A very brief look at p-adic Numbers

Stuyvesant Senior Math Team

Aditya Pahuja

Taught in March 2024

Contents

1 Introduction

1.1 Hensel's analogy

The creation of the p-adic numbers is attributed to German mathematician Kurt Hensel. Hensel was exploring a problem about algebraic numbers (i.e. numbers expressible as a root of a complex polynomial, like $\sqrt{2}+\sqrt[3]{2}$), which, when thought of as a problem about algebraic functions (i.e. functions expressible as a root of a complex polynomial, like $\sqrt{X^3-3X+1}$), became easy to solve because he could express algebraic functions as power series.

In particular, given a polynomial $P(X)$ in the ring of complex polynomials $\mathbb{C}[X]$ and some $\alpha \in \mathbb{C}$, we know by the Taylor formula that

$$P(X) = a_0 + a_1(X-\alpha) + a_2(X-\alpha)^2 + \cdots + a_n(X-\alpha)^n$$

for some complex numbers a_i (to find the a_i, pick a_n, then a_{n-1}, then a_{n-2}, and so on to match coefficients); this gives us information on how $P(x)$ behaves near α.

Back in the land of integers, it turns out that we have a very similar thing happening. Where $X-\alpha$ appeared above, we can consider prime numbers p (why are the $X-\alpha$ related to prime numbers?), which means that each integer ("polynomial") can be expressed as

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k,$$

which gives us information about how n behaves "near p" (more precisely, "mod p^i for all i").

However, we can push the complex polynomial thinking further by thinking about rational functions in general: for example, the expansion

$$\frac{X^2+X}{X-1} = 2(X-1)^{-1} + 3 + (X-1)$$

with $\alpha = 1$ still gives us information near α, and in this vein, each rational function can be locally expressed as a power series at any point that looks like

$$\sum_{k \geq n_0} a_k (X-\alpha)^k.$$

(The technical term for this is a "finite-tailed Laurent series," and the set of such series centered around α is denoted $C((X-\alpha))$.) We can refine this a bit by thinking of these expansions as "formal power series" — that is, they are just carriers of coefficients rather than functions, so that we can avoid worries of convergence.

In a similar vein, we can do this with $\mathbb{Q}$; given a prime $p = 3$, for example, we can write

$$\frac{24}{17} = \frac{2p+2p^2}{2+2p+p^2} = p + p^3 + 2p^5 + p^7 + p^8 + 2p^9 + \cdots = \ldots 2110201010_3.$$

This is the canonical way to represent numbers in the **3-adic numbers**; of course, we can generalize to any prime p as we wish.

Exercise 1.1. Write out the 3-adic representations of $\frac{8}{17}$, $\frac{8}{51}$, and $-\frac{24}{17}$.

Exercise 1.2. Given the p-adic representation of some y, describe the p-adic representation of $-y$.

Of course, we already had access to all of these numbers in regular old base p, so why bother with these Laurent series in p?

Exercise 1.3 (Unimportant)**.** In fact, p-adic expansions look a lot like regular base p expansions:

- Show that the p-adic representation of a number is either finite or eventually periodic if and only if this number is rational. When is it finite?
- How does the p-adic expansion of a rational number convey information relating to divisibility by p?

One of the main points we will be using is that p-adic numbers give us information modulo every power of p, just by reading off digits from the p-adic representation (in contrast, try reading off $\frac{8}{17} \pmod{3^{12}}$ from the normal base 3 expansion!). This is a microcosm of how p-adic numbers so readily provide information "locally at p," which makes some problems very, very nice to handle (again, just like Laurent series helped Hensel with algebraic functions).

1.2 A more foundational view

The 5th-grade definition of real numbers is something like "you can smush whatever you want after the decimal point" — that is, $\mathbb{R}$ is the set of numbers expressible as

$$\sum_{k \geq n_0} a_k 10^{-k}$$

where the a_i are digits. This, while true, is incredibly unsatisfying and sheds no insight into the structure of $\mathbb{R}$. "Finite-tailed Laurent series in p" is an equally meaningless expression in that, again, we have no sense of the structure of $\mathbb{Q}_p$.

Rather, $\mathbb{R}$ can be thought of as the result of taking $\mathbb{Q}$ and "filling in the gaps" in the number line. For example, the sequence of rationals

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \cdots,$$

where the nth term is the ratio of the $(n+1)$-th and the nth Fibonacci numbers, converges to $\varphi = \frac{1+\sqrt{5}}{2}$, which is obviously irrational. Thus, the reals are often defined as a "completion" of $\mathbb{Q}$, in that every convergent sequence of reals actually converges to a real number. (Interested readers are encouraged to learn about Richard Dedekind's original construction of the real numbers — it's seriously cool stuff.)

The idea that we will spend considerable time exploring here is what happens when we perturb what it means for a sequence to converge; in particular, with just the right changes (namely, our notion of "distance"), we will give rise to the p-adic numbers.

2 Metric spaces and convergence

The topological properties of a set — that is, the properties of the set relating to continuity and convergence — are understood using the structure of **metric spaces**, which, to put it tersely, are "sets with a distance function".

To talk about distance, though, we first have to talk about size.

2.1 What does "big" mean?

In everyday life, we normally measure size with our absolute value function, which (at least in the reals) is given by

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

We will reduce this to its most important properties as follows:

Definition 2.1 — Let k be an arbitrary field[a]. Then, $|\bullet| : k \to \mathbb{R}_{\geq 0}$ is an **absolute value** on k if

(i) $|x| = 0$ if and only if $x = 0$,

(ii) $|x||y| = |xy|$, and

(iii) $|x + y| \leq |x| + |y|$

for all x, $y \in k$. Also, if $|\bullet|$ satisfies the stronger condition

$$|x + y| \leq \max(|x|, |y|)$$

in place of (iii), then it is called **non-archimedean**; otherwise, it is called **archimedean**.

[a] A field is a set endowed with commutative addition and multiplication operations in which multiplication distributes over addition. We denote the multiplicative identity with 1 and the additive identity with 0. Some examples of fields are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and the integers modulo any prime p.

A silly example of a non-archimedean absolute value is the so-called trivial one, defined by clamping every nonzero element of k to 1.

These properties will let us extend this size function into a reasonable-looking distance function later on, since property (iii), the triangle inequality, is the most important feature of distance. For now, though, let's talk about a couple of examples via a related structure:

Definition 2.2 — A **valuation** ν on a field k is a function $\nu : k \to \mathbb{R}$ such that

(i) $\nu(x) = +\infty$ if and only if $x = 0$,

(ii) $\nu(xy) = \nu(x) + \nu(y)$, and

(iii) $\nu(x + y) \geq \min(\nu(x), \nu(y))$

for all x, $y \in k$.

(Do you see the resemblance to non-archimedean absolute values?)

The valuation that the p-adic numbers are based off of is the aptly-named **p-adic valuation**:

Definition 2.3 — Let p be a prime. The p-adic valuation is defined as follows: let $\nu_p \colon \mathbb{Z}\backslash\{0\} \to \mathbb{Z}$ (that is, from nonzero integers to integers) have the property that $\nu_p(n)$ is the largest integer e satisfying $p^e \mid n$. Then, extend this to $\mathbb{Q}$ using $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$ and $\nu_p(0) = +\infty$ (why does this choice of $\nu_p(0)$ make sense?).

To be thorough, we will check that this is indeed a valuation on $\mathbb{Q}$.

- Property (i) is obviously satisfied by construction.
- Property (ii) is obvious if either number is zero, so assume otherwise. Then, any rational has a unique prime factorization (for example, $21/10 = 2^{-1}3^{1}5^{-1}7^{1}$); the exponents, of course, encode the value of $\nu_p(x)$ across all choices of p, so, by exponent properties, we get what we want.
- Property (iii) follows from factoring out the largest possible power of p. If $x = p^{\nu_p(x)} \cdot x'$ and $y = p^{\nu_p(y)} \cdot y'$ with WLOG $\nu_p(x) \le \nu_p(y)$,

  $$x + y = p^{\nu_p(x)}(x' + p^{\nu_p(y)-\nu_p(x)}y').$$

  This means that, at minimum, the sum has a $p^{\nu_p(x)}$ attached to it, so we need to show that the term in the parentheses has a nonnegative ν_p, which follows from writing x' and y' as ratios of integers and noting that, when reduced, their denominators are by definition not going to contain any powers of p, and the $p^{\nu_p(y)-\nu_p(x)}$ obviously doesn't contribute to the denominator.

As alluded to, we can directly turn this into an absolute value:

Definition 2.4 — The **p-adic absolute value** is a function $|\bullet|_p \colon \mathbb{Q} \to \mathbb{R}^+$ given by

$$|x|_p = p^{-\nu_p(x)},$$

where we interpret $p^{-\infty}$ as 0. (The choice of p as our base is in some sense arbitrary; we could have chosen any $c > 1$ so that $|x|_p = c^{-\nu_p(x)}$ and still gotten a non-archimedean absolute value.)

Exercise 2.1 (Some computational practice)**.** Compute $|35|_7$, $|56/12|_7$, $|177553|_7$, and $|3/686|_7$.

We find here that "smaller" numbers — that is, the numbers closer to 0 — are ones that are "more divisible" by p (i.e. their ν_p is large), while "larger" numbers are "less divisible" in that their ν_p is small. This should highlight how strange the geometry induced by $|\bullet|_p$ is, especially compared to the nicely behaved nature of size in $\mathbb{R}$.

2.2 The geometry of the p-adic absolute value

As you may have anticipated, given an absolute value on a field k, we can describe the distance between two elements of k by $d(x, y) = |x - y|$. Having a notion of distance now means we can do geometry!

First, some obvious properties we expect to have:

Proposition 2.5 (Absolute value properties)**.** For any x, y, and z in a field k,

(i) $d(x, y) \geq 0$, with equality if and only if $x = y$.

(ii) $d(x, y) = d(y, x)$.

(iii) $d(x, z) \leq d(x, y) + d(y, z)$ (a.k.a. the triangle inequality).

Feel free to go through the proofs of these on your own; they follow directly from the absolute value axioms.

A set endowed with such a metric d is called a **metric space**, and these structures form the foundation of real analysis and topology.

Lemma 2.6. Let k be a field with an absolute value, and let d be the induced metric. Then, the absolute value is non-archimedean if and only if, for all x, y, and $z \in k$,

$$d(x, z) \leq \max(d(x, y), d(y, z)).$$

Proof. For the forward direction (i.e. if the inequality is true), we have

$$|x + z| = d(x, -z) \leq \max(d(x, 0), d(0, -z)) = \max(|x - 0|, |0 + z|) = \max(|x|, |z|)$$

for any x and z, which is what it means for $|\bullet|$ to be archimedean.

For the backwards direction,

$$d(x, z) = |x - z| = |(x - y) + (y - z)| \leq \max(|x - y|, |y - z|) = \max(d(x, y), d(y, z)),$$

as given by the non-archimedean property. □

This is a very strong constraint, known as the **ultrametric inequality**. A metric satisfying this is an **ultrametric**, and a metric space with such a metric is called an **ultrametric space**.

Theorem 2.7. Let k be a field with a non-archimedean absolute value. Then, if $x, y \in k$ and $|x| \neq |y|$,

$$|x + y| = \max(|x|, |y|).$$

Proof. Without loss of generality, let $|x| > |y|$. Then, on one hand,

$$|x + y| \leq \max(|x|, |y|) = |x|$$

by the non-archimedean property. On the other hand,

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

where $|y| = |-y|$ because it can be shown that $|-1| = 1$. However, $|x| > |y|$, so the inequality can only hold if $\max(|x + y|, |y|) = |x + y|$. Therefore, $|x|$ is both at least and at most $|x + y|$, so it equals $|x + y|$. □

The following corollary represents how strange ultrametrics are, as it is responsible for many of the esoteric topological aspects of the p-adic absolute value.

Corollary 2.8. All "triangles" in an ultrametric space are isosceles; that is, for all x, y, $z \in k$, at least two of $d(x,y)$, $d(y,z)$, and $d(z,x)$ are equal.

2.3 Cauchy sequences and completeness

Definition 2.9 (Completeness and density) — Let k be a field with absolute value $|\bullet|$.

(i) A sequence of elements x_0, x_1, x_2, ... in k is called a **Cauchy sequence** if, for every $\varepsilon > 0$, there exists an M such that $|x_m - x_n| < \varepsilon$ whenever $m, n \geq M$. In other words, for each $\varepsilon > 0$, all but finitely many terms of the sequence can be contained in an open ball of radius ε.

(ii) We say that k is **complete** with respect to the absolute value if every Cauchy sequence of elements of k has a limit in k.

(iii) We say that $S \subseteq k$ is **dense** in k if, for every $x \in k$, we can find elements of S that is arbitrarily close to x. Symbolically, this means that given $\varepsilon > 0$, we can find $s \in S$ such that $|x - s| < \varepsilon$.

Note the analogy with the real numbers here: we mentioned earlier that $\mathbb{R}$ is a completion of $\mathbb{Q}$ (with respect to the standard absolute value, to be precise), and $\mathbb{Q}$ is dense in $\mathbb{R}$ because any two real numbers have a rational number between them. In fact, density guarantees that $\mathbb{R}$ is in some sense the smallest field containing $\mathbb{Q}$ with the completeness property because

- Completeness necessitates that any such field includes the limit of any Cauchy sequence in $\mathbb{Q}$.
- Density ensures that every element of $\mathbb{R}$ is the limit of a Cauchy sequence in $\mathbb{Q}$.

We wish to do something similar with respect to the p-adic absolute value; that is, we will establish the existence of a field $\mathbb{Q}_p$, the p-adic numbers, that is complete with respect to $|\bullet|_p$ and in which $\mathbb{Q}$ is dense.

First, let's understand Cauchy sequences under the stronger framework of a non-archimedean absolute value.

Lemma 2.10. Let k have a non-archimedean absolute value. Then, a sequence (x_n) is Cauchy if and only if

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

Proof. Let $m = n + r > n$. Then,

$$\begin{aligned} |x_m - x_n| &= |(x_{n+r} - x_{n+r-1}) + (x_{n+r-1} - x_{n+r-2}) + \cdots + (x_{n+1} - n)| \\ &\leq \max(|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \ldots, |x_{n+1} - x_n|) \end{aligned}$$

using the non-archimedean property, at which point the result follows because $|x_m - x_n|$ must approach 0 as n grows large, irrespective of the value of r. □

Recall that Lemma 3.2 is not even close to true under normal circumstances, such as the classical example of $x_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ — in other words, a sequence being Cauchy is normally a much stronger condition than this limit, so supplanting Cauchy with this new condition makes analysis much easier.

Lemma 2.11. If $\lim_{n\to\infty} |x_n| = 0$, then $\lim_{n\to\infty} x_n = 0$.

Proof. By the definition of a limit, for each $\varepsilon > 0$, there exists an $M(\varepsilon)$ such that whenever $n > M(\varepsilon)$, $||x_n| - 0| < \varepsilon$. However, since $||x_n| - 0| = |x_n - 0|$, this directly implies that x_n approaches 0 as n goes to infinity. □

Lemma 2.12. Let (x_n) be a Cauchy sequence and let (y_n) be a sequence for which

$$\lim_{n\to\infty} |x_n - y_n| = 0.$$

Then, (y_n) is a Cauchy sequence and, if $\lim_{n\to\infty} x_n$ exists, then $\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n$.

Proof. First, by Lemma 2.10, the given information is equivalent to

$$\lim_{n\to\infty} |x_{n+1} - x_n| = \lim_{n\to\infty} |(x_{n+1} - y_{n+1}) - (x_n - y_n)|.$$

This means that

$$\begin{aligned} 0 \le \lim_{n\to\infty} |y_{n+1} - y_n| &= \lim_{n\to\infty} |(y_{n+1} - y_n) - (x_{n+1} - x_n) + (x_{n+1} - x_n)| \\ &\le \lim_{n\to\infty} \max(|(y_{n+1} - y_n) - (x_{n+1} - x_n)|, |x_{n+1} - x_n|) \\ &= 0, \end{aligned}$$

implying (y_n) is Cauchy and thus converges. The second part of the lemma is fairly obvious and left as an exercise. □

Let's also verify that arithmetic operations are continuous in any field with a metric, just to practice computing limits. As a reminder:

Definition 2.13 — Let X and Y be metric spaces with metrics d_X and d_Y respectively. A function $f\colon X \to Y$ is **continuous** at a point $c \in X$ if, for all $\varepsilon > 0$, there exists a δ such that whenever $d_X(x - c) < \delta$, $d_Y(f(x), f(c)) < \varepsilon$. If f is continuous at all points in $S \subseteq X$, then we say that f is continuous on S.

In English, we are saying that f is continuous at c if, for each $\varepsilon > 0$, $f(x)$ is less than ε away from $f(c)$ whenever x is sufficiently close to c.

Exercise 2.2 (Field operations are well-behaved)**.** Show that, given a field k with metric d, addition, multiplication, taking inverses, and the absolute value corresponding to d are all continuous functions over k. To be specific, let x_0 and y_0 be elements of k and show that, for $\varepsilon > 0$, there exists a $\delta > 0$ such that, whenever $d(x, x_0) < \delta$ and $d(y, y_0) < \delta$, we have

(i) $d(x + y, x_0 + y_0) < \varepsilon$;

(ii) $d(xy, x_0y_0) < \varepsilon$;

(iii) $d(1/x, 1/x_0) < \varepsilon$;

(iv) $d(|x|, |x_0|) < \varepsilon$.

In particular, polynomials and rational functions with coefficients in k are guaranteed to be continuous (except whenever the denominator is 0).

3 What does $\mathbb{Q}_p$ look like?

3.1 Constructing $\mathbb{Q}_p$

First, we've been asserting that $\mathbb{Q}$ is incomplete with respect to $|\bullet|_p$; let's actually prove this, so that we know the rest of this section is actually accomplishing something.

Theorem 3.1 ($\mathbb{Q}$ is incomplete)**.** $\mathbb{Q}$ is not complete under the p-adic absolute value; that is, there exists a Cauchy sequence of rational numbers that does not have a limit in $\mathbb{Q}$.

Proof. We will show this for $p = 17$; it should fairly obviously generalize to odd primes.

Define (x_n) inductively as follows:

- x_1 is a solution to $x_1^2 \equiv 8 \pmod{p}$.
- For $n > 1$, x_n is defined as an integer satisfying

$$\begin{aligned} x_n^2 &\equiv 8 \pmod{p^n} \\ x_n &\equiv x_{n-1} \pmod{p^{n-1}}. \end{aligned}$$

We just need to prove that this process never gets stuck — that is, x_n can always be defined in terms of x_{n-1}. Writing $x_n = x_{n-1} + p^{n-1}r$, we need to pick r so that

$$(x_{n-1} + p^{n-1}r)^2 = x_{n-1}^2 + 2p^{n-1}r + p^n(\text{junk}) \equiv x_{n-1}^2 + 2p^{n-1}r \equiv 8 \pmod{p^n}.$$

Solving for r, then, we get

$$\begin{aligned} x_{n-1}^2 - 8 &\equiv -2p^{n-1}r \pmod{p^n} \\ \frac{x_{n-1}^2 - 8}{-2p^{n-1}} &\equiv r \pmod{p}, \end{aligned}$$

so there exist values of r that allow our recursive definition to work.

The upshot of this definition is that

- The sequence is Cauchy, since

$$|x_n - x_{n-1}|_8 \le p^{-(n-1)} \to 0$$

  whence Lemma 2.10 applies.

- The sequence $(x_1^2, x_2^2, x_3^2, \dots)$ has limit 8, since

$$|x_n^2 - 8|_p \le p^{-n} \to 0,$$

  so (x_n) should converge to $\sqrt{8} \notin \mathbb{Q}$ because $x \mapsto x^2$ is a continuous map on $\mathbb{Q}$ with respect to $|\bullet|_p$.

For $p = 2$, the same idea works, but with cubes; the issue with squares is that $(a + b \cdot 2^k)^2 \equiv a^2 \pmod{2^{k+1}}$ (in particular $\binom{2}{1}$ being even is bad), which doesn't give us the leeway that we had with odd primes via choosing r. □

What we want to do in principle is say "for each Cauchy sequence if $\mathbb{Q}$ that doesn't have a limit, add its limit to $\mathbb{Q}$." However, we can't literally do this because those limits don't exist yet. The analogous issue with the real numbers would be trying to say "okay, let's just append φ to $\mathbb{Q}$ so that F_{n+1}/F_n converges," as if $\sqrt{5}$ means anything without the framework of $\mathbb{R}$.

The way we skirt around this issue is by defining L to be a Cauchy sequence that *should* converge to L — in other words, our "numbers" are really just Cauchy sequences. In light of this, let's define $\mathcal{C}$ as the set of Cauchy sequences of $\mathbb{Q}$ under the p-adic absolute value.

Proposition 3.2. We can define arithmetic of Cauchy sequences as follows:

$$(x_n) + (y_n) = (x_n + y_n)$$
$$(x_y)(y_n) = (x_n y_n).$$

In particular, adding or multiplying Cauchy sequences term-by-term still results in a Cauchy sequence. Also, the constant sequence $(0, 0, \dots)$ is the additive identity and $(1, 1, \dots)$ is the multiplicative identity.

In the jargon, this means that $\mathcal{C}$ is a **commutative ring with unity**.

Proof. For the first part, we need to show that $(x_n + y_n)$ and $(x_n y_n)$ are both Cauchy sequences. The former is a result of

$$\lim_{n\to\infty} |x_{n+1} + y_{n+1} - x_n - y_n| \le \lim_{n\to\infty} \max(|x_{n+1} - x_n|, |y_{n+1} - y_n|) = 0,$$

and the latter is a result of

$$\begin{aligned}\lim_{n\to\infty} |x_{n+1}y_{n+1} - x_n y_n| &= \lim_{n\to\infty} |x_{n+1}y_{n+1} - x_{n+1}y_n + x_{n+1}y_n - x_n y_n| \\ &= \lim_{n\to\infty} \max(|x_{n+1}| \cdot |y_{n+1} - y_n|, |y_n| \cdot |x_{n+1} - x_n|) = 0.\end{aligned}$$

The statements about identities are immediate because 0 and 1 are the identities in $\mathbb{Q}$. □

Exercise 3.1 ($\mathcal{C}$ is not a field)**.** Find a nonconstant sequence (x_n) that has no inverse; in other words, there is no (y_n) such that $(x_n)(y_n) = (1, 1, \dots)$. There are many, many different flavors of examples.

For brevity, we will henceforth refer to the constant sequence $(x, x, \dots)$ as $\tilde{x}$, where $x \in \mathbb{Q}$.

The current issue with $\mathcal{C}$ is that there exist different sequences that should have the same limit — in particular, if the difference of two sequences tends to zero, we want to consider them to be the same. Denote this relation $(x_n) \sim (y_n)$.

Now, define $\mathcal{N}$ to be the subset of $\mathcal{C}$ whose limit is 0, so that $(x_n) \sim (y_n)$ if and only if $(x_n) - (y_n) \in \mathcal{N}$. Then, $\mathcal{C}$ can be partitioned into sets of elements that are all equivalent with respect to $\sim$. To be explicit, for any Cauchy sequence of rationals (x_n), let

$$S((x_n)) = \{(y_n) \in \mathcal{C} : (x_n) \sim (y_n)\}.$$

You can think of this as reducing $\mathcal{C}$ "modulo $\mathcal{N}$." The point is that if two elements of $\mathcal{C}$ differ by an element of $\mathcal{N}$, then they should correspond to the same number in $\mathbb{Q}_p$.

Exercise 3.2. Why does saying "modulo $\mathcal{N}$" make sense? Replace $\mathcal{C}$ with $\mathbb{Z}$ and $\mathcal{N}$ with $n\mathbb{Z}$, the set of multiples of some integer n, and compare.

Theorem 3.3 ($\mathbb{Q}_p$ is a field)**.** Let α and β be two elements of $\mathcal{C}$. Define addition and multiplication of elements of $\mathbb{Q}_p$ as follows:

$$S(\alpha) + S(\beta) = S(\alpha + \beta)$$
$$S(\alpha)S(\beta) = S(\alpha\beta).$$

Then, $\mathbb{Q}_p$ is a field under these operations whose additive identity is $S(\tilde{0}) = \mathcal{N}$ and whose multiplicative identity is $S(\tilde{1})$.

Proof. We need to check that these operations are well-defined and that any nonzero $S(\alpha)$ has a multiplicative inverse; the other field axioms follow easily.

To check that the operations are well-defined, we need to verify that the output of any arithmetic expression is invariant of which element of $S(\alpha)$ and $S(\beta)$ we choose in place of α and β. That is, if $\alpha_1 \sim \alpha_2$ and $\beta_1 \sim \beta_2$, then we need to check that

$$S(\alpha_1) + S(\beta_1) = S(\alpha_2) + S(\beta_2)$$
$$S(\alpha_1)S(\beta_1) = S(\alpha_2)S(\beta_2).$$

(Compare this to showing that operations mod n are well-defined.) By definition, these translate to

$$S(\alpha_1 + \beta_1) = S(\alpha_2 + \beta_2)$$
$$S(\alpha_1\beta_1) = S(\alpha_2\beta_2),$$

which are true if and only if $\alpha_1 + \beta_1 \sim \alpha_2 + \beta_2$ and $\alpha_1\beta_1 \sim \alpha_2\beta_2$ respectively.

To prove these relations, we mimic a similar argument to the one we made years ago when showing that addition and multiplication make sense with integers mod n; namely, let $\alpha_1 = \alpha_2 + n_\alpha$ and $\beta_1 = \beta_2 + n_\beta$, where n_α and n_β are elements of $\mathcal{N}$. Then, for addition,

$$\alpha_1 + \beta_1 = \alpha_2 + \beta_2 + n_\alpha + n_\beta,$$

so since $\mathcal{N}$ is closed under addition, $n_\alpha + n_\beta$ is in $\mathcal{N}$ and thus $\alpha_1 + \beta_1 \sim \alpha_2 + \beta_2$. For multiplication,

$$\alpha_1\beta_1 = (\alpha_2 + n_\alpha)(\beta_2 + n_\beta) = \alpha_2\beta_2 + n_\alpha\beta_2 + n_\beta\alpha_2 + n_\alpha n_\beta,$$

and since $\mathcal{N}$ absorbs multiplication, we get $\alpha_1\beta_1 \sim \alpha_2\beta_2$.

Also, since $S(\alpha) + S(\tilde{0}) = S(\alpha)$, we see that $S(\tilde{0})$ is the additive identity; similarly, $S(\tilde{1})$ is the multiplicative identity.

All that remains now is to show that multiplicative inverses exist for nonzero numbers (why can the additive identity not have an inverse?). Let (x_k) be a Cauchy sequence not in $\mathcal{N}$. By the contrapositive of Lemma 2.11,

$$\lim_{n\to\infty} |x_k| \neq 0,$$

so, since $|x_k| \geq 0$, there exists a positive c for which $|x_k| > c$ for all sufficiently large k, say all $k > M$. In particular, $x_k \neq 0$ for all such k, so we can consider the sequence (y_k) defined by

$$y_k = \begin{cases} 0 & k \leq M \\ \frac{1}{x_k} & k > M. \end{cases}$$

Clearly $(x_k)(y_k)$ is the sequence

$$(\underbrace{0, 0, \ldots, 0}_{M \text{ zeroes}}, 1, 1, \ldots),$$

so

$$\tilde{1} - (x_k)(y_k) = (1, 1, \ldots, 1, 0, 0, \ldots) \in \mathcal{N},$$

meaning $S((x_k))S((y_k)) = S((x_k)(y_k)) = S(\tilde{1})$ and thus $S((x_k))$ has an inverse. □

In short, taking $\mathcal{C}$ mod $\mathcal{N}$ gives us a field! (The technical term for this structure is the **quotient ring** $\mathcal{C}/\mathcal{N}$; it is a field because the **ideal** $\mathcal{N}$ is **maximal**.) For conciseness, we will generally refer to the sets $S((x_k))$ by some representative element (e.g. we will just say "$\tilde{1}$" for the multiplicative identity) and take care to ensure that our theorems are true irrespective of which element we choose.

Now, we need to verify that this new field $\mathbb{Q}_p$ has all the properties we want.

Definition 3.4 (Extending $|\bullet|_p$) — Let λ be an element of $\mathbb{Q}_p$ and (x_n) be any Cauchy sequence representing λ (so $\lambda = S((x_n))$). Then, define

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

The existence of this limit holds in general fields with absolute value, as the sequence being Cauchy is a result of the fact

$$|x - y| > ||x| - |y||$$

for any absolute value $|\bullet|$. Given the existence of the limit, we will show more strongly that the limit is either zero or an integral power of p.

Proof. Suppose the absolute value sequence converges to something nonzero. Then, the sequence of integers given by $\nu_p(x_n)$ also converges (e.g. by continuity of $\log_p$). But this means that the sequence has to eventually be constant as, given $k \in \mathbb{Z}$ and any $\varepsilon < 1$, there is exactly one integer within ε of k, namely k. Therefore the absolute value sequence is eventually constant, stabilizing at some $p^{-\nu}$ where ν is the limit of the ν_p sequence. □

Remark 3.5. Keep in mind that the limit in Definition 3.4 is with respect to the normal absolute value and not the p-adic one (in particular, that's why I can cite the continuity of log).

Proposition 3.6 ($|\bullet|_p$ is still an absolute value)**.** Using our new definition of $|\lambda|_p$, the following statements hold:

(i) The function is still well-defined; that is, if (x_n) and (y_n) both represent λ, then

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

(ii) The extended function is still a non-archimedean absolute value on $\mathbb{Q}_p$.

(iii) Essentially obvious: if $x \in \mathbb{Q}$, then $|\tilde{x}|_p = |x|_p$. In other words, the extended definition is consistent with our original definition in $\mathbb{Q}$.

Exercise 3.3. Prove Proposition 3.6.

It is worth noting at this point that we don't technically have $\mathbb{Q}$ as a subset of $\mathbb{Q}_p$; rather, what we're actually doing is looking at the *copy* of $\mathbb{Q}$ induced by the function $x \mapsto \tilde{x}$. We say that this map is an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ (the hook on the arrow emphasizes that this map is injective), and identify $\mathbb{Q}$ with its image. In line with this, we will simply refer to $\tilde{x}$ by x.

Theorem 3.7 (Denseness)**.** For every $\lambda \in \mathbb{Q}_p$ and $\varepsilon > 0$, there exists an $x \in \mathbb{Q}$ such that

$$|\lambda - x|_p < \varepsilon.$$

Proof. By construction, there exists a sequence of rationals (x_n) converging to λ. Since

$$\lim_{n\to\infty} |\lambda - x_n|_p = 0,$$

we can just take x_i for sufficiently large i no matter what ε is. □

Theorem 3.8 (Completeness)**.** Every Cauchy sequence of elements of $\mathbb{Q}_p$ converges to an element of $\mathbb{Q}_p$.

Proof. This essentially follows directly from denseness. The idea is as follows: consider a Cauchy sequence of p-adic numbers λ_1, λ_2, λ_3, ... Then, because $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, we can find a sequence of rationals x_1, x_2, x_3, ... such that

$$\lim_{n\to\infty} |\lambda_n - x_n|_p = 0.$$

By Lemma 2.12, this means (λ_n) and (x_n) are both Cauchy sequences. Since (x_n) is a sequence of rationals, it converges in $\mathbb{Q}_p$, ergo so does (λ_n), i.e. every Cauchy sequence of elements of $\mathbb{Q}_p$ converges. □

Thus, we are done: the field $\mathbb{Q}_p$, as we have defined it, is a completion of $\mathbb{Q}$ under $|\bullet|_p$.

3.2 Understanding $\mathbb{Q}_p$

Although we have described $\mathbb{Q}_p$ rigorously, there is still some legwork to do in the way of being able to understand its elements in the way that we described in the introduction.

Definition 3.9 — Define the **p-adic integers** $\mathbb{Z}_p$ as the set

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

The p-adic integers behave very nicely in their own right:.

Theorem 3.10. The completion of $\mathbb{Z}$ under $|\bullet_p|$ is $\mathbb{Z}_p$. Specifically:

(i) Given $x \in \mathbb{Z}_p$ and $n \geq 1$, there is a unique integer α satisfying $0 \leq \alpha < p^n$ and $|x - \alpha|_p \leq p^{-n}$.

(ii) For each $x \in \mathbb{Z}_p$, there is a Cauchy sequence of integers (α_n) converging to x with the following two properties:

- $0 \leq \alpha_n < p^n$
- $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$

Proof. First, we show (i). Since $\mathbb{Z}_p$ is a subset of $\mathbb{Q}_p$, we can find an arbitrarily close rational $\frac{a}{b}$ to x with $\gcd(a, b) = 1$. In particular, pick this number so that

$$\left|x - \frac{a}{b}\right|_p \leq p^{-n},$$

so that

$$\left|\frac{a}{b}\right|_p \leq \max\left(|x|_p, \left|x - \frac{a}{b}\right|_p\right) \leq 1.$$

This implies that $p \nmid b$. Therefore, we can pick an integer b' such that

$$x \equiv \frac{a}{b} \equiv ab' \pmod{p^n}$$

(in particular, this is how we generalize the notion of "mod p^n" to $\mathbb{Z}_p$). Then, the uniqueness of α is obvious, as there is only one α between 0 and p^n such that $\alpha \equiv ab' \pmod{p^n}$.

From here, (ii) follows immediately, as everything we did mod p^n was uniquely determined by x. □

If we really wanted, we could therefore have built up the entirety of Section 3 with $\mathbb{Z}_p$, and then defined $\mathbb{Q}_p$ as the **fraction field** of $\mathbb{Z}_p$, in analogy with the relationship between $\mathbb{Z}$ and $\mathbb{Q}$:

$$\mathbb{Q}_p = \left\{\frac{x}{y} : x, y \in \mathbb{Z}_p\right\}.$$

This means that, if we write out the base p representations of the α_n, we get a sequence

$$\begin{aligned}
\alpha_1 &= a_0 \\
\alpha_2 &= a_0 + a_1 p \\
\alpha_3 &= a_0 + a_1 p + a_2 p^2 \\
\alpha_4 &= a_0 + a_1 p + a_2 p^2 + a_3 p^3 \\
&\vdots
\end{aligned}$$

where the a_i are between 0 and $p - 1$ inclusive. This means that the (α_n) sequence converges to

$$\alpha = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

In $\mathbb{Z}$, most elements don't have an inverse; in order to find x for which $2x = 1$, we are forced to go into $\mathbb{Q}$. Life in $\mathbb{Z}_p$ is much nicer in this regard.

Theorem 3.11 (Units in $\mathbb{Z}_p$)**.** Let x be a p-adic integer. Then, there exists a y such that $xy = 1$ if and only if $|x|_p = 1$. Elements of $\mathbb{Z}_p$ with this property are called **units**.

Proof. If you have worked with generating functions before, this should look incredibly familiar. In particular, we will just work with $x = x_0 + x_1 p + x_2 p^2 + \cdots$ and $y = y_0 + y_1 p + y_2 p^2 + \cdots$ as formal power series in p, where the size condition tells us that x_0 is nonzero. Then, the coefficient of p^n in xy is equal to

$$\sum_{k=0}^{n} x_k y_{n-k}.$$

We want this to be $1 \pmod p$ when $n = 0$ and $0 \pmod p$ otherwise. In particular, since $x_0 \not\equiv 0 \pmod p$, we can choose y_n to make $x_0 y_n$ anything modulo p, which means that we define

$$y_n \equiv -\frac{1}{x_0} \sum_{k=1}^{n} x_k y_{n-k} \pmod p$$

for $n > 0$, and $y_0 = -\frac{1}{x_0}$. □

This means every element of $\mathbb{Z}_p$ is either 0 or can be expressed as $p^n u$, where n is a nonnegative integer and u is a unit. In turn, we can characterize $\mathbb{Q}_p$. For some $q \in \mathbb{Q}_p$, let ν be the integer such that $|p^\nu q|_p = 1$, so that $p^\nu q$ is a unit. Then, using the base-p expansion, we see that

$$p^\nu q = a_0 + a_1 p + a_2 p^2 + \cdots \iff q = a_0 p^{-\nu} + a_1 p^{-\nu+1} + \cdots + a_\nu + a_{\nu+1} p + \cdots$$

This also yields a more natural definition of $\nu_p(q)$ as the smallest integer ν such that $q \in p^\nu \mathbb{Z}_p$, where

$$p^\nu \mathbb{Z}_p = \{p^\nu x : x \in \mathbb{Z}_p\}.$$

Exercise 3.4. Prove that this is consistent with the limit definition of $|\bullet|_p$.

4 Hensel's Lemma

4.1 The Theorem

As usual, we begin with an analogy in the real numbers. Let's say that you wanted to approximate a real root of some polynomial, like

$$P(x) = x^3 - 6x^2 + 9x - 2.$$

We can start with a guess, like $r_0 = 0$. Of course, $P(r_0) = -2$, so r_0 isn't a root. However, we can create a linear approximation of $P(x)$ near r_0 with the line

$$y - P(r_0) = P'(r_0)(x - r_0)$$

and look at where this approximation hits the x-axis. Assuming our initial guess was "decent," this x-intercept will be closer to a root of P than r_0. Computationally, we thus try to improve on r_0 by setting

$$r_1 = r_0 - \frac{P(r_0)}{P'(r_0)}.$$

Repeating the same process, we thus get a sequence

$$r_n = r_{n-1} - \frac{P(r_{n-1})}{P'(r_{n-1})},$$

which, if our initial guess was "decent," will converge to a real root of P. In this case, (r_n) will converge to $2 - \sqrt{3}$.

This process is known as Newton's method for approximating roots of polynomials, and we will work to understand its p-adic analogue. First, let's define what we will mean by $P'(x)$.

Definition 4.1 — Let $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial with coefficients in $\mathbb{Z}_p$. The **formal derivative** of $P(x)$ is

$$P'(x) = a_1 + 2a_2x + 3a_3x^2 + \cdots + na_nx^{n-1}.$$

The important part of this definition of a derivative is that the Taylor formula still works:

Lemma 4.2 (Taylor formula)**.** For any polynomial $F(x)$ with coefficients in $\mathbb{Q}_p$,

$$F(x+h) = F(x) + F'(x)h + \frac{1}{2!}F''(x)h^2 + \frac{1}{3!}F'''(x)h^3 + \cdots$$

Proof. We can do this by simply equating coefficients (same as in the $\mathbb{R}$ case). Let $F^{(n)}(x)$ be the nth derivative of $F(x)$, with $F^{(0)}(x) = F(x)$. Then, the coefficient of x^m in $F^{(k)}(x)$ is

$$[x^m]F^{(k)}(x) = \binom{m+k}{k} a_{m+k}h^k,$$

which means that the coefficient of x^m in the right-hand side is

$$\sum_{k=0}^{\infty} \binom{m+k}{k} a_{m+k}h^k,$$

where we take $a_N = 0$ for $N > n$.

On the other hand, the x^m coefficient in the left-hand side is the sum of the x^m coefficients over all the terms of the form $a_k(x+h)^k$, which yields

$$\sum_{k=0}^{\infty} \binom{k}{m} a_k h^{k-m} = \sum_{k=m}^{\infty} \binom{k}{m} a_k h^{k-m} = \sum_{k=0}^{\infty} \binom{k+m}{m} a_{k+m} h^k.$$

This is clearly equal to the previous sum, as desired. □

Now, we are ready to state the big theorem.

Theorem 4.3 (Hensel's lemma, mk. I)**.** Let $F(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ have coefficients in $\mathbb{Z}_p$. Suppose that there exists an $\alpha_1 \in \mathbb{Z}_p$ such that

$$F(\alpha_1) \equiv 0 \pmod{p}, \quad F'(\alpha_1) \not\equiv 0 \pmod{p}.$$

Then, there exists a unique $\alpha \equiv \alpha_1 \pmod{p}$ such that $F(\alpha) = 0$.

Proof. We will construct a sequence of p-adic integers with the following conditions:

(i) $F(\alpha_n) \equiv 0 \pmod{p^n}$

(ii) $F'(\alpha_n) \not\equiv 0 \pmod{p}$

(iii) $\alpha_n \equiv \alpha_{n+1} \pmod{p^n}$.

This sequence will obviously be Cauchy, so it will tend to a limit α, which means that by continuity we will have $F(\alpha) = 0$.

Now, suppose that we already have α_n. To satisfy condition (iii), we man take $\alpha_{n+1} = \alpha_n + p^n b_n$, where $b_n \in \mathbb{Z}_p$. Then, by the Taylor formula,

$$\begin{aligned} F(\alpha_{n+1}) &= F(\alpha_n + p^n b_n) \\ &\equiv F(\alpha_n) + F'(\alpha_n)p^n b_n \pmod{p^n}. \end{aligned}$$

Since $F'(\alpha_n)$ is invertible mod p by assumption, there is a unique b_n between 0 and $p-1$ that makes the expression 0, which gives us condition (i). Condition (ii) can be easily checked by using the Taylor formula: specifically,

$$F'(\alpha_{n+1}) \equiv F'(\alpha_n) \pmod{p},$$

since the rest of the terms have the $b_n p^n$ multiplier.

Moreover, the uniqueness assertion is a result of the fact that the sequence is uniquely determined mod p^n at each step, and elements of $\mathbb{Z}_p$ at the end of the day are just a gluing together of their mod p^n components. □

To be explicit, the value of b_n can just be taken as $-\frac{F(\alpha_n)}{p^n F'(\alpha_n)}$ (since we only care about it mod p anyway), at which point

$$\alpha_{n+1} = \alpha_n - p^n \cdot \frac{F(\alpha_n)}{p^n F'(\alpha_n)} = \alpha_n - \frac{F(\alpha_n)}{F'(\alpha_n)},$$

showing that this process spits out the same recursion as Newton's method.

Interestingly, the mod p condition on F' can be loosened: if $\nu_p(F'(\alpha_n))$ is small enough, then $\frac{F(\alpha_n)}{F'(\alpha_n)}$ would still be in $\mathbb{Z}_p$ anyway, which is the main point of our algorithm. So, as long as $\nu_p(F'(\alpha_n))$ stays "small enough," it can still be possible to make this process work. To be precise:

Theorem 4.4 (Hensel's lemma, mk. II)**.** As before, let F be a polynomial in $\mathbb{Z}_p[x]$. Suppose that $\alpha_1 \in \mathbb{Z}_p$ satisfies $|F(\alpha_1)|_p < |F'(\alpha_1)|_p^2$. Then, there exists a unique root $\alpha \in \mathbb{Z}_p$ of F such that $|\alpha - \alpha_1|_p < |F'(\alpha_1)|_p$.

The details of the proof are omitted, as the process is very much identical to that of the first version.

4.2 Examples

Hensel's lemma is so powerful because it often guarantees the existence of a solution to a polynomial based solely on mod p information.

Some simple examples:

Theorem 4.5 (Squares)**.** Let u be a p-adic unit and n an integer. Then, $p^n u$ is the square of some p-adic number if and only if n is even and u is a square mod p.

Theorem 4.6 ($(p-1)$-th roots of unity)**.** The p-adic numbers contain the $(p-1)$-th roots of unity.

The latter theorem relies on the fact that the derivative of $X^n - 1$, which is nX^{n-1}, vanishes only at zero when $p \nmid n$. In fact, we get that all the primitive roots of unity are in $\mathbb{Q}_p$ when n is any divisor of $p-1$. More strongly, these are the only numbers for which nontrivial roots of unity exist!

Theorem 4.7. Suppose $p \nmid n$. Then, nth roots of unity exist if and only if $n \mid p$.

As mentioned above, we can get rid of the $p \nmid n$ condition with some more effort (specifically, some analysis with the p-adic logarithm), but that is too in depth to discuss here.