DA GREAT BEANY TREATISE ON P-ADICS

HELENA HEINONEN

1. introduction

It wasn't obvious to the Greeks that there are numbers that couldn't be written as a ratio of two numbers. Pythagoras and his followers were deep admirers of numerical ratios and studied their existence in the world, as they arose in music, geometry, cosmology, and the body. In fact, they believed that all numbers could be represented as a ratio —meaning a rational number — and the existence of an *irrational* number was seen as an affront to the gods [oA30, p64]. Legend says that in 470 B.C. when Hippasus proved the irrationality of $\sqrt{2}$, he was drowned for spreading such absurd truths! [Ang94, p35]

In this paper we'll discuss how we can rigorously think of these crazy irrational numbers as a sequence of the more familiar rationals, using a process called completion of a metric space. By defining different metrics on $\mathbb{Q}$ we can obtain more exotic number systems, such as the p-adics. Not only do irrational numbers such as $\sqrt{2}$ appear in the p-adics, but we can also find solutions to equations such as $f(x) = -1$, which have no *real* solutions!

2. Mathematical Background

2.1. **Construction of the Real Numbers.** First we want to discuss how one can construct the set of real numbers by completing the rationals.

When dealing with a set of numbers, we often want to have a way to measure the distance between two of them. This desire introduces the notion of a *metric.*

Definition 2.2. [Rud76, Def 2.15] Let M be a set. A function

$$d : M \times M \to \mathbb{R}$$

is a *metric* if for all $(x, y) \in M \times M$ we have:

(1) $d(x, y) \geq 0$ and $d(x, y) = 0$ if and only if $x = y$
(2) $d(x, y) = d(y, x)$ for all $x, y \in M$
(3) $d(x, y) \leq d(x, z) + d(z, y)$ for all $x, y, z \in M$

We define a *metric space* (M, d) to be a set of elements M equipped with a metric d.

Example 2.3. In $\mathbb{Q}$, we usually define the metric as the *Euclidean Distance*: $d(x, y) = |x-y|$ for all $x, y \in \mathbb{Q}$. Notice the Euclidean metric on $\mathbb{Q}$ takes on values only in $\mathbb{Q}$ rather than all of $\mathbb{R}$.

Certain quantities, such as the solutions to the equation $x^2 = 2$ or the circumference of a circle of diameter 1, cannot be written as a ratio of integers. However, we can think of these quantities as a limit of rational numbers approximating them arbitrarily well. Formally, we can think of a real number as the limit of a Cauchy sequence of rational numbers:

Definition 2.4. [Rud76, Def 3.8] Let (M, d) be a metric space. The sequence $(a_n) \in M$ is *Cauchy* if for all $\epsilon > 0$ there exists positive integer N such that if $m, n > N$ then $d(a_m, a_n) < \epsilon$.

For example, we can think of the real number π as (the limit of) this Cauchy sequence of rationals:

$$(3, 3.1, 3.14, 3.141, 3.1415, 3.14159, ...)$$

Notice, that this is not the *only* Cauchy sequence converging to π. We could also write $(3, 3.14, 3.1415, 3.141592, ...)$. This motivates the idea of equivalent Cauchy sequences:

Definition 2.5. Two Cauchy sequences (a_n) and (b_n) are called *equivalent* if $d(a_n, b_n) \to 0$ as $n \to \infty$.

One can verify that Definition 2.5 is in fact an equivalence relation by checking reflexivity, symmetry, and transitivity. Now, we can define the completion of a metric space:

Definition 2.6. [Rud76, Def 3.12] A metric space (M, d) is *complete* if every Cauchy sequence in M converges to a unique point in M.

Given any metric space, there is a natural way to complete it to obtain a complete metric space.

Definition 2.7. [Kat07, Thm 1.1] Let (M, d) be a metric space. The *completion* $(\widehat{M}, \widehat{d})$ is the set of all equivalence classes of Cauchy sequences of elements in M. The metric $\widehat{d}$ between two equivalence classes represented by (a_n) and (b_n) respectively is defined to be:

$$\widehat{d}((a_n), (b_n)) = lim_{n\to\infty} d(a_n, b_n).$$

Implicit in the statement of Definition 2.7 is the fact that the metric $\widehat{d}$ is not dependent on the choice of representative for each equivalence class of Cauchy sequences [Kat07, Ex. 18].

The set M lives naturally inside $\widehat{M}$. Formally, we can define the map

$$f : M \to \widehat{M}$$

which sends any element x in M to the constant sequence $(x, x, x, x, ...)$. Thinking of M as existing inside of $\widehat{M}$ in this way, M is dense in $\widehat{M}$.

This process of completion can be applied to $\mathbb{Q}$ to obtain $\mathbb{R}$ by using the standard Euclidean metric. For example, the Cauchy sequence $(3, 3.1, 3.14, 3.141, 3.1415, 3.14159, \dots)$ has no limit in the rationals. However, it is a representative for the equivalence class of Cauchy sequences of rational numbers which we can identify with the real number π.

Note that a complete metric space is equal to its completion [Kat07, Prop1.3].

2.8. **Completion of Fields.** Completion often respects arithmetic operations such as addition and multiplication, but in order to formalize this we must define a normed field.

Definition 2.9. [Kob84] A *Normed Field* is a field X equipped with a notion of size, or *norm*, i.e. there exists a map from X to $\mathbb{R}$, $x \to \|x\|$, such that:

(1) $\|x\| \geq 0$ for all $x \in X$
(2) $\|x\| = 0$ if and only if $x = 0$
(3) $\|xy\| = \|x\|\|y\|$ for all $x, y \in X$
(4) $\|x + y\| \leq \|x\| + \|y\|$ for all $x, y \in X$

Example 2.10. The field $\mathbb{Q}$ has the familiar Euclidean norm which is just the absolute value: $\|x\| = |x|$

Proposition 2.11. Normed fields have an induced metric structure: $d(x, y) = \|x - y\|$.

Proof. To verify that $d(x, y)$ is indeed a metric, we simply need to verify the properties in Definition 2.2. Take $x, y, z \in X$. Then:

(1) $d(x, y) = \|x - y\| \geq 0$.
(2) $d(x, y) = \|x - y\| = 0$ if and only if $x - y = 0 \iff x = y$.
(3) $d(x, y) = \|x - y\| = \| - (y - x)\| = \| - 1\|\|y - x\| = \|y - x\| = d(y, x)$.
(4) $d(x, y) = \|x - y\| = \|(x - z) + (z - y)\| \leq \|x - z\| + \|z - y\| = d(x, z) + d(z, y)$.

□

Example 2.12. Using the Euclidean norm on $\mathbb{Q}$, we obtain the induced metric $d(x, y) = |x - y|$. This is the usual Euclidean distance.

Proposition 2.13. [Kat07, Thm 1.19] Let M be a normed field, and consider M as a metric space with the induced metric $d(x, y) = \|x - y\|$. Then the completion $\widehat{M}$ is also a field.

Proof. The elements of $\widehat{M}$ can be represented by Cauchy sequences, so for any $(a_n), (b_n) \in \widehat{M}$, we can define component wise addition and multiplication:

$$((a_n) + (b_n)) = (a_n + b_n) \text{ and } ((a_n) \cdot (b_n)) = (a_n \cdot b_n).$$

These operations can be checked to be independent of the choice of representatives. The completion $\widehat{M}$ forms a commutative ring under these operations with the additive identity $0 = (0, 0, 0, \dots)$ and multiplicative identity $1 = (1, 1, 1, \dots)$. To prove $\widehat{M}$ is a field, we need to find an inverse for any non-zero Cauchy sequence $(a_n) \in \widehat{M}$. Let (a_n) be any non-zero Cauchy sequence in $\widehat{M}$. Non-zero Cauchy sequence means (a_n) is not equivalent to the constant sequence $(0, 0, \dots)$, i.e. there exists integers $c, N > 0$ such that

$$\|a_n\| \ > c \ \text{ for all } n \geq N.$$

Now define the sequence $(a_n)^{-1}$ as:

$$(a_n)^{-1} = \begin{cases} 0, & \text{if } 1 \leq n \leq N - 1 \\ \frac{1}{a_n}, & \text{if } n \geq N \end{cases}$$

This sequence $(a_n)^{-1}$ is indeed Cauchy: Take $\epsilon > 0$ and $n, m \geq N$, then

$$\|a_n^{-1} - a_m^{-1}\| = \|\frac{1}{a_n} - \frac{1}{a_m}\| = \frac{\|a_m - a_n\|}{\|a_m\| \cdot \|a_n\|} \leq c^{-2}\|a_m - a_n\| < c^{-2} \cdot \epsilon$$

because (a_n) is Cauchy.

Furthermore, the product of the Cauchy sequences (a_n) and $(a_n)^{-1}$ is:

$$(a_n)(a_n)^{-1} = \begin{cases} 0, & \text{if } 1 \leq n \leq N-1 \\ 1, & \text{if } n \geq N \end{cases}$$

which is equivalent to the constant Cauchy sequence $(1, 1, 1, ...)$, the multiplicative identity. □

As an example, because $\mathbb{Q}$ is a normed field, the completion of $\mathbb{Q}$ with the Euclidean metric, namely $\mathbb{R}$, is a field as well.

But there are many different ways to think about the distance between two numbers which give rise to whole new number systems, with similar algebraic properties.

3. Construction of the p-adic numbers

The most natural way we, as humans, define the distance between two numbers is the Euclidean metric $d(x, y) = |x - y|$ as it corresponds to the distance between x and y on the real number line. As we have seen, we can use this metric to complete $\mathbb{Q}$ into the field of real numbers $\mathbb{R}$. But what if we define a different way to describe the distance between two rational numbers?

Definition 3.1. Let p be prime, $x \in \mathbb{Q}$.

$$val_p(x) = \begin{cases} \text{highest power of p which divides x}, & x \in \mathbb{Z} \\ val_p(a) - val_p(b), & x = \frac{a}{b} \end{cases}$$

The p-adic valuation of 0 is defined to be ∞.

Proposition 3.2. $val_p(xy) = val_p(x) + val_p(y)$ for all $x, y \in \mathbb{Q}$

Proof. Without loss of generality we can assume $x, y \neq 0$ so their p-adic valuations are finite. Let $val_p(x) = n$ and $val_p(y) = m$ so we can write $x = \frac{a}{b} \cdot p^n$ and $y = \frac{c}{d} \cdot p^m$ where p does not divide a, b, c, or d, and $m, n \in \mathbb{Z}$. Then $xy = \frac{ac}{cb} \cdot p^{n+m}$ hence $val_p(xy) = n + m = val_p(x) + val_p(y)$. □

This p-adic valuation allows us to define the following norm on the rationals:

Definition 3.3. The p-adic norm on $\mathbb{Q}$ is

$$|x|_p = \begin{cases} \frac{1}{p^{val_p(x)}}, & x \neq 0 \\ 0, & x = 0. \end{cases}$$

One can verify that $|x|_p$ is indeed a norm:

(1) Positive definite follows directly from the definition of the p-adic norm.
(2) $|x \cdot y|_p = \frac{1}{p^{val_p(xy)}} = \frac{1}{p^{val_p(x)+val_p(y)}} = \frac{1}{p^{val_p(x)}} \cdot \frac{1}{p^{val_p(y)}} = |x|_p \cdot |y|_p$
(3) Triangle inequality: without loss of generality, we can assume $x, y \neq 0$. Let

$$x = \frac{p^n \cdot a}{b} \text{ and } y = \frac{p^m \cdot c}{d}$$

where $p \not| a, b, c, d$. We will assume $0 \leq m \leq n$ because if $n, m < 0$ we can multiply x and y by sufficiently large power of p to obtain x', y' such that their exponents are positive, from which the same argument will hold because the norm is multiplicative. Now:

$$x + y = \frac{p^m(ad + bcp^{n-m})}{bd}$$

Hence:

$$|x + y|_p \leq \frac{1}{p^m} = max(\frac{1}{p^m}, \frac{1}{p^n}) = max(|x|_p, |y)_p) \leq |x|_p + |y|_p$$

By Proposition 2.11, this norm induces the following metric on $\mathbb{Q}$:

$$d_p(x, y) = |x - y|_p \text{ for all } x, y \in \mathbb{Q}.$$

Remark 3.4. Since we showed that $|x + y|_p \leq max(|x|_p, |y|_p)$, the p-adic norm satisfies the strong triangle inequality, making it a *non-Archimedean norm.* [Gou20, Def 2.1.1].

From now on we will let p be a fixed prime. Our goal is to complete $\mathbb{Q}$ with respect to the p-adic metric.

Example 3.5. Let $(a_n) = (\sum_{k=1}^{n} p^k)$ be the sequence of rational numbers:

$$(p, \ p + p^2, \ p + p^2 + p^3, \ p + p^2 + p^3 + p^4, \ \dots)$$

Using the p-adic metric we can verify that (a_n) is in fact Cauchy. Assuming $n > m$ we have:

$$\begin{aligned} d(a_n, a_m) = & \ |p^{m+1} + p^{m+2} + \cdots + p^n|_p \\ = & \ |p^{m+1}(1 + p + p^2 + \cdots + p^{n-m-1})|_p \\ = & \ \frac{1}{p^{m+1}} \to 0 \text{ as } m \to \infty. \end{aligned}$$

Clearly, with the Euclidean metric, the sequence in Example 3.5 is not Cauchy because it does not converge. However, with the p-adic metric, the sequence (a_n) *is* Cauchy.

Similarly to how we constructed $\mathbb{R}$ from $\mathbb{Q}$ by completing the field $\mathbb{Q}$ with respect to the Euclidean metric, we can now define a *p-adic number* to be an equivalence class of Cauchy sequences under the p-adic metric.

Definition 3.6. The set of all equivalence classes of Cauchy sequences under the p-adic norm is called the *field of p-adic numbers.* Equivalently, the field of p-adic numbers is the completion of the normed field $\mathbb{Q}$ using the p-adic norm.

We can extend the p-adic norm $|\alpha|_p$ defined in Definition 3.3 for any $\alpha \in \mathbb{Q}_p$ to be:

$$|\alpha|_p = \lim_{n\to\infty} |a_n|_p$$

where (a_n) is a Cauchy sequence of rationals representing α.

Likewise, the p-adic metric on $\mathbb{Q}$ extends to $\mathbb{Q}_p$ as in Definition 2.7.

Note that the range of $|\alpha|_p$ is the discrete subset $\{p^n, n \in \mathbb{Z}\} \cup \{0\} \subseteq \mathbb{Q}$. Contrast this with the Euclidean norm on $\mathbb{Q}$ which took on values in $\mathbb{Q}$, and the Euclidean norm on $\mathbb{R}$ which took on all non-negative values in $\mathbb{R}$.

The p-adic numbers are complete in the following sense: every Cauchy sequence (using the p-adic metric of course) converges to a point inside $\mathbb{Q}_p$. Hence our sequence (a_n) from Example 3.5 is a representative for the equivalence class of Cauchy sequences representing the p-adic number: $\sum_{k=1}^{\infty} p^k$. However this number is not rational, hence $\mathbb{Q}$ is *not* complete with respect to the p-adic metric.

3.7. p-adic Integers.

Definition 3.8. [Kob84, p13] We define a *p-adic integer* to be an element α of $\mathbb{Q}_p$ such that $|\alpha|_p \leq 1$.

We denote the set of all p-adic integers by $\mathbb{Z}_p$. Just as the integers $\mathbb{Z}$ are a sub-ring of $\mathbb{Q}$, the p-adic integers $\mathbb{Z}_p$ are a sub-ring of $\mathbb{Q}_p$. Indeed, we already know $\mathbb{Z}_p$ is a subset of the field $\mathbb{Q}_p$, so it suffices to verify that $\mathbb{Z}_p$ is closed under addition and multiplication. This can be done using the properties of a norm. [Kob84, p13].

Remark 3.9. The units in $\mathbb{Z}_p$ are all $u \in \mathbb{Z}_p$ such that $|u|_p = 1$, i.e. $val_p(u) = 0$. This follows from the multiplicative property of norms:

$$|u|_p \cdot |\frac{1}{u}|_p = |u \cdot \frac{1}{u}|_p = |1|_p = 1,$$

So the inverse of u lies in $\mathbb{Z}_p$.

Recall that the definition of a p-adic number is actually an *equivalence class* of Cauchy sequences of rationals. This means that many different sequences can be used to represent the same p-adic number! To make things easier for notation, let us define a *canonical p-adic expansion* for any p-adic number α.

Theorem 3.10. [Kat07, Thm 1.30] Let α be a p-adic integer. Then there exists exactly one representative Cauchy sequence (a_n) such that for $n = 1, 2, ...$:

(1) $a_n \in \mathbb{Z}$ for $0 \leq a_n < p^n$
(2) $a_n \equiv a_{n+1} \pmod{p^n}$

Using Theorem 3.10 we can see that a p-adic integer can also be defined as follows:

Definition 3.11. [Lan02, p51] A p-adic integer can be defined as a sequence of residues:

$$a_1 \mod p, \quad a_2 \mod p^2, \quad a_3 \mod p^3, \quad \ldots$$

with each a_n congruent to its predecessor mod p^{n-1}. (Equivalently, each a_n maps to a_{n-1} under the natural quotient maps $\mathbb{Z}/(p^{n+1}) \to \mathbb{Z}/(p^n)$.)

Indeed: condition (1) in Theorem 3.10 guarantees that when we choose the residue class representative in Definition 3.11, we can always pick the unique representative between 0 and $p^n - 1$ to obtain the *unique* Cauchy sequence of integers (the so-called *canonical* representation of α). Condition (2) ensures each a_{n+1} maps to a_n as needed.

Example 3.12. Consider the sequence of integers beginning with

$$(3, 10, 108, \dots).$$

This sequences represents the first 3 terms of the canonical representative for some equivalence class of Cauchy sequences in $\mathbb{Z}_7$ because it satisfies conditions (1) and (2) in Theorem 3.10. Therefore it represents a 7-adic integer α. Using the notation in Definition 3.11,

$$\alpha = (3 \mod 7,\ \ 10 \mod 7^2,\ \ 108 \mod 7^3, \dots).$$

Similarly, the sequence $(4, 39, 235, \dots)$ is the canonical representative of a 7-adic integer:

$$\beta = (4 \mod 7,\ \ 39 \mod 7^2,\ \ 235 \mod 7^3,\ \ \dots).$$

Using the ring structure on $\mathbb{Z}_7$, we can add $\alpha + \beta$ to obtain another 7-adic integer:

$$(7 \mod 7,\ \ 49 \mod 7^2,\ \ 343 \mod 7^3,\ \ \dots)$$

which has the canonical Cauchy sequence $(0, 0, 0, \dots)$, the zero element of $\mathbb{Z}_7$. Hence, α and β are in fact additive inverses in $\mathbb{Z}_7$!

3.13. **Canonical Representation of a p-adic Number.** Now we have the tools to represent any p-adic integer using a canonical base p expansion.

For any p-adic integer, Theorem 3.10 says there exists a unique Cauchy sequence $(a_n) = (a_1, a_2, a_3, \dots)$ representing α and such that conditions (1) and (2) hold. More conveniently, we can write each term $a_n \in \mathbb{Z}$ using base p expansion:

$$a_n = d_0 + d_1 p + \cdots + d_{n-1} p^{n-1}$$

where each $d_n \in \{0, 1, 2, \dots, p-1\} \subseteq \mathbb{Z}$ are called the *p-adic digits.* Since $a_{n+1} \equiv a_n \pmod{p^n}$, we have that

$$a_{n+1} = d_0 + d_1 p + \cdots + d_{n-1} p^{n-1} + d_n p^n$$

with the same p-adic digits d_0 through d_{n-1} as for a_n. Hence

$$\alpha = \sum_{n=0}^{\infty} d_n p^n \tag{1}$$

where each d_n are the p-adic digits of α. The sequence of partial sums

$$(d_0,\ \ d_0 + d_1 p,\ \ d_0 + d_1 p + d_2 p^2,\ \ d_0 + d_1 p + d_2 p^2 + d_3 p^4,\ \ \dots)$$

is the canonical Cauchy sequence representing α guaranteed by Theorem 3.10. Because $\mathbb{Q}_p$ is complete, it converges to the p-adic number α. If the digits d_i are chosen between 0 and $p - 1$, then this expression is unique.

Example 3.14. The canonical representation of the multiplicative identity $1 \in \mathbb{Q}_p$ is:

$$(1, 1 + 0p, 1 + 0p + 0p^2, \dots).$$

Remark 3.15. We can uniquely write any p-adic number $\alpha = u \cdot p^m$ where u is a p-adic unit (See remark 3.9) and $m \in \mathbb{Z}$. Now, $|\alpha|_p = 1/p^m$.

Borrowing notation from the decimal expansions of real numbers, we can write any p-adic integer in base p with digits extending infinitely far to the left:

$$\alpha = [\dots d_n \dots d_3 d_2 d_1 d_0.]_p$$

In this notation, each d_n is the same p-adic digit as in the canonical sequence representation (equation 1) of α.

There are two cases to consider when trying to write down some $\alpha \in \mathbb{Q}_p$ as a "p-adic decimal" expansion: $|\alpha|_p \leq 1$ and $|\alpha|_p > 1$. The first case is when α is a p-adic integer, handled by Theorem 3.10. For α that are not p-adic integers, we need the following trick:

Remark 3.16. If $\alpha \in \mathbb{Q}_p$ such that α is a p-adic integer, i.e. $\alpha = \sum_{n=0}^{\infty} d_n p^n = [\dots d_2 d_1 d_0]_p$, then multiplying α by p^m will move the decimal point m digits to the right because:

$$\begin{aligned}\alpha \cdot p^m &= \sum_{n=0}^{\infty} d_n p^{n+m} \\ &= 0 + 0 \cdot p + 0 \cdot p^2 + \dots + d_0 \cdot p^m + d_1 \cdot p^{m+1} + d_2 \cdot p^{m+2} + \dots \\ &= [\dots d_2 d_1 d_0 0 \dots 0]_p.\end{aligned}$$

Hence we can reduce to the case where α is a p-adic integer by multiplying α by an appropriate power p^m. Now we can write:

$$\alpha = \dots d_n \dots d_2 d_1 d_0 . d_{-1} \dots d_{-m}$$

as a fraction in base p with infinitely many p-adic digits to the left and finitely many (m) digits to the right ($d_{-m} \neq 0$).

Remark 3.17. If the canonical expansion of α contains digits only to the left of the point (i.e. only non-negative powers of p), then α is a p-adic integer.

Example 3.18. Take $79 \in \mathbb{Z}_3 \subseteq \mathbb{Q}_3$. Using Definition 3.11,

$$79 = (1 \mod 3, \quad 7 \mod 9, \quad 25 \mod 29, \quad 79 \mod 81, \quad 79 \mod 243, \dots).$$

Using the canonical expansion as in Theorem 3.10,

$$79 = (1, 1 + 2 \cdot 3, 1 + 2 \cdot 3 + 2 \cdot 3^2, 1 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3, \dots) = [\dots 02221]_3$$

.

Example 3.19. Now take $\frac{79}{3} \in \mathbb{Q}_3$.

$$\frac{79}{3} = 1 \cdot 3^{-1} + 2 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2 + 0 \cdot 3^3 + \dots = [\dots 0222.1]_3$$

Notice how the decimal moved one place over to the left.

4. Comparison of $\mathbb{R}$ and the p-adics

4.1. **Decimal Expansion.** Any p-adic number $\alpha \in \mathbb{Q}_p$ can be represented as the infinite power series

$$\alpha = \sum_{n=-m}^{\infty} d_n p^n$$

where $d\_m \neq 0$ and each $d_n \in \{0, 1, ..., p-1\} \subseteq \mathbb{Z}$ represents the infinite p-adic digits of the α when written in base p. This infinite power series converges (in the p-adic sense) to

$$\alpha = [\ldots d_2 d_1 d_0 . d_{-1} \ldots d_{-m}]_p$$

. Similarly, any real number can be represented as an infinite power series of 1/10. Take any real $r \in [0, 1]$ so we can write $r = 0.a_1 a_2 a_3 a_4 \ldots$ where each $a_i \in \{0, 1, ..., 9\}$. The infinite power series

$$\sum_{n=1}^{\infty} \frac{a_n}{10^n}$$

converges (using the Euclidean metric on $\mathbb{Q}$) to the real number $r = 0.a_1 a_2 a_3 a_4 \ldots$

However, note that we do not obtain uniqueness in the reals when using infinite decimal expansion. For example:

$$1.0000 \cdots = 0.999 \ldots$$

4.2. **Recognizing Rational Numbers.** Both the set of rational numbers and the set of integers exist naturally inside $\mathbb{Q}_p$.

Proposition 4.3. If non-negative $a \in \mathbb{Q}$ has denominator a power of p, then the p-adic decimal expansion of a terminates.

Proof. If $a \in \mathbb{Z}$, then the denominator has a power $p^0 = 1$. Hence, Definition 3.11 gives us that any $a \in \mathbb{Z}$ can be represented with the Cauchy sequence of integers $(a_n) = (a \bmod p^n) = (a \bmod p,\ a \bmod p^2,\ \ldots,\ a \bmod p^n,\ \ldots)$. This Cauchy sequence representing the integer $a \in \mathbb{Z}$ will eventually look like $(\ldots, a,\ a,\ a, \ldots)$ as soon as $p^n > a$. So for large enough n, this sequence will become constant. Writing a in the base p expansion, eventually the p-adic digit $d_n = 0$ for all n. Dividing a by a power of p^m gives us the rational number $\frac{a}{p^m}$. Since the decimal expansion of a eventually terminates, and dividing by p^m only moves the decimal place over m digits (Remark 3.16), then the p-adic expansion of the rational $\frac{a}{p^m}$ will also terminate (see Example 3.19). □

Hence, one can recognize a real integer (i.e. an element of $\mathbb{Z}$) among the p-adic integers by a finite number of p-adic digits and only 0s to the right of the decimal (see example 3.18).

To recognize a real rational (i.e. an element of $\mathbb{Q}$) among $\mathbb{Q}_p$ whose denominator is *not* a power of p, we have the following theorem:

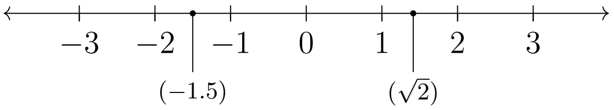
Theorem 4.4. [Kat07, Thm 1.38] The canonical p-adic expansion represents a rational number if and only if it is eventually periodic to the left.

Example 4.5. Take $1/2 \in \mathbb{Q}_3$. To find the canonical sequence of a_n's as defined in Theorem 3.10, each a_n should be something mod 3^n that after doubling it is $1 + 3^n$: $(2, 5, 14, 41, 122, \ldots)$. Writing in 3-adic decimal expansion, we can see that it is eventually periodic:

$$\frac{1}{2} = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \cdots = [\ldots 1112]_3$$

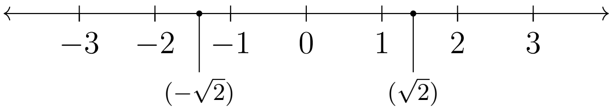
Now we have the tools to recognize when the canonical p-adic expansion of a number represents a real integer or rational! Compare this to the real numbers where we can recognize an integer by the infinite 0s to the right of their decimal point in their decimal expansion or a rational by its eventually periodic decimal expansion.

4.6. **A Geometric Comparison.** The real numbers can neatly be represented on a number line. For example, the real numbers $\sqrt{2}$ and -1.5 can be plotted on the following number line:



and the distance, $d(-1.5, \sqrt{2}) = |-1.5 - \sqrt{2}|$, between them is simply their Euclidean distance on this line. Two points which are physically close on the line are close in terms of their Euclidean metric. Additionally, solutions to any equation can be plotted on the number line, so long as the equation has real solutions.

Example 4.7. The solutions to the equation: $x^2 = 2$ can be plotted:



However, this neat visual representation breaks down when we try to plot p-adic numbers on a number line. For example, 84 and 3 are quite far away in terms of their Euclidean metric, while p-adically: $|84 - 3|_3 = 1/3^4$. Quite small!

Another example: both $|27|_3$ and $|108|_3$ have the same value: $1/3^3$. However they lie at different points on the real number line.

How can we construct a tool to visualize the p-adic numbers (for some fixed p) and the distances between them? Can we use it to plot p-adic solutions to equations? Yes!

By the definition of p-adic integer, we can see that the set of all p-adic integers

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

forms a closed disc of radius one in the metric space $\mathbb{Q}_p$ (with the p-adic metric of course). This is very different from the set of integers in $\mathbb{R}$ which are evenly spaced throughout the real number line, instead of clustered in a disc near the origin!

More generally, we can study open or closed balls in the metric space $\mathbb{Q}_p$. Let us define the *open p-adic disc* centered at $\alpha \in \mathbb{Q}_p$ of radius p^{-n} to be the open set:

$$B(\alpha, \frac{1}{p^n}) = \{x \in \mathbb{Q}_p \mid d(x, \alpha) < \frac{1}{p^n}\}.$$

The *closed p-adic disc* is its closure:

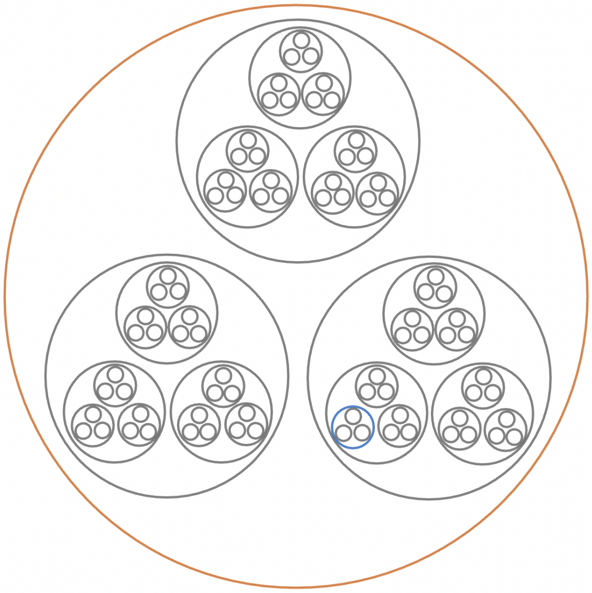
$$\overline{B}(\alpha, \frac{1}{p^n}) = \{x \in \mathbb{Q}_p \mid d(x, \alpha) \leq \frac{1}{p^n}\}.$$

The p-adic numbers have the following amazing property, which allows us to create a totally different topological structure to visualize them!

Theorem 4.8. [Gou20, Thm 2.3.6(v)] Any two open p-adic discs are either disjoint or one is contained entirely in the other.

This is very different from $\mathbb{R}$. For example, the open balls $B(0,1)$ and $B(\frac{1}{2},1)$ are the overlapping intervals $(-1,1) \cap (-\frac{1}{2},\frac{3}{2}) = (-\frac{1}{2},1)$.

Let's see how these discs look in $\mathbb{Q}_3$. I created the following image with the software GeoGebra:



The disc bounded by the orange circle represents the closed ball $\overline{B}(0,1)$. Everything inside this disc is a p-adic integer, that is, these numbers have no (non-zero) digits to the right of the decimal. Notice that inside $\overline{B}(0,1)$, there are three new discs — balls of radius 1/3 — each completely contained inside $\overline{B}(0,1)$ but disjoint from each other. These discs are centered at the p-adic integers $[0.]_3, [1.]_3$, and $[2.]_3$, respectively. The disc closest to the top represents all integers with a 0 as its d_0 digit, then moving clockwise for digits $d_0 = 1$ or $d_0 = 2$. Continuing in this fashion, there are three new discs inside each previous disc, of radius $1/3^n$ for increasing n. As an example, the disc bounded by the blue circle above represents the closed ball of all 3-adic numbers:

$$\overline{B}([221.0]_3, \frac{1}{27})$$

Everything in this ball shares the first several 3-adic digits:

$$[\ldots 221.0]_3$$

The pattern replicates forever to create a fractal-like pattern covering $\mathbb{Z}_3$ (since we began with the disc bounded by the orange circle $\overline{B}(0,1)$). If we were to zoom out, we'd see that $\overline{B}(0,1)$ is simply the top-most circle inside the disc of 3-adic numbers which all share the common digit $d_{-1} = 0$.

If we continue the process forever, any p-adic number will be contained in a sequence of discs with ever-shrinking radius, as a limit. To visualize when two p-adic numbers are close to one another, instead of observing their Euclidean distance on a real number line, we note how many discs they share in common!

5. Finding p-adic roots

Some equations such as $f(x) = x^2 - 2 = 0$ have no rational solutions. However, the real completion of $\mathbb{Q}$ does have solutions to this equation, namely $x = \sqrt{2}$. Do p-adic solutions exist as well, for some fixed prime p? I.e. is there a p-adic number with digits $d_i \in \{0, 1, ..., p-1\}$ such that

$$(d_0 + d_1 \cdot p + d_2 \cdot p^2 + ...)^2 = 2 + 0 \cdot 5 + 0 \cdot 5^2 + ...$$

To answer this question, we must examine $f(x) \mod p$.

Example 5.1. Take $p = 7$ and let $f(x) = x^2 - 2$.

To solve this congruence mod 7, we observe that 2 is a quadratic residue mod 7, meaning there exists $a \in \mathbb{Z}$ such that $a^2 \equiv 2$ mod 7. Indeed, $f(3) = 3^2 - 2 = 9 - 2 \equiv 0$ mod 7. Does the existence of a root mod 7 guarantee a solution mod higher powers of 7? The answer is yes!

Theorem 5.2. Hensel's Lifting Lemma. Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial. For any fixed $a \in \mathbb{Z}_p$ such that $f(a) \equiv 0 \text{ mod p}$ and $f'(a) \not\equiv 0 \text{ mod p}$, there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv a$ mod p.

Proof. We will prove the following statement by induction on n:

S(n): There exists $a_n \in \mathbb{Z}_p$,

$$a_n = d_0 + d_1 p + d_2 p^2 + \cdots + d_{n-1} p^{n-1}$$

(where the d_i*s are its canonical p-adic digits) such that*

$$f(a_n) \equiv 0 \mod p^n \textit{ and } a_n \equiv a \mod p.$$

If a root $a_n \in \mathbb{Z}_p$ exists mod p^n for all n, then by taking the limit as $n \to \infty$, we will obtain the true p-adic root α such that $f(\alpha) = 0$.

The base case for $n = 1$ follows if we let $a_1 = d_0$ equal the first p-adic digit of a from the hypothesis. Thus $a_1 \equiv a$ and $f(a_1) \equiv 0 \mod p$. Now we want to show that $S(n-1)$ implies $S(n)$. Let $a_n = a_{n-1} + d_{n-1} p^{n-1}$ for some unknown p-adic digit $d_{n-1} \in \{0, 1, \ldots, p-1\}$ which we will solve for so that $f(a_n) \equiv 0 \mod p^n$. From $S(n-1)$, we know that $f(a_{n-1}) \equiv 0 \mod p^{n-1}$. Let $f(x) = \sum_{k=0}^{m} c_k x^k$ with coefficients $c_k \in \mathbb{Z}_p$. Expanding out $f(a_n)$ and using the binomial theorem we get:

$$\begin{aligned} f(a_n) &= f(a_{n-1} + d_{n-1}p^{n-1}) \\ &= \sum_{k=0}^{m} c_k(a_{n-1} + d_{n-1}p^{n-1})^k \\ &= c_0 + \sum_{k=1}^{m} c_k(a_{n-1}^k + ka_{n-1}^{k-1}d_{n-1}p^{n-1} + \text{ terms divisible by } p^n) \\ &\equiv f(a_{n-1}) + d_{n-1}p^{n-1}f'(a_{n-1}) \mod p^n \end{aligned}$$

By inductive assumption, $f(a_{n-1}) \equiv 0 \mod p^{n-1}$, so $f(a_{n-1}) = qp^{n-1}$. Hence:

$$f(a_n) \equiv qp^{n-1} + d_{n-1}p^{n-1}f'(a_{n-1}) \mod p^n$$

for some $q \in \{0, 1, \ldots, p-1\}$. This allows us to find d_{n-1} by solving:

$$q + d_{n-1}f'(a_{n-1}) \equiv 0 \mod p$$

Note $a_{n-1} \equiv a \mod p$ so $f'(a_{n-1}) \equiv f'(a) \not\equiv 0 \mod p$. Thus:

$$d_{n-1} \equiv \frac{-q}{f'(a_{n-1})} \mod p$$

will satisfy $f(a_n) \equiv qp^{n-1} + d_{n-1}p^{n-1}f'(a_{n-1}) \equiv 0 \mod p^n$. Thus we have shown $S(n)$ holds for all n. Now let $\alpha = \sum_{n=0}^{\infty} d_n p^n$. Note that $f(\alpha) = 0$ because $f(\alpha) \equiv f(a_n) \equiv 0 \mod p^n$ for all n. This proves the existence of $\alpha \in \mathbb{Z}_p$. The uniqueness follows from the uniqueness of the canonical expansion of α from Theorem 3.10. □

Hensel's lemma allows us to lift certain solutions mod p to a p-adic solution, meaning we have a solution to the congruence $f(x) \equiv 0$ mod p^n for all n. Continuing Example 5.1, we can see that the 7-adic integer:

$$3 = [3]_7 = 3 + 0p + 0p^2 + \ldots$$

satisfies the conditions of Hensel's Lemma. Indeed: $f(3) \equiv 0 \mod 7$ and $f'(3) = 2 \cdot 3 \not\equiv 0$ mod 7. Therefore, we can uniquely lift this solution to obtain the 7-adic solution:

$$\alpha = 3 + 1 \cdot 7 + 2 \cdot 7^2 + \cdots = [...213]_7$$

Let's illustrate how we computed this solution by using the p-adic version of Newton's Method outlined in the induction proof of Theorem 5.2 to find each next element of the p-adic sequence. If a_n is a solution to the congruence $f(x) \equiv 0$ mod p^n then

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} \mod p^{n+1}$$

is a solution mod p^{n+1}.

We start by letting $a_1 = 3$ because $f(3) \equiv 0 \mod 7$. To find a_2 we compute:

$$3 - \frac{f(3)}{f'(3)} = 3 - \frac{9}{6} \mod 7^2.$$

Since $\frac{9}{6}$ mod 7^2 is congruent to -7 (because 9 and -42 lie in the same congruence class mod 49), we get that $a_2 = 3 - (-7) = 10$.

Then:

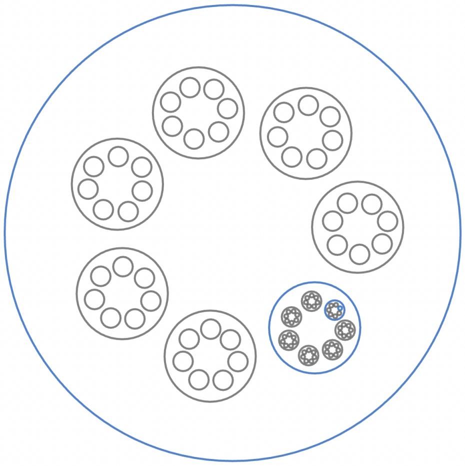
$$a_3 = 10 - \frac{f(10)}{f'(10)} = 10 - \frac{98}{20} \mod 7^3$$

Since $98 \equiv -1960 \mod 343$, we get that $10 - \frac{98}{20} \equiv 10 - (-98) \equiv 108 \mod 343$ so $a_3 = 108$. So the Cauchy sequence begins $(3, 10, 108, \dots)$, which if we write each element in base 7 we get: $(3, 3 + 1 \cdot 7, 3 + 1 \cdot 7 + 2 \cdot 49, \dots) = [\dots 213]_7 = \alpha$.

Computing these 7-adic roots by hand as shown above is quite tedious, so I wrote a python script to compute them for me; see appendix A. It takes integers a, p, and d as inputs to compute the first d digits of the square root of a in the the p-adics. From this code we easily compute the first 10 digits to be:

$$\alpha = [\dots 6421216213]_7$$

Using the discs as mentioned in section 4.6, we can graph this solution as such:



Each 7-adic digit of α determines the infinite sequence of nested discs containing α. For each layer n, the disc closest to the top represents all 7-adic numbers with $d_n = 0$ then going clockwise, $d_n = 1, 2, \dots 6$. Because α is a 7-adic integer, it lies in the disc of radius 1 (that is, $\mathbb{Z}_7$), represented by the largest disc. Then, because $d_0 = 3$, α lies in the 3rd disc, shown in blue, then $d_1 = 1$ so α lies in the 2nd disc, and so on. Continuing infinitely, we see how α lies in a series of nested discs.

Notice that $f(x) \mod 7$ has two square roots. In addition to 3, we also have $f(4) \equiv 0 \mod 7$, which we can lift to obtain:

$$\beta = [\dots 0245450454]$$

again computed using my python script. Notice how $\beta = -\alpha$ (see Example 3.12).

Notice how $f(x) = x^2 - 2$ has no rational solutions, yet we are able to find both a real solutions $(\pm\sqrt{2})$ and 7-adic solution ($\alpha = [...213]_7 = -\beta$). What if no real solution exists?

Is it still possible to find a p-adic solution for some prime p? Let's observe the following example:

Example 5.3. Let $f(x) = x^2 + 1$.

First, let's try to find a 3-adic root. To do so, we need to solve the following congruence:

$$x^2 = -1 \equiv 2 \mod 3.$$

However, notice that $0^2 \equiv 0 \mod 3, 1^2 \equiv 1 \mod 3$, and $2^2 \equiv 1 \mod 3$. We have exhausted all the possible congruence classes modulo 3, hence there is no solution to the congruence modulo 3. Thus it is impossible to find a 3-adic solution to Example 5.3.

Can we find a solution in the 5-adics instead?

$$f(x) \equiv x^2 - 4 \mod 5$$

Thus we obtain the solution $f(2) \equiv 0 \mod 5$. Since $f'(2) \not\equiv 0 \mod 5$, we can applying Theorem 5.2 and obtain a unique 5-adic root of $f(x)$. Using my python script, I compute the first 7 digits of the 5-adic solutions to be:

$$\alpha = [\dots 2431212]_5 \quad \text{and} \quad \beta = [\dots 2013233]_5$$

We can begin to verify that these are the solutions by computing whether a partial sum up to digit d_3 is a solution mod 5^3:

$$(2 + 1 \cdot 5^1 + 2 \cdot 5^2 + 1 \cdot 5^3)^2 = 33124 \equiv -1 \mod 5^3$$

and

$$(3 + 3 \cdot 5^1 + 2 \cdot 5^2 + 3 \cdot 5^3)^2 = 196249 \equiv -1 \mod 5^3.$$

Why does there exist a 5-adic solution, but not a 3-adic solution? We can use this neat trick to easily figure out when a p-adic root exists:

Corollary 5.4. Let $f(x) = x^2 - a \in \mathbb{Z}[x]$ and p be an odd prime such that p does not divide a. Then there exists a p-adic root if and only if a is a quadratic residue mod p.

Proof. If a is a quadratic residue mod p then we can solve the congruence $x^2 \equiv a \mod p$. Since $p \neq 2$, then $f'(a) = 2a \not\equiv 0 \mod p$ hence a root exists by Theorem 5.2. If there exists a p-adic root, then there exists a solution mod p^n for each n, so in particular, there exists a solution mod p. □

My Python script could easily be adapted to solve any equations satisfying the hypotheses of Hensel's Lemma. If these conditions fail to hold, it could be further adapted to deploy stronger theorems such as the following:

Theorem 5.5. [Kob84, p19] Let $f(x) \in \mathbb{Z}_p[x]$. If $a \in \mathbb{Z}_p$ satisfies $f(a) \equiv 0 \mod p^{2d+1}$ and $f'(a) \equiv 0 \mod p^d$, but $f'(a) \not\equiv 0 \mod p^{d+1}$, then there is a unique solution $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv a \mod p^{d+1}$.

6. Conclusion

A natural question which arises now is: can we define even more exotic norms beyond the Euclidean and p-adic norms to complete $\mathbb{Q}$? In short, no: the Euclidean and p-adic norms are the only non-trivial norms on $\mathbb{Q}$, meaning $\mathbb{R}$ and $\mathbb{Q}_p$ are the *only* ways to complete $\mathbb{Q}$ in which we obtain a complete metric space that is also a field [Gou20, Ostrowski]. Concepts such as limits, convergence, continuity, and differentiation which all depend on the norm on a complete metric space can be studied both in $\mathbb{R}$ and the p-adics.

The same way Pythagorus questioned the existence of irrationals, one might question, do these exotic p-adic numbers really exist? In this paper we saw by shifting the way we think of the distance between numbers that in fact they do! And if I had been around in 470 B.C., the mere writing of this paper would have probably had me drowned as well!

Acknowledgements. Thanks my MOC house friends for keeping me sane while struggling with Python code, to Karen Smith for help with latex (especially bibtex), and to Professor Jonathan Love for introducing me to p-adic numbers!

References

[Ang94] W. S. Anglin, *Mathematics: a concise history and philosophy*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1994, Readings in Mathematics. MR 1301327

[Gou20] Fernando Q. Gouvêa, *p-adic numbers*, Universitext, Springer, Cham, [2020] ©2020, An introduction, Third edition of [1251959]. MR 4175370

[Kat07] Svetlana Katok, *p-adic analysis compared with real*, Student Mathematical Library, vol. 37, American Mathematical Society, Providence, RI; Mathematics Advanced Study Semesters, University Park, PA, 2007. MR 2298943

[Kob84] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR 754003

[Lan02] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR 1878556

[oA30] Pappus of Alexandria, *The commentary of pappus on book x of euclid's elements*, Cambridge, Harvard university press, 1930, Arabic text and translation by William Thomson, with introductory remarks, notes, and glossary of technical terms by Gustav Junge and William Thomson.

[Rud76] Walter Rudin, *Principles of mathematical analysis*, third ed., International Series in Pure and Applied Mathematics, McGraw-Hill Book Co., New York-Auckland-Düsseldorf, 1976. MR 0385023

Appendix A. Python Code

You can find my code on my GitHub (`https://github.com/helenaheinonen/math377`).