

1.1 Getting real

Quote 1.1

“God made the integers; all else is the work of man”—Leopold Kronecker

Let’s begin by appreciating how far we have come, not just as individuals who have learned volumes of mathematics, but as a society which has collectively developed mathematical theory over millennia.

We will recall an old and subtle question: what is a real number? For now, we’ll content ourselves with some examples, and *complete* this discussion later.

Examples:

- (a) 3.14159... (= π)
- (b) 0.33333... (= $1/3$)
- (c) 1.41213... (= $\sqrt{2}$)

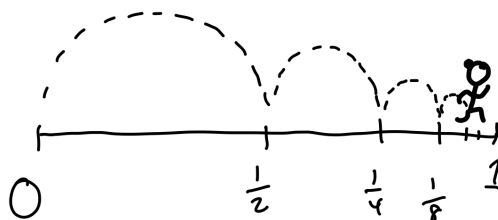
As familiar and natural as these numbers may seem to us now, it’s worth remembering that they were once quite controversial. This is illustrated by the colorful (likely apocryphal) tale of the Pythagorean who made the mistake of demonstrating to his fellow cult members that $\sqrt{2}$ was irrational while on a boat, for which they rewarded him with an all-expenses-paid trip to the bottom of the ocean.

As much as you may miss in-person conferences, a distinct advantage of Zoom is that you can’t be thrown off a boat. Let’s look, in the safety of our homes, at the infamous square root of two. The notation above is shorthand for:

$$\sqrt{2} = 1 \cdot \left(\frac{1}{10}\right)^0 + 4 \cdot \left(\frac{1}{10}\right)^1 + 1 \cdot \left(\frac{1}{10}\right)^2 + 2 \cdot \left(\frac{1}{10}\right)^3 + 1 \cdot \left(\frac{1}{10}\right)^4 + 3 \cdot \left(\frac{1}{10}\right)^5 + \dots$$

Why have we come to accept this? It’s an infinite sum, after all. Humans (including me, and maybe even including you!) were not always comfortable with those. Consider the following version of Zeno’s paradox.

Suppose Greek track-and-field legend Atalanta has to run a mile. In order to do that, she must first run half a mile. Then, she must run an additional quarter mile. Then an additional sixteenth of a mile. This is an infinite number of distances to run: an apparent “paradox.”



And yet, we have come to understand that these distances add up to 1. In general, we think of the infinite sum

$$\sum_{i=n_0}^{\infty} c_i \left(\frac{1}{10}\right)^i \text{ with } n_0 \in \mathbb{Z} \text{ and } c_i \in \{0, \dots, 9\}$$

as just another real number since the sum **converges**. Indeed, the course run by Atalanta is an example of a geometric series:

$$\frac{1}{2} \sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i$$

Which we can evaluate using the classic formula

$$\sum_{i=0}^{\infty} p^i = \frac{1}{1-p}$$

which we have learned converges as long as $|p| < 1$.

Along similar lines, the decimal expansion $\sum_{i=n_0}^{\infty} c_i \left(\frac{1}{10}\right)^i$ as above converges because the “tails” $\sum_{i=N}^{\infty} c_i \left(\frac{1}{10}\right)^i$ can be bounded above by $\left(\frac{1}{10}\right)^N$ times the convergent geometric series $9 \sum_{i=0}^{\infty} \left(\frac{1}{10}\right)^i$. The N th tail is thus $\left(\frac{1}{10}\right)^N$ times a bounded quantity, which goes to 0 since

$$\lim_{N \rightarrow \infty} \left(\frac{1}{10}\right)^N = 0.$$

1.2 Zeno’s p -aradox

Let’s look again at the geometric series

$$1 + p + p^2 + p^3 + \dots$$

this time we take p to be a prime number. In particular, $p > 1$, so this series seemingly fails to converge.

Enter p -atalanta. Runner p -atalanta runs a race, starting at 0, running first to point 4, then running 20 miles to point $4 + 4 \cdot 5^1$, then running another 100 miles to point $4 + 4 \cdot 5^1 + 4 \cdot 5^2$, etc, culminating in the series

$$4 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + 4 \cdot 5^5 + 4 \cdot 5^6 + \dots$$



Seemingly this does not converge because p -atalanta takes bigger and bigger steps. Yet we can approach this from a new, arithmetic perspective, where we view these steps as smaller and smaller.

1.3 A New Perspective

We first recall some definitions.

Definition 1.1

For two integers a, b with $a \neq 0$, we say that a **divides** b , and write $a|b$, if there exists $n \in \mathbb{Z}$ such that $b = na$. Examples: $2 | -6$, $25 | 625$, and $m | 0$ for all integers $m \neq 0$.

Definition 1.2

For two integers a, b and a natural number n , we say that a is **congruent** to b mod n , and write $a \equiv b \pmod{n}$, if $n|(b - a)$. Examples: $4 \equiv -1 \pmod{5}$, $3 \equiv 10 \pmod{7}$, $10 \equiv 108 \pmod{7^2}$

Consider the following arithmetic criterion for deciding two rational numbers are equal: Let p be a prime number. Two rational numbers α and β are equal if and only if for all $k \in \mathbb{Z}_{>0}$, p^k divides the numerator of the reduced form of $\alpha - \beta$.

Indeed, 0 is the only integer divisible by p^k for all k . However, we can relax this condition to obtain a criterion for an arithmetic type of “closeness”: Two rational numbers α, β are “ p -adically close” if p^k divides the numerator of the reduced form of $\alpha - \beta$ for “many” k .

Along these lines, we can start thinking of a rational number γ as “similar to” zero, or “close to” zero, or “small p -adically,” if γ is highly divisible by p . To give an example when $p = 5$,

625 is divisible by $5^1, 5^2, 5^3$, and 5^4 , 625 “almost” satisfies equality to 0—it’s 5-adically small.

With this perspective, p -atalanta’s steps $4, 4 \cdot 5, 4 \cdot 5^3, \dots$ are actually getting smaller as they are divisible by increasing powers of p , so that the series run by p -atalanta might reasonably converge to a number under our new notion of closeness.

To make this concrete, we make the following definition.

Definition 1.3

We define the set of p -adic numbers \mathbb{Q}_p to be the set

$$\mathbb{Q}_p = \left\{ \sum_{i=n_0}^{\infty} b_i p^i \mid n_0 \in \mathbb{Z} \text{ and } b_i \in \{0, 1, 2, \dots, p-1\} \right\}$$

Similarly, define the p -adic integers \mathbb{Z}_p to be the set

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} b_i p^i \mid n_0 \in \mathbb{Z} \text{ and } b_i \in \{0, 1, 2, \dots, p-1\} \right\}$$

Another fact that you have likely learned early on in your mathematical career is that the real numbers are uncountable, likely via Cantor’s Diagonalization argument. Cantor’s work was rather controversial at the time; some claimed it was tantamount to polytheism and Kronecker called him a “corrupter of youth.”

Exercise 1.1


Continue the tradition of corrupting the youth by showing \mathbb{Q}_p is uncountable.

1.4 Arithmetic in \mathbb{Q}_p

For any prime p , we can write any natural number in base p by expanding it as a sum of powers of p with coefficients between 0 and $p-1$, inclusive, analogously to its decimal expansion.

We thus have a natural map

$$\begin{aligned} \text{🐱} : \mathbb{N} &\rightarrow \mathbb{Q}_p \\ n &\mapsto \text{the base } p \text{ expansion of } n \end{aligned}$$

(this is called  since we can think of it as expansion into pigits, the p -adic analogue of digits).

The base p expansion of a natural number n can be calculated by a recursive procedure. Carrying out division with remainder, we can write $n = r + p \cdot m$, where r is the remainder. Then the 0th pigit of n is the remainder, r , and the rest of the pigits are the pigits of m , shifted over.

Examples for $p = 7$:


$$77 \mapsto 0 \cdot 7^0 + 4 \cdot 7^1 + 1 \cdot 7^2 + 0 \cdot 7^3 + \dots$$

$$37 \mapsto 2 \cdot 7^0 + 5 \cdot 7^1 + 0 \cdot 7^2 + 0 \cdot 7^3 + \dots$$

$$113 \mapsto 1 \cdot 7^0 + 2 \cdot 7^1 + 2 \cdot 7^2 + 0 \cdot 7^3 + \dots$$

The p -adic integers which have a finite expansion of the form $a = \sum_{i=0}^N b_i p^i$ are precisely those which come from natural numbers. Similarly, p -adic numbers which have a finite expansion $a = \sum_{i=n_0}^N b_i p^i$, with potentially negative n_0 , can be identified with the set of non-negative rational numbers whose denominator is a power of p .

Given a p -adic number $a = \sum_{i=n_0}^{\infty} b_i p^i$, we will let a_n denote the n th approximation $a_n = \sum_{i=n_0}^n b_i p^i$, which we think of as getting closer and closer to a .

The set \mathbb{Q}_p of p -adics is not just a set; we can define addition and multiplication of p -adic numbers, in a way that *extends addition and multiplication in* \mathbb{N} (making  a homomorphism).

To define addition and multiplication of p -adics, consider p -adic numbers $a = \sum_{i=n_0}^{\infty} b_i p^i$ and $a' = \sum_{i=m_0}^{\infty} b'_i p^i$. We can approximate them by finite expansions $a_n = \sum_{i=n_0}^n b_i p^i$ and $a'_m = \sum_{i=m_0}^m b'_i p^i$ and take the sum of these approximations. Importantly, the sum of the approximations $a_n + a'_m$, taken in the usual rational numbers, has the same coefficient of p^i as long as $n, m \geq i$ (think about why). Similarly, $a_n \cdot a'_m$ will have the same coefficient of p^i as long as $n \geq i - m_0$ and $m \geq i - n_0$. Since these pigits of the partial approximations to the sum and product stabilize, we can reasonably define them to be the pigits of $a + a'$ and $a \cdot a'$.

Definition 1.4

We define the sum of two p -adic numbers

$$a = \sum_{i=n_0}^{\infty} b_i p^i, \quad a' = \sum_{i=m_0}^{\infty} b'_i p^i$$

to be the p -adic number, denoted $a + a'$, whose n th pigit is the n th pigit of

$$a_n + a'_n = \sum_{i=n_0}^n b_i p^i + \sum_{i=m_0}^n b'_i p^i$$

where we add a_n and a'_n as rational numbers.

Similarly, the product $a \cdot a'$ is the p -adic number whose n th pigit is the n th pigit of $a_{n-m_0} \cdot a'_{n-n_0}$, multiplied as rational numbers.

We need only examine the numbers up to a finite position in order to compute any particular pigit of their sum or product.

Addition and multiplication obey the usual properties of commutativity, associativity and distributivity. This can be seen by checking each property up to the n th pigit, where it boils down to the analogous properties that we know are true for the rational numbers.

In practice, the algorithms for computing the decimal expansion of the sum and product of two p -adic numbers are directly analogous to the procedure for decimal expansions, and are done “column by column” with “carrying” for quantities that exceed the limit of $p - 1$. For example, for $p = 7$, we have

$$\begin{array}{r} 0 \cdot 7^0 + 4 \cdot 7^1 + 1 \cdot 7^2 + 0 \cdot 7^3 + \dots = 77 \\ + 2 \cdot 7^0 + 5 \cdot 7^1 + 0 \cdot 7^2 + 0 \cdot 7^3 + \dots = 37 \\ \hline + 1 \cdot 7^2 \\ = 2 \cdot 7^0 + 2 \cdot 7^1 + 1 \cdot 7^2 + 0 \cdot 7^3 + \dots = 114 \\ \hline = 2 \cdot 7^0 + 2 \cdot 7^1 + 2 \cdot 7^2 + 0 \cdot 7^3 + \dots = 114 \end{array}$$

and so $\text{pig}(77) + \text{pig}(37) = \text{pig}(77+37)$, as we would expect!

Note, when adding $4+5$ we get 9 , which is not a proper pigit; so we write it as $9 = 2 \cdot 7^0 + 1 \cdot 7$ and carry the 1 .

Now let's look at an example of addition with a p -adic number which does not come from a natural number.

Returning to the course run by p -atalanta, let $p = 5$ and $a = 4 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + 4 \cdot 5^5 + 4 \cdot 5^6 + \dots$

Let us add a to 1:

$$\begin{array}{r} 4 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + 4 \cdot 5^3 + \dots = a \\ + 1 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + 0 \cdot 5^3 + \dots = 1 \\ \hline + 1 \cdot 5^1 \\ = 0 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + 4 \cdot 5^3 + \dots \end{array}$$

since $1 + 4 = 5 = 0 \cdot 5^0 + 1 \cdot 5^1$, so we carry the one. We continue calculating the next pigit:

$$\begin{array}{r} + 1 \cdot 5^2 \\ = 0 \cdot 5^0 + 0 \cdot 5^1 + 4 \cdot 5^2 + 4 \cdot 5^3 + \dots \end{array}$$

We can continue in this way ad infinitum, computing each pigit in turn to be 0, so that we can only conclude that

$$\begin{array}{r} 4 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + 4 \cdot 5^3 + \dots = a \\ + 1 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + 0 \cdot 5^3 + \dots = 1 \\ \hline = 0 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + 0 \cdot 5^3 + \dots = 0 \end{array}$$

Since $a + 1 = 0$, a must equal -1 , the additive inverse of 1. After running her course, p -atalanta finally finds herself at her destination, -1 .



Exercise 1.2

Show that every p -adic number $a \in \mathbb{Q}_p$ has an additive inverse. What are the pigits of the additive inverse $-a$?

What about division? Let's think about what the 5-adic expansion of $1/3$ would be, if such a thing exists. It must be a number of the form $b_0 \cdot 5^0 + b_1 \cdot 5^1 + b_2 \cdot 5^2 + b_3 \cdot 5^3 + \dots$ that, when multiplied by 3, gives 1:

$$3(b_0 \cdot 5^0 + b_1 \cdot 5^1 + b_2 \cdot 5^2 + b_3 \cdot 5^3 + \dots) = 1 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + 0 \cdot 5^3 + \dots$$

The 0th pigit of the product is the 0th pigit of $3b_0 \cdot 5^0$, which is precisely the remainder when $3b_0$ is divided by 5. Thus we have

$$3b_0 \equiv 1 \pmod{5}$$

there is a unique value of $b_0 \in \{0, \dots, 4\}$ that satisfies this linear equation, $b_0 = 2$. Having found b_0 , we can subtract $3b_0 \cdot 5^0 = 1 \cdot 5^0 + 1 \cdot 5^1$ from both sides of the equation:

$$3(b_0 \cdot 5^0 + b_1 \cdot 5^1 + b_2 \cdot 5^2 + b_3 \cdot 5^3 + \dots) - 3b_0 \cdot 5^0 = 0 \cdot 5^0 - 1 \cdot 5^1 + 0 \cdot 5^2 + 0 \cdot 5^3 + \dots$$

$$3(b_1 \cdot 5^1 + b_2 \cdot 5^2 + b_3 \cdot 5^3 + \dots) = 0 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + 4 \cdot 5^3 + \dots$$

where we use our knowledge of the p -adic expansion of -1 . Now we can repeat this procedure to find b_1, b_2 , and so on. Each time we find the pigit that, when multiplied by 3 mod 5, matches the desired pigit, then carry out the multiplication by that pigit and subtract.

We can present this process with long-division shorthand:

$$\begin{array}{r}
 \quad \quad \color{red}{2} \color{orange}{3} \color{yellow}{1} \color{green}{3} \color{blue}{\dots} \\
 3 \left| \begin{array}{r} 1 \color{orange}{0} \color{orange}{0} \color{orange}{0} \color{orange}{0} \color{orange}{0} \color{blue}{\dots} \\ - \color{red}{1} \color{red}{1} \\ \hline \color{orange}{4} \color{orange}{4} \color{orange}{4} \color{orange}{4} \color{blue}{\dots} \\ - \color{orange}{4} \color{yellow}{1} \\ \hline \color{orange}{3} \color{orange}{4} \color{orange}{4} \color{blue}{\dots} \\ - \color{orange}{3} \color{orange}{0} \color{orange}{0} \\ \hline \color{orange}{4} \color{orange}{4} \color{blue}{\dots} \end{array} \right.
 \end{array}$$

This algorithm can always be carried out to find the multiplicative inverse of any nonzero p -adic number.

Theorem 1.5
 \mathbb{Q}_p is a field.

Proof: We have already defined addition and multiplication, and noted that they have the desired properties of commutativity, associativity and distributivity. You will show that every p -adic number has an additive inverse. It remains to show that every nonzero p -adic number has a multiplicative inverse.

It suffices to show that every nonzero p -adic *integer* has a multiplicative inverse. Indeed, any p -adic number a can be written in the form $a = p^{n_0}a'$ where $a' \in \mathbb{Z}_p$. If we can find a multiplicative inverse $(a')^{-1}$, then $p^{-n_0}(a')^{-1}$ will be a multiplicative inverse of a . For similar reasoning we can also assume, by factoring out an appropriate power of p , that $a = \sum_{i=0}^{\infty} b_i p^i$, with $b_0 \neq 0$. We now formalize the algorithm discussed above.

We describe an algorithm to find the digits of a number $x = \sum_{j=0}^{\infty} c_j p^j$ which we claim is a^{-1} . Define c_0 to be the multiplicative inverse of $b_0 \pmod p$ (the existence of this inverse relies crucially on the fact that p is prime and $b_0 \not\equiv 0 \pmod p$). Then use the Euclidean algorithm). Note that this ensures that $a \cdot c_0$ can be written as $1 + pa'$ for some p -adic integer $a' \in \mathbb{Z}_p$. Thus the difference $d_0 := 1 - a \cdot (c_0 p^0) = -pa'$, a number whose first nonzero digit is no earlier than in position p^1 .

Now for the recursive definition, let $m \geq 0$ and assume we have defined c_i for $i \leq m$, in such a way that the difference $d_m := 1 - a \cdot (\sum_{j=0}^m c_j p^j)$ is of the form $p^{m+1}a'$ for some $a' \in \mathbb{Z}_p$. Let the 0th digit of a' be b'_0 . Then define c_{m+1} to be the unique number solving the equation $c_{m+1} \cdot b_0 \equiv b'_0 \pmod p$, which again exists since b_0 is nonzero. With this choice, the difference $d_{m+1} = 1 - a \cdot (\sum_{j=0}^{m+1} c_j p^j)$ must be of the form $p^{m+2}a''$ for some p -adic integer a'' , allowing the recursion to continue.

Now that we have defined the p -adic expansion of x , we must show that $a \cdot x = 1$. Indeed, for any $m \geq 0$ we have by construction that $1 - a \cdot (\sum_{j=0}^m c_j p^j)$ is of the form $p^{m+1}a'$ for some p -adic integer $a' \in \mathbb{Z}_p$. But in particular, this means that 1 and $a \cdot x$ agree on the digits up to position p^m . Since m is arbitrary, $1 = a \cdot x$. \square

1.5 Rooting Around

Let's see if we can find a square root of 2 in \mathbb{Q}_7 . We will look for an element $a = \sum_{i=0}^{\infty} b_i 7^i$ such that $a^2 = 2$, which we represent with the following tableau.

$$\begin{array}{rcccccc}
 & b_0 & + & b_1 \cdot 7 & + & b_2 \cdot 7^2 & + & b_3 \cdot 7^3 & + & \dots \\
 \times & b_0 & + & b_1 \cdot 7 & + & b_2 \cdot 7^2 & + & b_3 \cdot 7^3 & + & \dots \\
 \hline
 & b_0^2 & + & b_0 b_1 \cdot 7 & + & b_0 b_2 \cdot 7^2 & + & \dots & & \\
 + & & & b_0 b_1 \cdot 7 & + & b_1^2 \cdot 7^2 & + & \dots & & \\
 + & & & & & b_0 b_2 \cdot 7^2 & + & \dots & & \\
 \vdots & & & \vdots & & & & & & \\
 \hline
 = & 2 & + & 0 \cdot 7 & + & 0 \cdot 7^2 & + & 0 \cdot 7^3 & + & \dots
 \end{array}$$

The coefficient of 7^i of the product can be calculated by adding all the columns *up to* the i th.

- **Step 0:** From the 0th (red) column of the above sum, we can conclude that we must have $b_0^2 \equiv 2 \pmod{7}$. There are two choices for such a b_0 ; we choose $b_0 = 3$. Note that $b_0^2 = 2 + 1 \cdot 7$, so we carry a 1.
- **Step 1:** Substituting in $b_0 = 3$, the next (orange) column gives $(3b_1 + 3b_1 + 1)7 \equiv 0 \pmod{7^2}$. Equivalently, $3b_1 + 3b_1 + 1 \equiv 0 \pmod{7}$. The unique digit satisfying this is $b_1 = 1$. Again, we carry a 1 to the next column.
- **Step 2:** Substituting in $b_0 = 3$ and $b_1 = 1$, the the next (yellow) column gives $(3b_2 + 1 + 3b_2 + 1)7^2 \equiv 0 \pmod{7^3}$. The unique solution is $b_2 = 2$.

Try to convince yourself that we can continue in this way to successfully compute every digit b_i , so that the resulting number a is a square root of 2.

What about $\sqrt{-1}$ in \mathbb{Q}_7 ? Anything seems possible now! Suppose $a = \sum_{i=0}^{\infty} b_i 7^i$ squares to -1 , which has expansion $6 + 6 \cdot 7 + 6 \cdot 7^2 + \dots$. Then we would have $b_0^2 \equiv 6 \pmod{7}$, but there is no such integer b_0 , and hence no $\sqrt{-1}$.

Undeterred, we look in \mathbb{Q}_5 for a $\sqrt{-1}$, which we will denote $a = \sum_{i=0}^{\infty} b_i 5^i$.

$$\begin{array}{r}
 b_0 + b_1 \cdot 5 + b_2 \cdot 5^2 + b_3 \cdot 5^3 + \dots \\
 \times b_0 + b_1 \cdot 5 + b_2 \cdot 5^2 + b_3 \cdot 5^3 + \dots \\
 \hline
 b_0^2 + b_0 b_1 \cdot 5 + b_0 b_2 \cdot 5^2 + \dots \\
 + b_0 b_1 \cdot 5 + b_1^2 \cdot 5^2 + \dots \\
 + b_0 b_2 \cdot 5^2 + \dots \\
 \vdots \qquad \qquad \qquad \vdots \\
 \hline
 = 4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \dots
 \end{array}$$

- Step 0: $b_0^2 \equiv 4 \pmod{5}$. There are two choices for such a b_0 ; we choose $b_0 = 3$.
- Step 1: $(6b_1 + 1)5 \equiv 4 \pmod{5^2}$. Equivalently, $b_1 + 1 \equiv 4 \pmod{5}$, so $b_1 = 3$.
- Step 2: $b_2 = 2$.

For which primes p do you think \mathbb{Q}_p has a square root of -1 ?

1.6 A Coherent Explanation

We have been doing all these calculations by computing “approximations” to solutions in \mathbb{Q}_p .

In the example we just computed, $\sqrt{-1}$ in \mathbb{Q}_5 , we had

$$\begin{aligned}
 a_0 &= 3 \\
 a_1 &= 3 + 3 \cdot 5 \\
 a_2 &= 3 + 3 \cdot 5 + 2 \cdot 5^2
 \end{aligned}$$

Definition 1.6

A sequence of integers a_n such that $0 \leq a_n \leq p^n = 1$ is **coherent** if for all $n \geq 1$,

$$a_n \equiv a_{n+1} \pmod{p^n}$$

The sequence of approximations a_0, a_1, a_2, \dots is a coherent sequence of solutions to the equation $x^2 = -1 \pmod{p, p^2, p^3, \dots}$. In the next lecture, we will fit this into a formal framework.