An Introduction to the p-adic Numbers

Alistair Pattison, Akash Ganguly, John Byun

May 2023

Abstract

In this paper, we trace the first chapter of Gouvêa [3] to give an intuitive and motivated introduction to the p-adic numbers. We explore the consequences of writing integers n as polynomials in base p, where p is a prime and show how similar power series can be generated for rational numbers a/b. We give a working definition of the p-adic numbers $\mathbb{Q}_p$ and investigate congruences modulo p^n that have no solutions in $\mathbb{Q}$ to show that the 7-adic numbers, $\mathbb{Q}_7$, are strictly larger than the rational numbers, $\mathbb{Q}$. Along the way, we observe several situations in which we require large powers of p to behave like "small" numbers, which naturally leads us to define the p-adic absolute value.

Contents

1 The History of p-adic Numbers

At the beginning of the twentieth century, German mathematician Kurt Hensel noticed several similarities between two rings and their derivative objects: the ring of integers $\mathbb{Z}$ and the ring of polynomials in one variable with complex coefficients $\mathbb{C}[x]$. On the surface, they are both unique factorization domains[1] with the analogous object to the primes p in $\mathbb{Z}$ being given by the monomials $(x-\alpha)$ in $\mathbb{C}[x]$. Both rings also give rise to a corresponding fraction field given by taking quotients of elements from each ring. For $\mathbb{Z}$, the fraction field is the familiar $\mathbb{Q}$. For $\mathbb{C}[x]$, the corresponding field of fractions is

$$\mathbb{C}(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{C}[x] \right\}. \tag{1}$$

Hensel wanted to see just how far he could stretch this analogy. In particular, he noticed that in $\mathbb{C}(x)$, we are able to write every element $f(x)/g(x)$ as series

$$f(x) = \frac{p(x)}{q(x)} = \sum_{i \geq n_0} a_i (x-\alpha)^i \tag{2}$$

that converges for all x near α in $\mathbb{C}$. This expansion is called a *Laurent series* and is a complex analogue of the familiar Taylor series from calculus. The important thing to note here is that we are able to represent a somewhat complicated function as a (possibly infinite) power series in a linear polynomial $(x-\alpha)$. Recall from the previous paragraph that these monomials are exactly the "primes" of $\mathbb{C}[x]$.[2] Hensel then considered the analogue of Laurent series in $\mathbb{Q}$, the fraction field of $\mathbb{Z}$. Can we take a fraction a/b and write it as a series with respect to a single prime p as we are able to in $\mathbb{C}(x)$? If so, how do we do it? What are the consequences? Answering these questions are the main objectives of this paper.

2 Expanding Numbers in Base p

When we write the number 428, what we really mean is $8 + 2 \cdot 10 + 4 \cdot 10^2$, but there's nothing fundamental about using the number 10 as our base. Much of the theory behind p-adic numbers can be motivated by the simple idea of writing an integer in base p, where p is prime, and treating the

[1] For a reference on this, see chapters 8 and 9 of Dummit and Foote [2].

[2] Readers familiar with the notion might note that these linear polynomials are exactly the prime ideals of $\mathbb{C}[x]$.

resulting expansion as a formal polynomial in p. For example, expanding 428 in base $p = 7$ gives us the polynomial

$$428 = 1 + 5p + p^2 + p^3. \tag{3}$$

On it's own, this isn't particularly useful, but interesting things happen when we extend this idea to rational numbers a/b. To do so, we write a and b in base p, and take the series expansion given by "dividing" the resulting rational function while treating p as a formal variable. This idea is rather abstract, so as an example we consider $p = 3$ and the fraction $15/11$. We have that $15 = 2p + p^2$ and $11 = 2 + p^2$, so

$$\begin{aligned} \frac{15}{11} &= \frac{2p + p^2}{2 + p^2} \\ &= p + 2 \cdot p^2 + 2 \cdot p^3 + p^4 + p^5 + 0 \cdot p^6 + 2 \cdot p^7 + 2 \cdot p^8 + p^9 + p^{10} + 0 \cdot p^{11} + \cdots \end{aligned} \tag{4}$$

where the pattern of coefficients $2, 2, 1, 1, 0$ repeats forever. One can check that this is the correct expansion by multiplying through by the denominator $11 = 2+p^2$ and simplifying with the knowledge that $p = 3$, so $3p^k = p^{k+1}$:

$$\begin{aligned} &(2 + p^2)(p + 2 \cdot p^2 + 2 \cdot p^3 + p^4 + p^5 + 2 \cdot p^7 + 2 \cdot p^8 + p^9 + p^{10}) \\ &\quad = 2p + 4p^2 + 5p^3 + 4p^4 + 4p^5 + p^6 + 5p^7 + \cdots \\ &\quad = 2p + p^2 + 6p^3 + 4p^4 + \cdots \\ &\quad = 2p + p^2 + 6p^4 + 4p^5 + \cdots \\ &\quad = 2p + p^2 + 6p^5 + p^6 + \cdots \\ &\quad = 2p + p^2 + 3p^6 + 5p^7 + \cdots \\ &\quad = 2p + p^2 + 6p^7 + \cdots . \end{aligned} \tag{5}$$

Notice how the higher-order terms telescope off to the right. The cancellation we observe hints at a sort of "convergence": any finite truncation of the process leaves error terms, but if we could continue our simplification "to infinity" everything would just work out. Keep this example in the back of your mind as we introduce the p-adic absolute value at the end of this paper.

This process of writing rational numbers as series works for *any* rational a/b, and motivates the following working definition for the p-adic numbers:

Definition 1 (The p-adic numbers)**.** *Given a prime p, the p-adic numbers $\mathbb{Q}_p$ are the set of all finite-tailed Laurent series of the form*

$$\sum_{i \geq n_0} a_i p^i = a_{n_0} p^{n_0} + a_{n_1} p^{n_1} + a_{n_2} p^{n_2} + \cdots . \tag{6}$$

By "finite tailed", we mean that the smallest exponent of p in the sum is finite, but the series may (and often does) extend to positive infinity.

There is a natural inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}_p$ given by writing an integer a in base p. Additionally, the process described above for computing a series expansion of any rational number with respect to p induces another inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. This gives rise to a further question: Is this inclusion a bijection? If we could find a finite-tailed Laurent series that is not the result of computing the p-adic expansion of a rational number, then we would have that the map is not bijective. Appealing to our analogy with $\mathbb{C}(x)$, we would expect that such a series exists. For example, the Laurent series for $\sin(x)$ is not the series for any rational function. But what would these p-adic numbers even look like? And how do we find them?

3 Solving Congruences Modulo p^n

It turns out that we can find irrational elements of $\mathbb{Q}_p$ by investigating solutions to equivalences of the form $x^2 \equiv a \mod p^n$, where a in $\mathbb{Z}$ such that $0 \leq a < p^n$. We begin by examining simple equations with rational (i.e. integer) solutions to develop some intuition before progressing to choices of a for which no rational solutions exist.

To start, we consider the sequence of equivalences given by

$$x^2 \equiv 25 \mod p^n \tag{7}$$

for all $n \in \mathbb{N}$. Our familiarity with the integers tells us that $x \equiv \pm 5 \mod p^n$ works for every n, and one might wonder whether there are any additional solutions. It turns out that for most choices of p, there are not.

Theorem 2 (Problem 9 in Gouvêa [3])**.** *If $p \neq 2, 5$, then the only solutions of $x^2 \equiv 25 \mod p^n$ up*

to congruence are ± 5.

Proof. Naively, we might like to factor the equation and set it equal to 0, like so:

$$x^2 \equiv 25 \mod p^n \iff x^2 - 25 \equiv 0 \mod p^n \iff (x+5)(x-5) \equiv 0 \mod p^n. \quad (8)$$

Unfortunately, $\mathbb{Z}/p^n\mathbb{Z}$ isn't an integral domain in general, so there may be zero-divisors and we can't immediately conclude that $x = \pm 5$. However, it turns out the modulus being a prime power where p is neither 2 nor 5, combined with a few tricks, is enough to get us what we want.

In particular, assume towards contradiction that $a = (x+5)$ and $b = (x-5)$ are non-zero integers. By the equivalence, we know that $p^n \mid ab$. By unique factorization, this means that if $p \nmid a$, then $p^n \mid b$. However, because a and b differ by a gap of size $10 = 2 \cdot 5$, if $p \neq 2, 5$, then $p \mid a$ implies $p \nmid b$ (which implies $p^n \mid a$, by the observation above). Similarly $p \mid b$ implies $p \nmid a$ implies $p^n \mid b$. Therefore $x \equiv \pm 5 \mod p^n$, as desired. □

If $p = 2$ or $p = 5$, then the implications $p \mid (x+5) \implies p \nmid (x-5)$ and $p \mid (x-5) \implies p \nmid (x+5)$ no longer hold, and we may obtain more than two solutions. For example, if we take $p = 2$ and $n = 5$, then the equivalence $x^2 \equiv 25 \mod 32$ has 2 additional solutions: $x \equiv \pm 21 \mod 32$.

We'll do a few more examples for good measure:

Theorem 3 (Problem 10 in Gouvêa [3])**.** *Similar ideas hold for* $x^2 \equiv 49 \mod 5^n$ *and* $x^3 \equiv 27 \mod 2^n$.

Proof. We can rearrange the first equivalence $x^2 \equiv 49 \mod 5^n$ as

$$x^2 - 49 \equiv 0 \mod 5^n \iff (x+7)(x-7) \equiv 0 \mod 5^n. \quad (9)$$

By unique factorization, we know that if $5^n \mid ab$ and $5 \nmid a$, then $5^n \mid b$. We know $5 \mid (x+7) \implies 5 \nmid (x-7)$ and $5 \mid (x-7) \implies 5 \nmid (x+7)$. Therefore $x \equiv \pm 5 \mod p^n$.

We can use a similar process for the second equivalence:

$$x^3 \equiv 27 \mod 2^n \iff x^3 - 27 \equiv 0 \mod 2^n \iff (x-3)(x^2+3x+9) \equiv 0 \mod 2^n. \quad (10)$$

Since $x^2 + 3x + 9$ is always odd, we know that for the equation to hold, we must have $2^n \mid x - 3$, which implies that $x \equiv 3 \mod 2^n$. □

We now turn our attention to the equivalence $x^2 \equiv 2 \mod 7^n$ which—if we ignore the modulus—is perhaps the simplest example of an equation with no rational solution. Thankfully, solving the equivalence with the modulus is much easier than solving the equation without it. For example, when $n = 1$, both 3 and $-3 \equiv 4 \mod 7$ are solutions. Are there more?

Theorem 4 (Problem 12 in Gouvêa [3])**.** *For each n, there can be at most two solutions to $x^2 \equiv 2 \mod 7^n$.*

Proof. We use essentially the same technique as in the previous two problems. In particular, let a and b be solutions to $x^2 \equiv 2 \mod 7^n$; we'll show that $a = \pm b$. By transitivity, we know that $a^2 \equiv b^2 \mod 7^n$ which we can rearrange to yield

$$(a + b)(a - b) \equiv 0 \mod 7^n. \tag{11}$$

Since a and b are solutions to $x^2 \equiv 2 \mod 7^n$, it follows that neither a nor b are divisible by 7. Therefore $7 \mid a + b \implies 7 \nmid a - b$ and $7 \mid a - b \implies 7 \nmid a + b$. Therefore $a \equiv \pm b \mod 7^n$. □

This lemma caps the number of possible solutions, but do solutions exist for every n? Are there always 2 solutions? And how do we find them?

We can find a solution modulo 7^2 by noticing that any solution to $x^2 \equiv 2 \mod 7^2$ must also be a solution to $x^2 \equiv 2 \mod 7$. But we know the solutions to this second equation: 3 and 4! Focusing on the first solution, we know that our solution to $x^2 \equiv 2 \mod 7^2$ must be of the form $3 + 7k$ for some k. So we have

$$\begin{aligned} 2 &\equiv (3 + 7k)^2 \\ &\equiv 9 + 42k + 49k^2 \\ &\equiv 9 + 42k \mod 7^2. \end{aligned} \tag{12}$$

Moving the 2 to the other side and dividing through by 7 gives $1 + 6k \equiv 0 \mod 7$ which we can solve to find $k \equiv 1 \mod 7$. Plugging this back in to our expression for x gives us

$$x \equiv (3 + 7 \cdot 1) = 10 \mod 7^2. \tag{13}$$

One can check that $10^2 = 100 \equiv 2 \mod 7^2$, and repeating this process for $n = 3$ gives $108^2 \equiv 2 \mod 7^3$. An interesting pattern emerges when we write out the base-p expansions for this sequence of solutions:

$$\begin{aligned} 3 &= 3 \\ 10 &= 3 + p \\ 108 &= 3 + p + 2p^2. \end{aligned} \tag{14}$$

The early terms in the expansion seem to be fixed, and when we compute solutions modulo higher powers of p, we just add higher order p terms to the right.

The sequence of numbers generated this way seems to "converging" to a value. The following definition makes this idea slightly more rigorous.

Definition 5. *A sequence of integers (α_n) is coherent with respect to a prime p if for all natural numbers n, we have*

(i) $0 \leq \alpha_n < p^n$ *and*

(ii) $\alpha_{n+1} \equiv \alpha_n \mod p^n$.

A nice interpretation of this definition is that for all $n \geq M$, the first M coefficients of the expansion of α_n will always be the same.

It would be nice if we could keep computing solutions to $x^2 \equiv 2 \mod p^n$ indefinitely in a coherent fashion, similarly to what happens when one finds the decimal expansion of $\sqrt{2}$ in the real numbers: as you compute more terms, the earlier terms stay the same, and the further you go, the more precision one gets. The following theorem verifies that we can indeed continue this process indefinitely.

Theorem 6 (Problem 13 in Gouvêa [3])**.** *Given some α_n such that $\alpha_n^2 \equiv 2 \mod 7^n$, there exists a unique α_{n+1} such that*

(i) $\alpha_{n+1} \equiv \alpha_n \mod 7^n$ *and*

(ii) $\alpha_{n+1}^2 \equiv 2 \mod 7^{n+1}$

An interpretation of this claim in the context of coherent sequences is that given a starting point $\alpha_1 \equiv 2 \mod 7^1$, we can generate a coherent sequence (α_n) such that each $\alpha_n \equiv 2 \mod 7^n$. We

started doing this in the previous few examples: this theorem implies that we may repeat this process for as long as we like, given enough patience.

Proof. By the first condition of the theorem, we know that $\alpha_{n+1} = \alpha_n + 7^n k$ for some integer k; we will solve for this k to find a closed form for α_{n+1}. Combining this equation with the theorem's second condition tells us that

$$\begin{aligned} 2 &\equiv \alpha_{n+1}^2 \\ &= (\alpha_n + 7^n k)^2 \\ &= \alpha_n^2 + 2 \cdot 7^n \, k \, \alpha_n + 7^{2n} k^2 \\ &\equiv \alpha_n^2 + 2 \cdot 7^n \, k \, \alpha_n \qquad\qquad \mod 7^{n+1}. \end{aligned} \tag{15}$$

Moving things around and dividing through by 7^n as in the previous example gives

$$2 \, k \, \alpha_n \;\equiv\; -\frac{\alpha_n^2 - 2}{7^n} \;\equiv\; 6 \, \frac{\alpha_n^2 - 2}{7^n} \mod 7. \tag{16}$$

This is a legal operation because the fact that $\alpha_n^2 \equiv 2 \mod 7^n$ guarantees that the fraction is an integer. We are now operating modulo 7, so every element has a multiplicative inverse and we may conclude that our desired k is the (unique) solution to

$$k \;\equiv\; 3 \, \alpha_n^{-1} \, \frac{\alpha_n^2 - 2}{7^n} \mod 7. \tag{17}$$

Therefore, $\alpha_{n+1} = \alpha_n + 7^n \, k$ is the unique value satisfying both our desired properties. □

n	1	2	3	4	5	6	7	8	9	10
α_n	3	10	108	2,166	4,567	38,181	155,830	1,802,916	24,862,120	266,983,762
k	3	1	2	6	1	2	1	2	4	6

Table 1: The first 10 terms in the expansion of x_1, found using the recursive method described in Theorem 6.

Using this theorem and a bit of computational help, we can compute more terms in our expansion, which we give in Table 1. This sequence of α_n doesn't "converge" in the typical sense of the word, but by continuing this process "to infinity", we get a power series in p which—by definition—is an

element of $\mathbb{Q}_7$. We call this power series x_1:

$$\begin{aligned}
\alpha_1 &= 3 \\
\alpha_2 &= 3 + 1\,p \\
\alpha_3 &= 3 + 1\,p + 2\,p^2 \\
\alpha_4 &= 3 + 1\,p + 2\,p^2 + 6\,p^3 \\
&\vdots \\
x_1 &= 3 + 1\,p + 2\,p^2 + 6\,p^3 + 1\,p^4 + 2\,p^5 + 1\,p^6 + 2\,p^7 + 4\,p^8 + 6\,p^9 + \cdots .
\end{aligned} \tag{18}$$

Theorem 7 (Problem 14 in Gouvêa [3])**.** *The number $x_1 \coloneqq \lim \alpha_n$ obtained above satisfies the equation $x_1^2 = 2$ in $\mathbb{Q}_7$.*

Given our current understanding of the p-adic numbers, the statement above is gibberish: how do we take a limit in $\mathbb{Q}_7$? If we interpret convergence in the familiar sense, the sequence $(\alpha_n) = 3, 10, 108, 2166, \ldots$ clearly blows up to infinity, so x_1 isn't even well defined. For the moment, let's put these concerns aside and see what we would need for $x_1^2 = 2$.

By construction of the sequence (α_n), we have that $\alpha_n^2 \equiv 2 \mod 7^n$, so

$$\alpha_n^2 = 2 + c_n\,p^n \tag{19}$$

for some $c_n \in \mathbb{N}$. Proceeding naively from this observation, we have

$$x_1^2 = \lim \alpha_n^2 = 2 + \lim c_n\,p^n. \tag{20}$$

For us to have $x_1^2 = 2$, the error term on the right must converge to something "small" in context of $\mathbb{Q}_7$. In the following section, we define the p-adic absolute value which makes this notion rigorous.

4 The p-adic Absolute Value

In the previous sections, our treatment of the p-adic numbers was very fast and loose: we did algebra naively treating p as a formal symbol, and convergence was treated as an afterthought. This section will begin to provide a little more mathematical rigor motivated by the intuition developed in the

previous sections, although it is by no means a comprehensive formal treatment of the subject. We direct readers to Gouvêa [3] for such a work.

The examples at the end of the previous section revealed the need for large powers of p to be "small" if we want our sequence α_n to converge. Although we don't think about it so explicitly when operating in $\mathbb{Q}$ or $\mathbb{R}$, one way we measure the size of a number is with its absolute value: -1000 is a "big" number because its absolute value $|1000|$ is large. When working in the p-adic numbers, we require a new and very different absolute value for things to make sense. Loosely, it measures how divisible a number is by p: the more divisible a number is by p, the smaller it is. This new p-adic absolute value is constructed as follows.

Definition 8 (The p-adic valuation)**.** *Let n be an integer with prime factorization $n = \prod_p p^{a_p}$. Then,*

$$\nu_p(n) \;=\; a_p \;=\; \begin{cases} \max\{k : p^k \mid n\} & \text{if } n \neq 0 \\ \infty & \text{if } n = 0 \end{cases} \tag{21}$$

is the **p-*adic valuation*** *of n, i.e., the largest power of p that divides n. This can be extended to the rationals as follows: For $a/b \in \mathbb{Q}^\times$,*

$$\nu_{p_i}(a/b) = \nu_p(a) - \nu_p(b). \tag{22}$$

We leverage the p-adic valuation to define our absolute value on $\mathbb{Q}_p$.

Definition 9 (The p-adic absolute value)**.** *For any $x \in \mathbb{Q}$, the* **p-*adic absolute value*** *of x is defined by*

$$|x|_p = \begin{cases} p^{-\nu_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases} \tag{23}$$

These are very novel constructions, so let's do a few examples. For $n = 625$ and $p = 5$, we have $\nu_5(625) = \nu_5(5^4) = 4$, and in general, $\nu_p(p^k) = \nu_p(p^k) = k$, and $|p^k|_p = \frac{1}{p^k}$: prime powers are tiny! In the case where $p = 2$, every odd number k has $\nu_2(k) = 0$, so $|k|_2 = 1$: Half of all integers are the same size! In fact, for any prime p and any integer k, the preimage of k, $\nu_p^{-1}(k)$ is countably infinite!

Things are equally strange for rational numbers. For example, $n = 1/2066715$ is minuscule under our typical understanding of size, but

$$\nu_3(1/2066715) = -\nu_3(3^{10} \cdot 5 \cdot 7) = -10 \tag{24}$$

so $|1/2066715|_3 = 3^{10} = 59049$. It's huge 3-adically! With $p = 33$ and $n = |123/48|_3$, things get even more strange. We calculate the valuation first: $\nu_3(123/48)$. Writing out the prime factorization $123 = 3 \cdot 41$ and $48 = 2^4 \cdot 3$ reveals

$$\nu_3(123/48) = \nu_3(123) - \nu_3(48) = 1 - 1 = 0 \tag{25}$$

which in turn implies $|123/48|_3 = 1$. This clues us in on the fact that the p-adic valuation, and thus the p-adic absolute value, does not depend on the representation of the rational number— we could have reduced our original fraction by cancelling out the common factor of 3 from the numerator and denominator, but this would not have changed our p-adic valuation.

This absolute value is exactly what we need to rigorously define convergence for our sequence α_n^2 using the standard definition from analysis[3]. Given any $\varepsilon > 0$, we define $\delta := \log_p(1/\varepsilon)$ so that for any $n > \delta$,

$$|a_n^2 - 2|_p = |c_n\, p^n|_p \leq |p^n|_p = \frac{1}{p^n} < \varepsilon. \tag{26}$$

Therefore, (a_n^2) converges to 2, and we can happily verify $x_1^2 = 2$ in $\mathbb{Q}_7$.

The polynomial $x^2 = 2$ famously does *not* have a root in $\mathbb{Q}$, so the existence of such a x_1 in $\mathbb{Q}_7$ shows that the 7-adics are strictly larger than the the rationals. In fact, for every prime p, there exist polynomials for which roots exist in $\mathbb{Q}_p$ but not $\mathbb{Q}$[4]. However, no $\mathbb{Q}_p$ is algebraically closed: For every p, there exist polynomials with no root in $\mathbb{Q}_p$[5]. For further explanation of these facts, see Section 1 of Gouvêa [3]

[3] See, for example, Chapter 2 of Abbott [1] for an overview.
[4] For example, consider the equation $x^2 = a$ where a is a quadratic residue modulo p.
[5] Similarly, $x^2 = b$ where b is a quadratic nonresidue modulo p.

5 Conclusion

In this paper, we gave an intuitive and motivated introduction to the p-adic numbers and the p-adic absolute value by exploring the consequences of writing integers n in base p and treating the expansions as a formal polynomials in p. We showed how similar infinite polynomials can be generated for rational numbers a/b and used this intuition to define the p-adic numbers, $\mathbb{Q}_p$. By investigating congruences modulo p^n that have no solutions in $\mathbb{Q}$, we were able to construct p-adic numbers that have no rational counterpart—with the stipulation that we interpret large powers of p to be "small". This naturally leads us to define the p-adic absolute value.

There is still much to learn about the p-adics including a rich algebraic structure and a topology induced by the metric $d(a,b) \coloneqq |a-b|_p$. We direct readers to Gouvêa [3] for a more complete treatment of the subject, but we hope that this light-hearted introduction piqued interest and provided the beginnings of an intuitive understanding should one decide to pursue the topic more comprehensively.

References

[1] Stephen Abbott. *Understanding Analysis*. 2015.

[2] D.S. Dummit and R.M. Foote. *Abstract Algebra*. 2003.

[3] Fernando Q. Gouvêa. *p-adic Numbers, An Introduction*. 2000.