{\to} \mathbb{Z}/p^{n-1}\mathbb{Z}, \forall\, n \geq 1$, then there exists a unique homomorphism $R \to \mathbb{Z}_p$ from which all the ψ_n are obtained, ie. $\mathbb{Z}_p$ is the 'closest' ring to this system insofar as any other R can only map its way to each of the $\mathbb{Z}/p^n\mathbb{Z}$ groups in a manner that respects the order of the φ_n maps via $\mathbb{Z}_p$ itself.

of p to $\mathbb{Z}_p$, facilitating division by any non-zero element of $\mathbb{Z}_p$.

Hensel's motivation for exploring the p-adic numbers was to discover an analogy between the power series expansion near a given point of a function and the p-adic expansion of a number.[2] Much as power series use local data, viz. values of subsequent derivatives at a point, to give 'global' information about the behaviour of a function on an interval, Hensel hoped to use the 'local' p-adic expansions as well as the real numbers to discover general properties of the zeroes of certain polynomials. However, Hensel did not employ this 'local-global' language in practice. This was properly the approach of Helmut Hasse, whose generalization of a theorem first proved for the case $\mathbb{K} = \mathbb{Q}$ by Hermann Minkowski is one of the masterpieces of twentieth century number theory.

Theorem 1. *(Hasse-Minkowski) In order for a quadratic form, ie. a homogeneous polynomial of degree two in n variables, to have a non-trivial zero in a number field $\mathbb{K}$, it is necessary and sufficient for it to have a non-trivial zero in $\mathbb{R}$ and $\mathbb{Q}_p$, $\forall\, p$.*

For a proof of this theorem and a far more incisive treatment of everything covered in this section, I encourage the reader to consult the text by Jean-Pierre Serre mentioned in the bibliography. What is of interest for our purposes is the matter of *convergence*.

1.2 The p-adic Norm

The 'well-behaved' functions of real analysis are just those whose (infinite) power series converge to finite values on an interval of interest. Similarly, we should like it if the p-adic numbers, which we shall see are akin to the reals insofar as they form a 'metric completion' of the rationals, were also well-behaved. Consider $\ldots 111_p = 1 + p + p^2 + \ldots + p^n + \ldots \in \mathbb{Z}_p$. With respect to the usual measure of cardinality, the absolute value, we see that since p is greater than one:

$$|1 + p + \ldots + p^n + \ldots| = \left| \sum_{n=0}^{\infty} p^n \right| \to \infty$$

Indeed, anyone with some background in calculus would hardly find this surprising. The fantastic insight behind the invention of p-adic analysis is that - algebraically speaking - there is no 'intuitive' notion of size! When our goal is number theoretic, such as that of Hensel and Hasse, we have no reason for preferring the norm given by the absolute value to any other. In order to mitigate troublesome sequences such as these, we are charged to find a norm with respect to which high powers of p are measurably small. This will furnish us with a metric that judges numbers as being close together not when the magnitude of their difference, or relative position on the real line, is comparatively small, but when they are both divisible by a similarly high power of p.

We presume that the reader is already familiar with the definitions of a norm and metric. Let us define $\mathrm{ord}_p : \mathbb{Q} \to \mathbb{Z}$ by $\mathrm{ord}_p(r) = t : r = p^t r_o$, where $p \not| r_o$ and $r \in \mathbb{Z}$ (if $p \not| r$, then $\mathrm{ord}_p(r) = 0$). When $r = \frac{a}{b} \in \mathbb{Q}$, $\mathrm{ord}_p(r) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$. If $r = 0$, we write $\mathrm{ord}_p(0) = \infty$.

[2] More precisely, he was concerned with the similar role played by prime numbers in number fields and linear factors in Laurent series of holomorphic functions.

Definition The p-adic norm, $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ and its metric $d_p(x,y) : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}_{\geq 0}$:

$$|x|_p = \begin{cases} p^{-\text{ord}_p(x)} & x \neq 0 \\ 0 & x = 0 \end{cases} \qquad d_p(x,y) = \begin{cases} p^{-\text{ord}_p(x-y)} & x \neq y \\ 0 & x = y \end{cases}$$

For example, $|250|_5 = |2 \cdot 5^3|_5 = \frac{1}{5^3} < |35|_5 = |6 \cdot 5|_5 = \frac{1}{5}$, such that numbers containing high powers of 5 are smaller than those that do not with respect to $|\cdot|_5$. As one might guess, the topology or spatial structure put on the rationals by such a metric will be quite peculiar by comparison with that given by the absolute value. For one thing, there is no notion of 'order', in terms of which we could arrange our numbers along a line from greatest to least, ex. $|125| < |216| < |250|$ with the absolute value, yet $|125|_5 = |250|_5 < |216|_5$ - which goes first?

A variety of topological curiousities are due to the fact that the p-adic metric is *non-Archimedean*: it satisfies a stronger version of the triangle inequality,[3] viz.

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

Proof. Take $x,y,z \in \mathbb{Q}$, then $x-y = (x-z)+(z-y)$ where we can write $x-z = p^{r_1}a_1$ and $z-y = p^{r_2}a_2$ such that neither a_1 nor a_2 are divisible by p. So $(x-z)+(z-y) = p^{r_1}a_1 + p^{r_2}a_2 = p^{\min\{r_1,r_2\}}k$ where $p \not| k$. Accordingly, $\text{ord}_p(x-y) \geq \min\{r_1,r_2\}$ so $p^{-\text{ord}_p(x-y)} = d_p(x,y) \leq \max\{p^{-r_1}, p^{-r_2}\} = \max\{d_p(x,z), d_p(z,y)\}$. □

We now demonstrate two classic oddities of non-Archimedean metrics on a field.

Proposition 1. *"All triangles are isosceles."*

Proof. The triangle inequality takes its name from the fact that in the complex plane with the usual Euclidean metric, the sum of two sides of a triangle is greater than the third side (with equality when one point of the 'triangle' lies on the line between the other two). The point of the proposition is that any triangle constructed between three non-collinear points via a non-Archimedean metric has at least two equal sides.

Let $|\cdot|$ be a non-Archimedean metric with $x,y,z \in \mathbb{F} : x,y \neq 0,\ z = 0$, then $d(x,y) = |x-y| \leq \max\{|x|,|y|\}$. Suppose first that $|x| < |y|$, ie. these two sides have different length. By the above inequality, the length of the third side, $x-y$ is thus $|x-y| \leq |y|$. Yet consider:

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

As $|y| > |x|$, it must be the case that $|y| \leq |x-y|$. Therefore, $|y| = |x-y|$, such that these two sides are equal. □

Proposition 2. *"Every point in an open disc is at its centre."*

Proof. Recall that an open disc of radius $r \in \mathbb{R}_{>0}$ with centre $a \in \mathbb{F}$ is given by

$$D(a,r) = \{x \in \mathbb{F} : |x-a| < r\}$$

[3] $d(x,y) \leq d(x,z) + d(z,y)$, metrics which satisfy only this inequality are called *Archimedean*, ex. the ordinary absolute value.

We can restate the proposition as follows: if $b \in D(a,r)$, then $D(b,r) = D(a,r)$.

If $x \in D(a,r)$, then $|x-a| < r$; since $b \in D(a,r)$, $|a-b| < r$ as well. Consider:

$$|x-b| = |(x-a)+(a-b)| \leq \max\{|x-a|, |a-b|\} < r$$

Therefore, $x \in D(b,r)$ and $D(a,r) \subseteq D(b,r)$. We prove the reverse for $x \in D(b,r)$ in the exact same way to obtain equality. □

In $\mathbb{R}$, the open discs under the absolute value are open intervals on the real line. The topology of the p-adic numbers is clearly not so easily imagined! See the opening pages of the text by Koblitz mentioned in the bibliography for an artist's enchanting conception of the 3-adic unit disc. A consequence of the second proposition is that two non-equal open discs under a non-Archimedean metric are either disjoint or one is contained within the other.

Our final concern in this section is a bit more technically advanced and deals with *connectedness*. In a metric space (X,d), that is a non-empty set with a metric in which any two points have an associated distance or value on that metric, a subset E is said to be *open* if every point a within it has a neighbourhood, ie. is the centre of an open disc of some radius, such that $D(a,r) \subset E$. A point a is called a limit point of E if every neighbourhood of a contains a point $b \neq a : b \in E$; the limit points of typical interest are those on the *boundary* of an open set. E is said to be *closed* if it contains all its limit points, such as the union of an open set with its boundary, the so-called *closure* of that open set. Examples in $(\mathbb{R}, |\cdot|)$ are the open discs $D(a,r)$, which have boundary $D'(a,r) = \{x \in \mathbb{R} : |x-a| = r\}$, and the closed discs $\overline{D}(a,r) = \{x \in \mathbb{R} : |x-a| \leq r\}$.

Definition Two subsets A, B of a metric space are said to be *separated* if both $A \cap \overline{B}$ and $\overline{A} \cap B$ are empty, ie. if no point of A lies in the closure of B and vice versa.

A set $E \subset X$ is *connected* if E is *not* a union of two non-empty separated sets.

The reader is encouraged to consult the text by Rudin mentioned in the bibliography if they are unfamiliar with these notions. What should be straightforward is to remark that any open interval on the real line is connected (try to find a separation of $(0,1) = A \cup B$ according to the definition above if you are unconvinced). In the non-Archimedean case, however, there are no non-trivial (ie. containing more than a single point) connected sets. We say such a space, ex. $(\mathbb{Q}_p, |\cdot|_p)$, is *totally disconnected*.

Lemma 2. *$D(a,r) \subset X$, a non-Archimedean metric space, is both open and closed.*

Proof. Assure yourself via the definition above that $D(a,r)$ is indeed an open set. Suppose $x \in X$ is a limit point of $D(a,r)$ and choose a number $s \leq r$, then $\exists\, y \in D(a,r) \cap D(x,s)$ (any neighbourhood of x contains a point in $D(a,r)$), which means $|y-a| < r$ and $|y-x| < s \leq r$. By the non-Archimedean inequality:

$$|x-a| \leq \max\{|x-y|, |y-a|\} < \max\{s,r\} \leq r$$

Therefore, $x \in D(a,r)$ and the open disc contains all its limit points; it is closed. □

Theorem 2. *X is totally disconnected, ie. if $a \in X$, the largest subset $C \subset X : a \in C$ and C is connected is just $\{a\}$.*

Proof. Suppose $C \supsetneq \{a\}$, for arbitrary a. We can choose $r > 0 : D(a,r) \cap C \neq C$. Without loss of generality, C is closed.[4] Consider:

$$C = (D(a,r) \cap C) \cup (D(a,r)^{\mathsf{c}} \cap C)$$

Where $D(a,r)^{\mathsf{c}}$ is the complement of $D(a,r)$, ie. the set of all points not in $D(a,r)$. $D(a,r)$ is closed and, noting that the intersection of a closed set with a closed set is closed, so is $D(a,r) \cap C$. $D(a,r)$ is open and, noting that the complement of an open set is closed, $D(a,r)^{\mathsf{c}} \cap C$ is closed. We have thus expressed C as the disjoint union of two closed sets, which contradicts our assumption that C was connected. Therefore $C = \{a\}$. □

2 Constructing $\mathbb{Q}_p$

2.1 Ostrowski's Theorem

Recall that $\mathbb{R}$ is the metric completion of $\mathbb{Q}$ with respect to the absolute value. That is, we can use the equivalence classes of Cauchy sequences[5] on $|\cdot|$ to 'fill in the gaps' between rational and irrational numbers (like $\sqrt{2}$). As will be shown, $\mathbb{Q}_p$ is also a complete metric space containing $\mathbb{Q}$, but of course $\mathbb{Q}_p$ is nothing like $\mathbb{R}$. Despite the many startling differences between Archimedean and non-Archimedean metric spaces, as far as norms on the rationals are concerned, our choices are surprisingly limited. The proof of this fact, viz. Ostrowski's theorem, is extremely compelling - albeit challenging - and we will first need some facts about equivalent norms to provide it. Two norms are equivalent if they establish the same topology (ie. sets open with respect to one norm are open with respect to the other). However, this is not an extremely useful definition for our purposes, so we use the following lemma.

Lemma 3. *For $|\cdot|_1, |\cdot|_2$ non-trivial norms[6] on a field $\mathbb{F}$, the following are equivalent:*

i) $|\cdot|_1$ *and* $|\cdot|_2$ *are equivalent.*

ii) $|x|_1 < 1$ *iff* $|x|_2 < 1, \forall\, x \in \mathbb{F}$

iii) There exists $\alpha \in \mathbb{R}_{>0} : |x|_1 = |x|_2^{\alpha}, \forall\, x \in \mathbb{F}$.

Proof. As follows:

i) ⇒ ii) One consequence of equivalence is that a sequence that converges with respect to $|\cdot|_1$ will do so on $|\cdot|_2$ as well. Consider the sequence $\{x^n\}$, convince yourself that, regardless of the metric chosen:

$$\lim_{n\to\infty} x^n = 0 \Leftrightarrow |x| < 1$$

For the implication to the right, test the claim for $\varepsilon < 1$; to the left, notice $|x| \in \mathbb{R}_{>0}$ means $|x| = \frac{1}{1+s}$ for some $s \in \mathbb{R}_{>0}$ and apply Bernoulli's inequality. Then $|x|_1 < 1$

[4] C is in fact a *connected component*, which means it is a closed subset of X; $C = \{a\}$ is indeed closed.

[5] A sequence $\{a_n\}$ in a metric space is *Cauchy* if for any $\varepsilon > 0, \exists\, N \in \mathbb{N} : m, n \geq N$ implies $d(a_n, a_m) < \varepsilon$.

[6] The trivial norm is just $|x| = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$.

implies the above limit goes to zero with respect to $|\cdot|_1$, which means it does so for $|\cdot|_2$ by their equivalence and thus that $|x|_2 < 1$.

ii) $\Rightarrow$ iii) First take any $x_o \in \mathbb{F} : |x_o|_1 \neq 1$ (such an element must exist, otherwise $|\cdot|_1$ is the trivial norm). If $|x_o|_1 > 1$, as we are in a field, $x_o^{-1} \in \mathbb{F}$ and $|x_o^{-1}|_1 = |x_o|_1^{-1} < 1$, so we can assume that $|x_o|_1 < 1$. By ii), $|x_o|_2 < 1$, so there exists some $\alpha \in \mathbb{R} : |x_o|_1 = |x_o|_2^{\alpha}$ and thus that $|x_o^n|_1 = |x_o^n|_2^{\alpha}, \forall\ n \in \mathbb{N}$. The trick is to show that this α works for any $x \in \mathbb{F}$.

Next take $x \in \mathbb{F} : x \neq x_o$. If $|x|_1 = |x_o|_1$, claim $|x|_2 = |x_o|_2$ and suppose otherwise. If $|x|_2 < |x_o|_2$, then $|\frac{x}{x_o}|_2 < 1$, meaning $|\frac{x}{x_o}|_1 < 1$, which is clearly not the case. If $|x|_2 > |x_o|_2$, then $\left|\frac{x_o}{x}\right|_2 < 1$, giving the same contradiction. Thus our choice of α holds for such x. If $|x|_1 = 1$, then $|x|_2 = 1$ by an argument identical to the one above for $|x_o|_2 = 1$ and the choice of α holds trivially. Take $x \in \mathbb{F} : |x|_1 \neq 1, |x|_1 \neq |x_o|_1$, as before we can assume that $|x|_1 < 1$ and so $|x|_2 < 1$ and there is some $\beta \in \mathbb{R} : |x|_1 = |x|_2^{\beta}$ and $|x^n|_1 = |x^n|_2^{\beta}$. For $n, m \in \mathbb{N}$, we have that:

$$|x|_1^m < |x_o|_1^n \Leftrightarrow \left|\frac{x^m}{x_o^n}\right|_1 < 1 \Leftrightarrow \left|\frac{x^m}{x_o^n}\right|_2 < 1 \Leftrightarrow |x|_2^m < |x_o|_2^n$$

Take logarithms of the first and last inequalities above.

$$m \ln |x|_1 < n \ln |x_o|_1 \Leftrightarrow m \ln |x|_2 < n \ln |x_o|_2$$

Rearranging the results, we obtain:

$$\frac{n}{m} > \frac{\ln |x_o|_1}{\ln |x|_1} \Leftrightarrow \frac{n}{m} > \frac{\ln |x_o|_2}{\ln |x|_2}$$

Thus, the set of fractions $\frac{n}{m}$ that are bigger than the quotient on the left is exactly the same as the set of those bigger than that on the right. Since n, m were arbitrary, this set is just $\mathbb{Q}_{>0}$, which is dense in $\mathbb{R}_{>0}$, ie. the image of the logarithm, and we can conclude that the two quotients are in fact equal. Keeping in mind that $|x_o|_1 = |x_o|_2^{\alpha}$ and $|x|_1 = |x|_2^{\beta}$, consider the following:

$$\frac{\ln |x_o|_1}{\ln |x|_1} = \frac{\ln |x_o|_2}{\ln |x|_2} \Leftrightarrow \frac{\ln |x_o|_1}{\ln |x_o|_2} = \frac{\ln |x|_1}{\ln |x|_2} \Leftrightarrow \frac{\ln |x_o|_2^{\alpha}}{\ln |x_o|_2} = \frac{\ln |x|_2^{\beta}}{\ln |x|_2} \Leftrightarrow \alpha = \beta$$

Which gives the desired result.

iii) $\Rightarrow$ i) By iii), we see that:

$$|x - a|_1 < r \Leftrightarrow |x - a|_2^{\alpha} \Leftrightarrow |x - a|_2 < r^{\frac{1}{\alpha}}$$

Therefore any open disc with respect to $|\cdot|_1$ is also an open disc on $|\cdot|_2$. The topology on a metric space is actually established via its open discs, so this is sufficient to prove that $|\cdot|_1$ and $|\cdot|_2$ are equivalent.

$\square$

Theorem 3. *(Ostrowski) Every non-trivial norm on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some p or else the ordinary absolute value (the so-called $p = \infty$ case)*[7].

Proof. In all that follows $|\cdot|$ is some non-trivial norm. ($|\cdot|_\infty$ is the absolute value.)

Case 1: Suppose there exists $n \in \mathbb{N} : |n| > 1$. By well-ordering, there is a least such n, call it n_o. Since $|n_o| > 1$, we can find (using logarithms) some $\alpha \in \mathbb{R}_{>0} : |n_o| = n_o^\alpha$ Take any $n \in \mathbb{N}$, write it to the base n_o and take its norm.

$$\begin{aligned} n &= a_0 + a_1 n + a_2 n^2 + \ldots + a_s n^s, \text{ where } 0 \leq a_i < n_o,\ a_s \neq 0 \\ |n| &\leq |a_0| + |a_1| n_o^\alpha + |a_2| n_o^{2\alpha} + \ldots + |a_s| n^{s\alpha} \end{aligned}$$

Since $a_i < n_o$ and n_o is the least integer to have norm greater than one, $|a_i| \leq 1, 1 \leq i \leq s$.

$$\begin{aligned} |n| &\leq 1 + n_o^\alpha + n_o^{2\alpha} + \ldots + n_o^{s\alpha} \\ &= n_o^{s\alpha}(1 + n_o^{-\alpha} + n_o^{-2\alpha} + \ldots + n_o^{-s\alpha} \\ &\leq n^\alpha \sum_{i=0}^{\infty} \left(\frac{1}{n_o^\alpha}\right)^i \end{aligned}$$

Where, since $a_s \neq 0$, $n \geq n_o^s$. As $n_o^\alpha > 1$, the above sum converges to a finite constant, call it C. It is thus the case that $|n| \leq C n^\alpha, \forall\ n \in \mathbb{N}$. Take $N \in \mathbb{N}$, consider:

$$|n^N| = |n|^N \leq C(n^N)^\alpha = C(n^\alpha)^N \Leftrightarrow |n| \leq \left(\sqrt[N]{C}\right) n^\alpha$$

Fix n and let $N \to \infty$, then we see that $|n| \leq n^\alpha$.

Take n in its base n_o expansion as before, then $n_o^{s+1} > n \geq n_o^s$. As $|n_o^{s+1}| = |n + n_o^{s+1} - n| \leq |n| + |n_o^{s+1} - n|$, we have that $|n| \geq |n_o^{s+1}| - |n_o^{s+1} - n| \geq n_o^{(s+1)\alpha} - (n_o^{s+1} - n)^\alpha$. Since $n \geq n_o^s$:

$$|n| \geq n_o^{(s+1)\alpha} - \left(n_o^{s+1} - n_o^s\right)^\alpha = n_o^{(s+1)\alpha}\left[1 - \left(1 - \frac{1}{n_o}\right)^\alpha\right] \geq C' n^\alpha$$

As $n_o^{s+1} > n$, for some constant C' that does not depend on n. Substituting in n^N and taking the limit of N^{th}-root as before, we see that $|n| \geq n^\alpha$ and accordingly that $|n| = n^\alpha$. For $x = \frac{n}{m} \in \mathbb{Q}_{>0}$:

$$\left|\frac{n}{m}\right| = \frac{|n|}{|m|} = \left(\frac{n}{m}\right)^\alpha$$

By the multiplicative property of norms. If $n \in \mathbb{Z}$ or $x \in \mathbb{Q}$ is negative, the fact that $|\cdot|$ is a norm entails $|n|, |x| \geq 0$ (with equality iff $n = x = 0$) and the above still holds when we note that the equality is in fact $|x| = |x|_\infty^\alpha$, which by the lemma means $|\cdot|$ is equivalent to the absolute value.

Case 2: Suppose that $|n| \leq 1, \forall\ n \in \mathbb{N}$. As $|\cdot|$ is non-trivial, there is a least such $n : |n| < 1$, call it n_o. Claim that n_o must be prime and suppose otherwise, viz. $n_o = n_1 \cdot n_2$. Since $n_1, n_2 < n_o$, $|n_1| = |n_2| = 1$ and so $|n_o| = 1$, contradicting the above. Let $n_o = p$.

[7]Although John Conway has contested that, insofar as Ostrowski has given us a kind of fundamental theorem of arithmetic for norms, the absolute value should instead be thought of as the case when $p = -1$.

Claim next that $|q| = 1$ for any prime $q \neq p$. Suppose otherwise, then $|q| < 1$ and we can find some $M, N \in \mathbb{N}$ large enough: $|q^N| = |q|^N < \frac{1}{2}$ and $|p^M| < \frac{1}{2}$. As $\gcd(p^M, q^N) = 1$, $\exists m, n \in \mathbb{N} : mp^M + nq^N = 1$. Consider:

$$1 = |1| = |mp^M + nq^N| \leq |mp^M| + |nq^N| = |m| \cdot |p^M| + |n| \cdot |q^N| \leq |p^M| + |q^N| < \frac{1}{2} + \frac{1}{2} = 1$$

Where we used the fact that $|m|, |n| \leq 1$. Evidently $1 < 1$ is a contradiction, so $|q| = 1$. Take $a \in \mathbb{N}$, by the fundamental theorem of arithmetic:

$$a = p_1^{s_1} \cdot p_r^{s_r} \Rightarrow |a| = |p_1|^{s_1} \cdot |p_r|^{s_r} = \begin{cases} 1 & p \text{ is not a factor of } a \\ |p_i|^{s_i} & \text{where } p_i = p \end{cases}$$

Let $c = |p|^{-1}$, then $|a| = c^{-\mathrm{ord}_p(a)}$. As above, multiplicativity and positivity of the norm give us the same equality for $x \in \mathbb{Q}$. Solving $c^{-\mathrm{ord}_p(x)} = \left(p^{-\mathrm{ord}_p(x)}\right)^{\alpha}$, for $\alpha \in \mathbb{R}$, we find that:

$$|x| = |x|_p^{\frac{\ln c}{\ln p}}$$

□

Alexander Ostrowski proved this theorem in 1916 when he was nearing twenty-three years old. Hasse gave the proof of his theorem in his dissertation five years later, about the time that he was twenty-three as well! The implications of the former result, that in studying functions on $\mathbb{Q}$ or perhaps any other number field, one should consider their behaviour with respect to the absolute value and p-adic norms, and thus on $\mathbb{R}$ and $\mathbb{Q}_p$, seem clear to the development of the latter.

2.2 $\mathbb{Q}_p$ is Complete

A metric space is *complete* if every Cauchy sequence of elements of that space converges such that each limit is an element of the space. As was said earlier, $\mathbb{Q}$ is not complete with respect to the absolute value. Nor is it with respect to the p-adic norm; to start to convince yourself of this fact, find a p such that $x^2 - 2$ has a solution in $\mathbb{Z}/p\,\mathbb{Z}$ and use it to construct a coherent sequence in $\mathbb{Z}_p$ using Hensel's lemma. In other words, show that $\sqrt{2} \in \mathbb{Q}_p$ for said p. To show that $\mathbb{Q}_p$ is complete, we will first sketch the construction of $\mathbb{Q}_p$ as the set of equivalence classes of Cauchy sequences with respect to $|\cdot|_p$.

Definition For $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$, let $\mathcal{C} = \{(x_n) : x_i \in \mathbb{Q}, (x_n) \text{ is Cauchy with respect to } |\cdot|_p\}$. Note that $\mathcal{C}$ is a ring with identity which contains $\mathbb{Q}$ under the inclusion $x \mapsto (x)$, the constant sequence.

Let $\mathcal{N} = \{(x_n) : \lim |x_n|_p = 0\} \subset \mathcal{C}$ be the set of sequences tending to zero. Note that $\mathcal{N}$ is a maximal ideal of $\mathcal{C}$, ie. any ideal generated by $(x_n) \in \mathcal{C} - \mathcal{N}$ and $\mathcal{N}$ is in fact all of $\mathcal{C}$. Finally, we define the field of p-adic numbers as the quotient of $\mathcal{C}$ by $\mathcal{N}$:

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

The p-adic norm extends to $\mathbb{Q}_p$ as follows. For $\lambda \in \mathbb{Q}_p$ represented by the Cauchy sequence (x_n), we define:

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

We remark formally that this last definition is sound because any $(x_n) \in \mathcal{C}-\mathcal{N}$ eventually stabilises. That is, there exists $N \in \mathbb{N} : |x_n|_p = |x_m|_p$ whenever $m, n \geq N$.

Proof. (x_n) does not tend to zero, so there exists $c, N_1 : n \geq N_1$ implies $|x_n| \geq c > 0$. However, there exists $N_2 : n, m \geq N_2$ entails $|x_n - x_m| < c$. Let $N = \max\{N_1, N_2\}$, then for $n, m \geq N$, we have that $|x_n - x_m| \leq \max\{|x_n|, |x_m|\}$ and is also less than c, yet $|x_n|, |x_m| \geq c$. $|x_n| = |x_m|$ accordingly. □

Elements of $\mathcal{C}$ which differ by an element of $\mathcal{N}$ should presumably converge to the same limit and so we identify them in $\mathbb{Q}_p$. As well, $\mathbb{Q}_p$ still contains $\mathbb{Q}$ under the inclusion $(x) \mapsto (x)+\mathcal{N}$, since two distinct constant sequences differ only by another constant sequence and so they remain distinct in $\mathbb{Q}_p$. However, we can say even more than this.

Proposition 3. *The image of $\mathbb{Q}$ under its inclusion is a dense subset[8] of $\mathbb{Q}_p$.*

Proof. Suppose $\lambda \in \mathbb{Q}_p$ is represented by the Cauchy sequence (x_n) and has neighbourhood $D(\lambda, \varepsilon)$. Then there exists $N \in \mathbb{N} : n, m \geq N$ entails $|x_n - x_m|_p < \varepsilon$. Let $y = x_N$ and consider the constant sequence $(y) \in \mathbb{Q}_p$. Claim that $(y) \in D(\lambda, \varepsilon)$, ie. $|\lambda - (y)|_p < \varepsilon$. Notice that $\lambda - (y)$ is represented by the sequence $(x_n - y)$, where $|(x_n - y)|_p = \lim |x_n - y|_p$. However, for any $n \geq N$, $|x_n - y|_p = |x_n - x_N|_p < \varepsilon$. Taking the limit gives the result, where ε was arbitrary. □

This mirrors the situation where $\mathbb{Q}$ is dense in $\mathbb{R}$.

Theorem 4. *$\mathbb{Q}_p$ is complete with respect to $|\cdot|_p$.*

Proof. Take (λ_n), a Cauchy sequence of elements of $\mathbb{Q}_p$, such that each $\lambda_i \in \mathbb{Q}_p$ is itself a Cauchy sequence in $\mathbb{Q}$ up to equivalence. First construct a candidate limit for (λ_n).

By the density of the inclusion of $\mathbb{Q}$ in $\mathbb{Q}_p$, for each $\lambda_i \in \mathbb{Q}_p$, there exists a constant sequence $(y^{(i)}) \in \mathbb{Q}_p$: $|\lambda_i - (y^{(i)})|_p < p^{-i}$. Accordingly, for any $\varepsilon > 0$, there is $N >> 0 : n \geq N$ entails $|\lambda_n - (y^{(n)})|_p < p^{-n} < \varepsilon$. Conclude that

$$\lim_{n\to\infty} |\lambda_n - (y^{(n)})|_p = 0$$

Next show that $y^{(1)}, \ldots, y^{(n)}, \ldots$ is a Cauchy sequence in $\mathbb{Q}$. Let $\lambda_i \in \mathbb{Q}_p$ be represented by $(x_n^{(i)})$. Similar to the above, notice:

$$|\lambda_i - (y^{(i)})|_p = |(x_n^{(i)}) - (y^{(i)})|_p = |(x_n^{(i)} - y^{(i)})|_p = \lim_{n\to\infty} |x_n^{(i)} - y^{(i)}|_p < p^{-i}$$

Since (λ_n) is Cauchy, there exists $M \in \mathbb{N}$: for $j, k \geq M$ we have

$$|\lambda_j - \lambda_k|_p = |(x_n^{(j)}) - (x_n^{(k)})|_p = |(x_n^{(j)} - x_n^{(k)})|_p = \lim_{n\to\infty} |x_n^{(j)} - x_n^{(k)}|_p < p^{-M}$$

[8] Any open neighbourhood of a point in $\mathbb{Q}_p$ contains an element of $\mathbb{Q}$.

By the non-Archimedean inequality for $|\cdot|_p$:

$$|y^{(r)} - y^{(s)}|_p \leq \max\{|y^{(r)} - x_n^{(r)}|_p, |x_n^{(r)} - y^{(s)}|_p\}$$
$$|x_n^{(r)} - y^{(s)}|_p \leq \max\{|x_n^{(r)} - x_n^{(s)}|_p, |x_n^{(s)} - y^{(s)}|_p\}$$

$$\therefore |y^{(r)} - y^{(s)}|_p \leq \max\{|x_n^{(r)} - y^{(r)}|_p, |x_n^{(r)} - x_n^{(s)}|_p, |x_n^{(s)} - y^{(s)}|_p\}$$

Given the above results, any of these three magnitudes can be made smaller than an arbitrary negative power of p for r, s sufficiently large. Conclude that the sequence is Cauchy.

Let $\lambda \in \mathbb{Q}_p$ be the element corresponding to the sequence $(y^{(n)})$, where we let n vary. Consider:

$$|\lambda_n - \lambda|_p = |(x_m^{(n)}) - (y^{(m)})|_p = |(x_m^{(n)} - y^{(m)})|_p = \lim_{m\to\infty} |x_m^{(n)} - y^{(m)}|_p$$

As $|x_m^{(n)} - y^{(m)}|_p \leq \max\{|x_m^{(n)} - x_m^{(m)}|_p, |x_m^{(m)} - y^{(m)}|_p\}$, we see that, given n sufficiently large and letting $m \to \infty$, either of the two magnitudes approaches zero. Conclude that:

$$\lim_{n\to\infty} \lambda_n = \lambda$$

Since an arbitrary Cauchy sequence in $\mathbb{Q}_p$ converges to a limit in $\mathbb{Q}_p$, it is complete. □

With this new understanding of $\mathbb{Q}_p$, we can actually reformulate the p-adic integers as $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}$. It should also be said that the p-adic expansion of any element of $\mathbb{Q}_p$, while permitting of infinitely many terms with positive powers of p, has only finitely many with negative powers.

My motivation to provide a proof - however laborious - of the fact that $\mathbb{Q}_p$ is complete came from its absence in the texts mentioned in the bibliography by Gouvêa and Koblitz, although the proof follows a program outlined by the former. Having some theoretical grasp of the foundations of p-adic analysis, I urge the reader to consult these texts in order to explore its techniques more thoroughly. For all its topological curiousities, one discovers that many results from calculus translate fluidly in the p-adic universe (with the marked exception of the mean-value theorem) and, thanks to the non-Archimedean inequality, are often easier to prove!

Bibliography

Darmon, H. *MATH 346/377 Lecture Notes.* McGill University, 2013.
Gouvêa, F. Q. *p-adic Numbers: An Introduction.* Springer-Verlag, 1997.
Koblitz, N. *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* Springer-Verlag, 1984.
Rudin, W. *Principles of Mathematical Analysis.* McGraw-Hill, 1976.
Serre, J-P. *Cours d'arithmétique.* Presses Universitaires de France, 1970.
Historical data and some examples were culled from Wikipedia.